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

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

Terminology

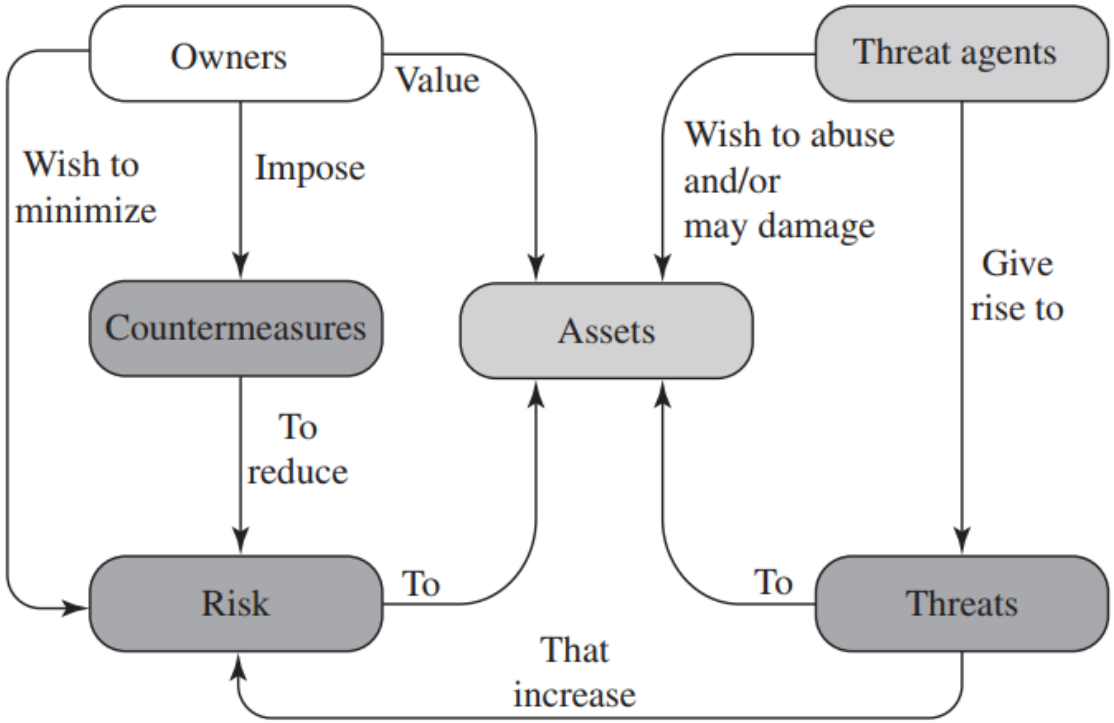
Risk and Security Policy

- 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

Terminology

innovate achieve lead

Security Concepts and Relationships



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

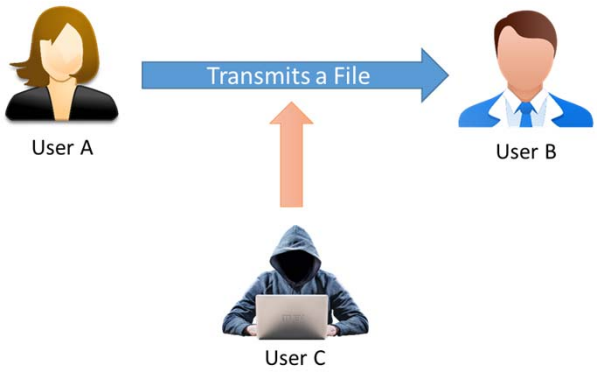
Unauthorized Disclosure

- Exposure
  - A threat action whereby sensitive and confidential data is directly released (or exposed) to an unauthorized entity
  - 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
    - An unauthorized user C is able to monitor the transmission and capture a copy of the file during its transmission



Threats & Attacks

innovate achieve lead

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 a;., 2019, Traffic Analysis Attack for Identifying Users' Online Activities, Published in IT Professional 2019

Threats & Attacks

innovate achieve lead

Unauthorized Disclosure

Threat Action	Types of Threat Actions	Description
Exposure *A threat action whereby sensitive data is directly released to an unauthorized entity.*	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

innovate achieve lead

Unauthorized Disclosure

Threat Action	Types of Threat Actions	Description
Intrusion *A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections.*	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

innovate achieve lead

Unauthorized Disclosure

Threat Action	Types of Threat Actions	Description
Interception *A threat action whereby an unauthorized entity directly accesses sensitive data travelling between authorized sources and destinations*	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
All electric equipment generates electromagnetic signals that are radiated from the equipment. These signals can contain secret information!. An attacker can eavesdrop on these signals and re-create the original information without the knowledge of the user.

Threats & Attacks

innovate achieve lead

Unauthorized Disclosure

Threat Action	Types of Threat Actions	Description
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 byproducts of communications*	Traffic Analysis	Gaining knowledge of data by observing the characteristics of communications that carry the data.
	Signal Analysis	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

innovate achieve lead

Deception

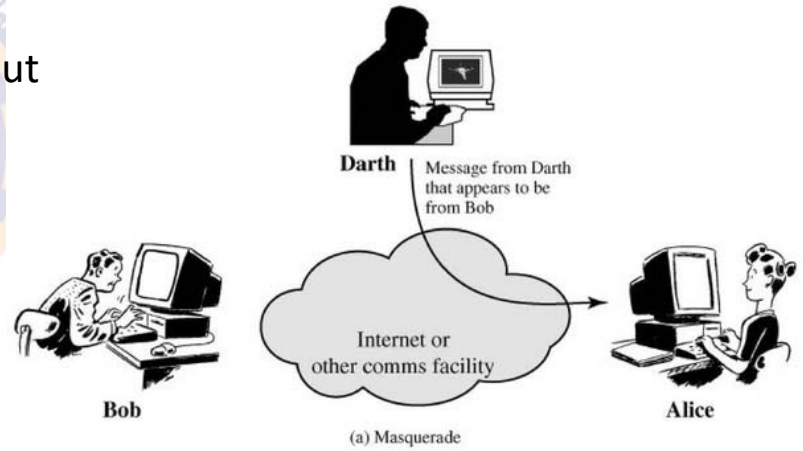
- A circumstance or event that may result in an authorized entity receiving false data and believing it to be true
- The following threat actions can cause deception:
  - Masquerade
    - A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as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

innovate achieve lead

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



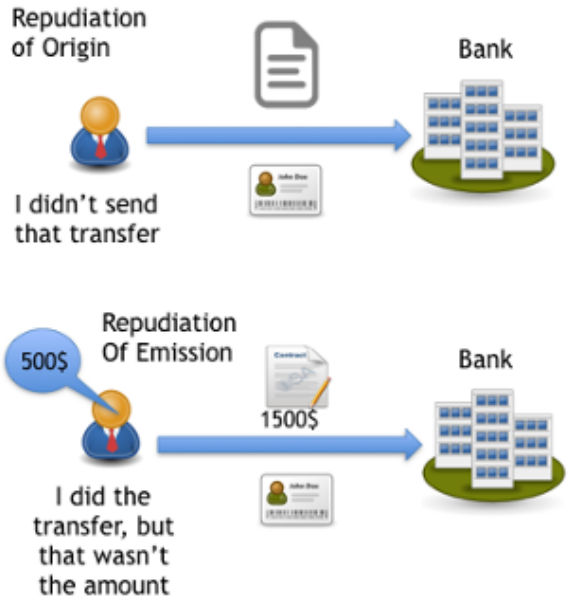
Active Attack – Masquerade

Threats & Attacks

innovate achieve lead

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 *A threat action whereby an unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.*	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 *A threat action whereby false data deceives an authorized entity*	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 *A threat action whereby an entity deceives another by falsely denying responsibility for an act.*	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

innovate achieve lead

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

innovate achieve lead

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 *Prevents or interrupts system operation by disabling a system component*	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
Corruption *A threat action that undesirably alters system operation by adversely modifying system functions or data.*	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

Threats & Attacks

Disruption

Threat Action	Types of Threat Actions	Description
Obstruction *A threat action that interrupts delivery of system services by hindering system operations.*	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 *An entity assumes unauthorized logical or physical control of a system resource.*	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 *A threat action that causes a system component to perform a function or service that is detrimental to system security.*	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 *A circumstance or event whereby an entity gains access to data for which the entity is not authorized*	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 *A circumstance or event that may result in an authorized entity receiving false data and believing it to be true*	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

innovate achieve lead

Summary

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


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!