CSE3501	Information Security Analysis and Audit	L	T	P	J	C
		2	0	2	4	4
Pre-requisite	NIL	Syllabus version				
		1.0				

Objective of the course

1. To introduce system security related incidents and insight on potential defenses, counter measures against common threat/vulnerabilities.
2. To provide the knowledge of installation, configuration and troubleshooting of information security devices.
3. To make students familiarize on the tools and common processes in information security audits and analysis of compromised systems.

Expected Outcome

After successfully completing the course the student should be able to

1. Contribute to managing information security
2. Co-ordinate responses to information security incidents
3. Contribute to information security audits
4. Support teams to prepare for and undergo information security audits
5. Maintain a healthy, safe and secure working environment
6. Provide data/information in standard formats
7. Develop knowledge, skills and competence in information security

Student Learning Outcomes (SLO) 1,2,17

1. Having an ability to apply mathematics and science in engineering applications
2. Having a clear understanding of the subject related concepts and of contemporary issues
17. Having an ability to use techniques, skills and modern engineering tools necessary for engineering practice

1	**Information Security Fundamentals**	7 hours

Definitions & challenges of security, Attacks & services, Security policies, Security Controls, Access control structures, Cryptography, Deception, Ethical Hacking, Firewalls, Identify and Access Management (IdAM).

2	**System Security**	6 hours

System Vulnerabilities, Network Security Systems, System Security, System Security Tools, Web Security, Application Security, Intrusion Detection Systems,

3	**Information Security Management**	3 hours

Monitor systems and apply controls, security assessment using automated tools, backups of security devices, Performance Analysis, Root cause analysis and Resolution, Information Security Policies, Procedures, Standards and Guidelines

4	**Incident Management**	5 hours

Security requirements, Risk Management, Risk Assessment, Security incident management, third party security management, Incident Components, Roles.

5	**Incident Response**	4 hours

Incident Response Lifecycle, Record, classify and prioritize information security incidents using standard templates and tools, Responses to information security incidents, Vulnerability Assessment, Incident Analysis

6	**Conducting Security Audits**	3 hours

Common issues in audit tasks and how to deal with these, Different systems and structures that may need information security audits and how they operate, including: servers and storage devices, infrastructure and networks , application hosting and content management, communication routes such as messaging, Features, configuration and specifications of information security systems and devices and associated processes and architecture, Common audit techniques, Record and report audit tasks, Methods and techniques for testing compliance.

7	**Information Security Audit Preparation**	2 hours

Establish the nature and scope of information security audits, Roles and responsibilities, Identify the procedures/guidelines/checklists, Identify the requirements of information security, audits and prepare for audits in advance, Liaise with appropriate people to gather data/information required for information security audits.

8	**Self and Work Management**	2 hours

Establish and agree work requirements with appropriate people, Keep the immediate work area clean and tidy, utilize time effectively, Use resources correctly and efficiently, Treat confidential information correctly, Work in line with organization's policies and procedures, Work within the limits of their job role.

	Total Lecture hours:	**30 hours**

Text Book(s)

1. William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3rd edition, 2014.
2. Nina Godbole, Information Systems Security: Security Management, Metrics, Frameworks and Best Practices, Wiley, 2017
3. Nina Godbole, Sunit Belapure, Cyber Security- Understanding cyber-crimes, computer forensics and legal perspectives, Wiley Publications, 2016
4. Andrew Vladimirov Michajlowski, Konstantin, Andrew A. Vladimirov, Konstantin V. Gavrilenko, Assessing Information Security: Strategies, Tactics, Logic and Framework, IT Governance Ltd, O'Reilly, 2010

Reference Books

1. Charles P. Pfleeger, Security in Computing, 4th Edition, Pearson, 2009.
2. Christopher J. Alberts, Audrey J. Dorofee , Managing Information Security Risks, Addison-Wesley Professional, 2004
3. Peter Zor, The Art of Computer Virus Research and Defense, Pearson Education Ltd, 2005
4. Lee Allen, Kevin Cardwell, Advanced Penetration Testing for Highly-Secured Environments - Second Edition, PACKT Publishers, 2016
5. Chuck Easttom , System Forensics Investigation and Response, Second Edition, Jones & Bartlett Learning, 2014
6. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni, Metasploit The Penetration Tester's Guide, No Starch Press, 2014
7. Practical Malware Analysis by Michael Sikorski and Andrew Honig, No Starch Press, 2015
9. Ref Links:
   https://www.iso.org/isoiec-27001-information-security.html
   https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final
   https://www.sans.org/reading-room/whitepapers/threats/paper/34180
   https://www.sscnasscom.com/qualification-pack/SSC/Q0901/

List of Experiments (Indicative)	SLO: 1,2,17

- Install and configure information security devices
- Security assessment of information security systems using automated tools.
- Vulnerability Identification and Prioritization
- Working with Exploits
- Password Cracking
- Web Application Security Configuration
- Patch Management
- Bypassing Antivirus Software
- Static Malware Analysis
- Dynamic Malware Analysis
- Penetration Testing
- MySQL SQL Injection
- Risk Assessment
- Information security incident Management
- Exhibit Security Analyst Role

	Total Laboratory Hours	**30 hours**

Recommended by Board of Studies	05.02.2020		
Approved by Academic Council	58	Date	26.02.2020

Introduction to Security

Objectives of the course

- Conduct assessments for **security threats and vulnerabilities** to assess the level of risk.
- Develop appropriate countermeasures in **operational** and **non-operational Situations.**
- Devise testing standards and cases of **confidentiality, integrity, authentication, availability, authorization, and non-repudiation of information.**
- Define and implement privacy standards, build privacy awareness to protect an organization's information assets.

Expected Outcome

- Carry out a security assessment of information security systems using **automated tools.**
- Analyze **information security, performance metrics** and issues for action by appropriate people.
- Organize data/information required for information security audits using standard templates and tools.
- Carry out required audit tasks using standard tools and following established procedures/guidelines/checklists.

Definitions

- Computer Security
  - Generic name for the collection of tools designed to protect data and to thwart hackers
- Network Security
  - Measures to protect data during their transmission
- Internet Security
  - Measures to protect data during their transmission
  - over a collection of interconnected networks
- Information Security
  - Protecting data against the unauthorized access, use, disclosure or disruption of information , especially electronic data, or the other measures taken to achieve.
  - Practice of protecting information by mitigating information risks.

3 Aspects of Security

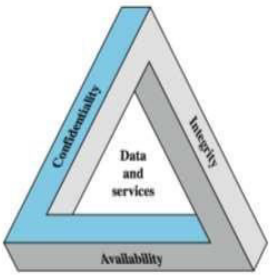
- **Security Attack**
  - Any action that compromises the security of information.
- **Security Mechanism**
  - A mechanism that is designed to detect, prevent, or
  - recover from a security attack.
- **Security Service**
  - A service that enhances the security of data processing systems and information transfers.
    - Makes use of one or more security mechanisms.

Computer Security Concept

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, information/data, and telecommunications).

3 Principles (Goals) of Information Security

1. **Confidentiality**
   - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
2. **Integrity**
   - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
3. **Availability**
   - Ensuring timely and reliable access to and use of information



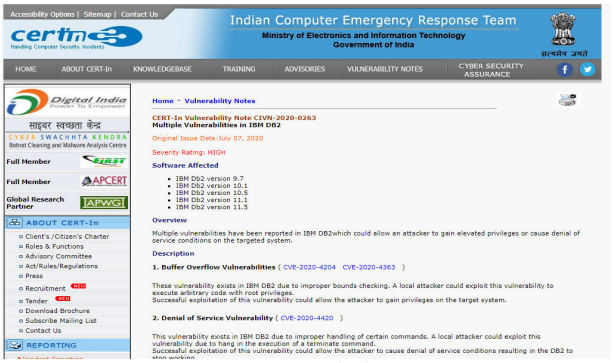
Security Threats

- A **Vulnerability** is a weakness in the security system.
  - For example, in procedures, design, or implementation, that might be exploited to cause loss or harm.
- A **Threat** to a computing system is a set of circumstances that has the potential to cause loss or harm.

Need for Information Security

- To universal growth & use of digital information (as confidential), there has also been a growth in thefts, including cyber attacks by hackers.
- This occurs in both governments and private companies.
- Need for keeping information safe from data breaks using a variety of tools and techniques.
- Information security analysts → protects information on computer network.
- They have special software → keep track of **who can access**, **who have accessed data**.

Sample CERT report



Report – as on 10th July 2020

https://www.cert.govt.nz/it-specialists/guides/how-to-report-a-vulnerability/

Sample CERT report

1. Buffer Overflow Vulnerabilities (CVE-2020-4204 CVE-2020-4363)

These vulnerability exists in IBM DB2 due to improper bounds checking. A local attacker could exploit this vulnerability to execute arbitrary code with root privileges.
Successful exploitation of this vulnerability could allow the attacker to gain privileges on the target system.

2. Denial of Service Vulnerability (CVE-2020-4420)

This vulnerability exists in IBM DB2 due to improper handling of certain commands. A local attacker could exploit this vulnerability due to hang in the execution of a terminate command.
Successful exploitation of this vulnerability could allow the attacker to cause denial of service conditions resulting in the DB2 to stop working.

3. Information Disclosure Vulnerability (CVE-2020-4387 CVE-2020-4386)

This vulnerability exists in IBM DB2 due to a symbolic link. A local attacker could exploit this vulnerability by using race condition of a symbolic link.
Successful exploitation of this vulnerability could allow the attacker to obtain sensitive information on the target system.

4. Denial of Service Vulnerability (CVE-2020-4355)

This vulnerability exists in IBM DB2 due to improper handling of Secure Sockets Layer (SSL) renegotiation requests. A remote attacker could exploit this vulnerability by executing specially crafted DB2 commands and increase the resource usage on the system.
Successful exploitation of this vulnerability could allow the attacker to cause denial of service conditions resulting in the DB2 to stop working.

5. Information Disclosure and Denial of Service Vulnerability (CVE-2020-4414)

This vulnerability exists in IBM DB2 due to improper usage of shared memory. A remote attacker could exploit this vulnerability

Report – as on 10th July 2020

Security analysts

- Focus on three main area
  - **Risk assessment** (identifying risks or issues an organization may face)
  - **Vulnerability assessment** (determining an organization's weaknesses to threats)
  - **Defence planning** (designing the protection architecture and installing security systems such as firewalls and data encryption programs)

Role of a Security Analyst in IT

- **Protect information and information systems from unauthorized access; disclosure; disruption; modification; perusal; inspection; recording**.
- Perform investigations to determine whether or not data has been compromised and related vulnerabilities.
- Ensure the **confidentiality, integrity and availability of data** to the 'right' users within/ outside of the organization.
- **Risk assessment** (identifying risks or issues an organization may face).
- **Vulnerability assessment** (to determine an organization's weaknesses to threats).
- **Defence planning** (designing the protection architecture and installing security systems such as firewalls and data encryption programs)

Types of Attacks

- Passive Attacks
- Active Attacks

PASSIVE ATTACKS

Passive Attacks

- A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities.
- The purpose is solely to gain information about the target and no data is changed on the target.
- In passive reconnaissance, an intruder monitors systems for vulnerabilities without interaction, through methods like session capture.
- In active reconnaissance, the intruder engages with the target system through methods like port scans.

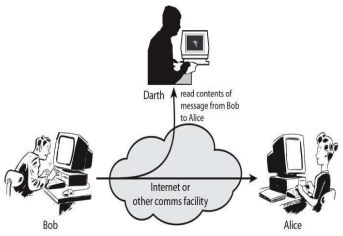
Types of Passive Attacks

- Interception Attack
- Traffic Analysis Attack

Interception

- The phenomenon of confidentiality plays an important role in this type of attack.
- The data or message which is sent by the sender is intercepted by an unauthorized individual where the message will be changed to the different form or it will be used by the individual for his malicious process.
- So the confidentiality of the message is lost in this type of attack.
- It is also known as “Release of message contents”.

Interception

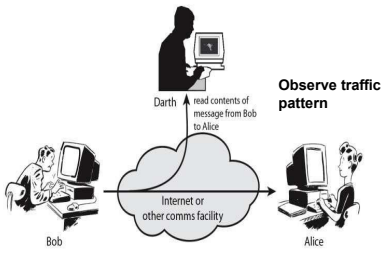


Release of message contents

Traffic Analysis

- Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication.
- It can be performed even when the messages are encrypted and cannot be decrypted.
- In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.
- Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security.

Traffic Analysis



ACTIVE ATTACKS

Active Attacks

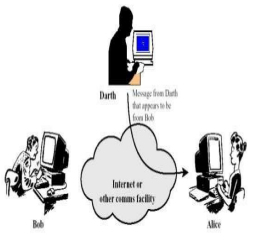
- An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en-route to the target.
- The purpose is to gain information about the target and no data is changed.
- However, passive attacks are often preparatory activities for active attacks.

Types of Active Attacks

- Masquerade Attack
- Interruption Attack
- Fabrication Attack
- Session Replay Attack
- Modification Attack
- Denial of Service (DOS) Attack

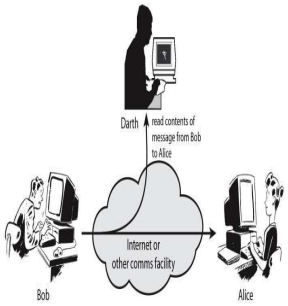
Masquerade

- In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for.
- A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.



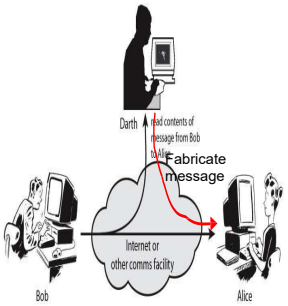
Interruption

- This type of attack is due to the obstruction of any kind during the communication process between one or more systems.
- So the systems which are used become unusable after this attack by the unauthorized users which results in the wastage of systems.



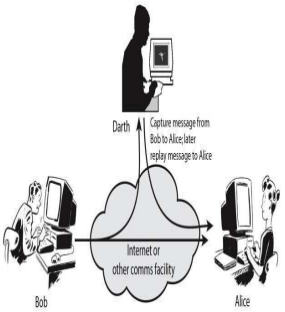
Fabrication

- In this type of attack a fake message is inserted into the network by an unauthorized user as if it is a valid user.
- This results in the loss of confidentiality, authenticity and integrity of the message.



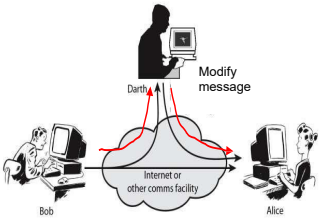
Session Replay Attack

- Session replay attacks, also known as, playback attacks or replay attacks, are network attacks that maliciously "repeat" or "delay" a valid data transmission.
- A hacker can do this by intercepting a session and stealing a user's unique session ID (stored as cookie, URl, or form field).
- Now, the hacker is able to masquerade himself or herself as an authorized user, and he or she will be granted full access to do anything that the authorized user can do on a website.



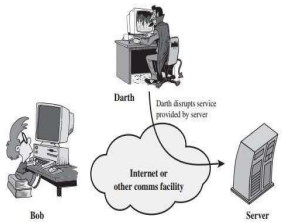
Modification

- In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.



Denial of Service (DOS)

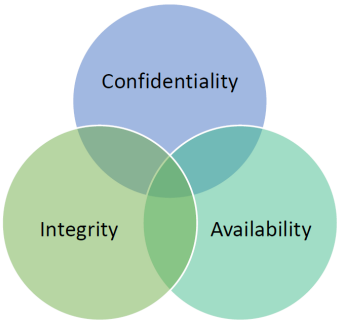
- In a denial of service (DoS) attack, users are deprived of access to a network or web resource.
- This is generally accomplished by overwhelming the target with more traffic than it can handle.



Module-1

INFORMATION ASSETS & THREATS

INFORMATION ASSETS & THREATS



INFORMATION ASSETS & THREATS

Security concerning IT and information is normally categorized in three categories to facilitate the management of information.

Confidentiality

Prevention of unauthorized disclosure or use of information assets

Integrity

Prevention of unauthorized modification of information assets

Availability

Ensuring authorized access of information assets when required for the duration required

THREATS TO INFORMATION ASSETS

- Key concerns of information assets security:
  - Theft
  - Fraud/ Forgery
  - Unauthorized information access
  - Interception or modification of data
  - Data management systems

VULNERABILITIES

- Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
- '**Threat agent or actor**'
  - It refers to the intent and method targeted at the intentional exploitation of the vulnerability or a situation and method that may accidentally trigger the vulnerability.

VULNERABILITIES

- '**Threat vector**'
  - is a path or a tool that a threat actor uses to attack the target.
- '**Threat targets**'
  - Anything that adds value to the threat actor such as PC, laptop, PDA, tablet, mobile phone, online bank account or identity.

THREAT CLASSIFICATION

Microsoft has proposed a threat classification called **STRIDE** from the initials of threat categories:

- **S**poofing of user identity
  - Identity Spoofing refers to the action of assuming (i.e., taking on) the identity of some other entity (human or non-human) and then using that identity to accomplish a goal. An adversary may craft messages that appear to come from a different principle or use stolen / spoofed authentication credentials.
- **T**ampering
  - Data tampering is the act of deliberately modifying (destroying, manipulating, or editing) data through unauthorized channels.
- **R**epudiation
  - A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions.
- **I**nformation disclosure (privacy breach or data leak)
  - Aimed at acquiring system specific information about a web site including software distribution, version numbers, and patch levels.
- **D**enial of Service (D.o.S.)
- **E**scalation of privilege
  - A privilege escalation attack is a type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network and its associated data and applications.

THREAT AGENTS CLASSIFICATION

- **Non-Target specific:**
  - Non-Target specific threat agents are computer viruses, worms, Trojans and logic bombs.
- **Employees:**
  - staff, contractors, operational/ maintenance personnel or security guards who are annoyed with the company.
- **Organized crime and criminals:**
  - criminals target information that is of value to them, such as bank accounts, credit cards or intellectual property that can be converted into money. Criminals will often make use of insiders to help them.

THREAT AGENTS CLASSIFICATION

- **Corporations:**
  - corporations are engaged in offensive information warfare or competitive intelligence. Partners and competitors come under this category.
- **Unintentional human error:**
  - accidents, carelessness etc.
- **Intentional human error:**
  - insider, outsider etc.
- **Natural:**
  - Flood, fire, lightning, meteor, earthquakes etc.

References

- https://www.ibm.com/support/knowledgecenter/SSB2MG_4.6.0/com.ibm.ips.doc/concepts/wap_information_disclosure.htm
- https://owasp.org/www-community/attacks/Repudiation_Attack#:~:text=Description,the%20identification%20of%20new%20actions.
- https://www.forcepoint.com/cyber-edu/spoofing
- https://study.com/academy/lesson/what-is-data-tampering-definition-prevention.html#:~:text=Data%20tampering%20is%20the%20act,editing)%20data%20through%20unauthorized%20channels.&text=In%20both%20instances%2C%20the%20intrusion,program%2C%20or%20organization%20can%20face.

Security Threats & Attacks

TYPES OF SECURITY ATTACKS

- VIRUS
- WORM
- TROJAN

VIRUS

- Virus is a malicious program able to inject its code into other programs/ applications or data files and the targeted areas become "infected".
- Installation of a virus is done without user's consent, and spreads in form of executable code transferred from one host to another.

Types of viruses

- Resident virus,
- Non-resident virus;
- Boot sector virus;
- Macro virus;
- File-infecting virus (fileinfector);
- Polymorphic virus;
- Metamorphic virus;
- Stealth virus;
- Companion virus
- Cavity virus.

Types of viruses

- **Resident virus** - Virus that embeds itself in the memory on a target host. It gets activated every time the OS starts or executes a specific action.
- **Non-resident virus** - when executed, this type of virus actively seeks targets for infections either on local, removable or on network locations.
- **Boot sector virus**
  - A boot sector virus is a computer virus that infects a storage device's master boot record (MBR).
  - It is not mandatory that a boot sector virus successfully boot the victim's PC to infect it.
  - As a result, even non-bootable media can trigger the spread of boot sector viruses.
  - These viruses copy their infected code either to the floppy disk's boot sector or to the hard disk's partition table.
  - During start-up, the virus gets loaded to the Computer's memory. As soon as the virus is saved to the memory, it infects the non-infected disks used by the system.

Types of Viruses

- **Macro virus**
  - Virus in macro language, embedded in Word, Excel, Outlook etc. documents.
  - It is executed as soon as the document that contains it is opened.
  - It corresponds to the macro execution within those documents, which under normal circumstances is automatic.
- **File-infecting virus (file-infector)**
  - When the infected file is being executed, the virus seeks out other files on the host and infects them with malicious code.
  - The malicious code is inserted either at the beginning of the host file code (prepending virus), in the middle (mid-infector) or in the end (appending virus).
- **Polymorphic virus**
  - Complicated computer virus that affects data types and functions.
  - Self-encrypted virus designed to avoid detection by a scanner.
  - Upon infection, it duplicates itself by creating usable, slightly modified, copies of itself.
- **Metamorphic virus**
  - Capable of changing its own code with each infection.
  - Rewriting process may cause the infection to appear different each time but the functionality of the code remains the same.

Types of Viruses

- **Stealth virus**
  - Memory resident virus utilizes various mechanisms to avoid detection.
  - E.g. by removing itself from the infected files and placing a copy of itself in a different location.
  - It maintain a clean copy of the infected files to provide it to the antivirus engine for scan while the infected version will remain undetected.
- **Armored virus**
  - Designed to thwart attempts by Analysts from examining its code by using various methods to make tracing, disassembling and reverse engineering more difficult.
  - It also protect itself from antivirus programs, making it more difficult to trace.
  - Attempts to trick the antivirus program into believing that its location is somewhere other than where it really is on the system.
- **Multipartite virus**
  - Attempts to attack both the file executable and the master boot record of the drive at the same time.

Types of viruses

- Camouflage virus
  - Able to report as a harmless program to the antivirus software.
  - Virus is similar code to the legitimate non-infected files code the antivirus application is tricked into believing that it has to do with the legitimate program as well.
  - Antivirus solutions have become more elaborate whereas the camouflage viruses are quite rare and not a serious threat due to the ease of their detection.
- Companion virus
  - Companion virus is a complicated computer virus, which, unlike traditional viruses, does not modify any files.
  - It creates a copy of the file and places a different extension on it, usually .com.
  - Unique quality makes it difficult to detect, as anti-virus software tends to use changes in files as clue.
- Cavity virus
  - Unlike traditional viruses the cavity virus does not attach itself to the end of the infected file but instead uses the empty spaces within the program files itself

WORM

- Worm is a malicious program category, exploiting operating system vulnerabilities to spread itself.
- In its design, worm is quite similar to a virus - considered even its sub-class.
- Unlike the viruses though worms can reproduce/ duplicate and spread by itself.

Types of WORMs

Email worms:

- spread through email messages, especially through those with attachments.

Internet worms:

- spread directly over the internet by exploiting access to open ports or system vulnerabilities**.**

Network worms:

- spread over open and unprotected network shares.

Multi-vector worms:

- having two or more various spread capabilities.

TROJAN

- Computer Trojan or Trojan Horses are named after the mythological Trojan horse owing to their similarity in operation strategy.
- Trojans are a type of malware software that masquerades itself as a not-malicious even useful application but it will actually do damage to the host computer after its installation.
- Unlike virus, Trojans do not self-replicate unless end user intervene to install.

Types of Trojan

- Remote Access Trojans (RAT) aka Backdoor Trojan
- Trojan-DDoS
- Trojan-Proxy
- Trojan-FTP
- Destructive Trojan
- Security Software Disabler Trojan
- Info Stealer (Data Sending/ Stealing Trojan)
- Keylogger Trojan
- Trojan - PSW (Password Stealer)
- Trojan - Banker
- Trojan-IM,.. etc..

Types of Trojan

- Remote Access Trojans (RAT) aka Backdoor Trojan
  - opens backdoor on the targeted system to allow the attacker remote access to the system or even complete control over it.
  - used as an entry point for DOS attack or for allowing worms or even other Trojans to the system.
  - A computer with a sophisticated backdoor program installed also may be referred as a "zombie" or a "bot".
  - A network of such bots may often be referred to as a "botnet".
- Trojan-DDoS
  - This Trojan is installed simultaneously on a large number of computers in order to create a zombie network (botnet) of machines that can be used (as attackers) in a DDoS attack on a particular target.
- Trojan-Proxy
  - A proxy Trojan is a virus, which hijacks and turns the host computer into a proxy server, part of a botnet, from which an attacker can stage anonymous activities and attacks.
- Trojan-FTP
  - Designed to open FTP ports on the targeted machine and allows a remote attacker to access the host.
  - Attacker can also access as well network shares or connections to further extent more and other threats.
- Destructive Trojan
  - This is designed to destroy or delete data. It is much like a virus.

Types of Trojan

- Keylogger Trojan
  - Data-sending Trojan that is recording every keystroke of the end user.
  - Used to steal sensitive information from targeted host and send it back to attacker.
  - Goal is to collect as much data as possible without any direct specification what the data will be.
- Trojan-PSW (Password Stealer)
  - Data-sending Trojans designed specifically to steal passwords from the targeted systems.
  - Its execution routine, it will very often first drop a keylogging component onto the infected machine.
- Trojan-Banker
  - Designed to steal online banking information to allow attacker further access to bank account or credit card information.
- Trojan-IM
  - A type of data-sending Trojan designed specifically to steal data or account information from instant messaging programs like MSN, Skype etc.
- Trojan-Game Thief
  - Trojan designed to steal information about online gaming account.

Types of Trojan

- Trojan Mail Finder – A Trojan used to harvest any emails found on the infected computer. The email list is then forwarded to the remote attacker.
- Trojan-Dropper - A Trojan-Dropper is a type of trojan that drops different type of standalone malware (trojans, worms, backdoors) to a system. It is usually an executable file that contains other files compressed inside its body. When a Trojan-Dropper is performed, it extracts these compressed files and saves them to a folder (usually a temporary one) on the computer.
- Trojan.Downloader – A Trojan that can download other malicious programs to the target computer. Very often combined with the functionality of Trojan-Dropper. Most downloaders that are encountered will attempt to download content from the internet rather than the local network. In order to successfully achieve its primary function, a downloader must run on a computer that is inadequately protected and connected to a network.
- Trojan.FakeAV – Trojan.FakeAV is a detection for Trojan horse programs that intentionally misrepresent the security status of a computer. These programs attempt to convince the user to purchase software in order to remove non-existent malware or security risks from the computer.
- Trojan-Spy – this Trojan has a similar functionality to the Info stealer or Trojan-PSW and its purpose is to spy on the actions executed on the target host. These can include tracking data entered via keystrokes, collecting screenshots, listing active processes/ services on the host or stealing passwords.

Types of Trojan

- Trojan-ArcBomb -These Trojans are archives designed to freeze or trigger slow performance or to flood the disk with a large amount of “empty” data when an attempt is made to unpack the archived data. The so-called archive bombs pose a particular threat for file and mail servers when an automated processing system is used to process incoming data.
- Trojan-Clicker or Trojan-AD clicker – A Trojan that continuously attempts to connect to specific websites in order to boost the visit counters on those sites. More specific functionality of the Trojan can include generating traffic to pay-per-click web advertising campaigns in order to create or boost revenue.
- Trojan-SMS – A Trojan used to send text messages from infected mobile devices to premium rate paid phone numbers.
- Trojan-Ransom (Trojan-Ransomlock) aka Ransomware Trojan - Trojan.Ransomlock is detection for Trojan horse programs that lock the desktop of a compromised computer making it unusable. The threat may arrive on the compromised computer by various means, such as visiting malicious sites, by opening untrusted links or advertisement
- Cryptolock Trojan (Trojan.Cryptolocker) – This is a new variation of Ransomware Trojan emerged in 2013, in a difference to a Ransomlock Trojan (that only locks computer screen or some part of computer functionality), the Cryptolock Trojan encrypts and locks individual files.

Types of Trojan

- Security Software Disabler Trojan – This is designed to stop security programs like antivirus solutions, firewalls or IPS either by disabling them or by killing the processes. This kind of Trojan functionality is combined often with destructive Trojan that can execute data deletion or corruption only after the security software is disabled. Security Software Disablers are entry Trojans that allow next level of attack on the targeted system.
- Info Stealer (Data Sending/ Stealing Trojan) - This Trojan is designed to provide an attacker with confidential or sensitive information from compromised host and send it to a predefined location (attacker). The stolen data comprise of login details, passwords, PII, credit card information etc. Data sending Trojans can also be designed to look for specific information only or can be more generic like Key-logger Trojans. Nowadays more than ever before attackers are concentrating on compromising end users for financial gain. The information stolen with use of Info stealer Trojan is often sold on the black market. Info stealers gather information by using several techniques. The most common techniques may include log key strokes, screen shots and web cam images, monitoring internet activity often for specific financial websites. The stolen information may be stored locally so that it can be retrieved for later use or it can be sent to a remote location where it can be accessed by an attacker. It is often encrypted before posting it to the malware author.

Other Security threats

Malware

- Malware refers to software viruses, spyware, adware, worms, Trojans, ransomeware etc.
- They are designed to cause damage to a targeted computer or cause a certain degree of operational disruption.

Rootkit

- Rootkit are malicious software designed to hide certain processes or programs from detection.
- Usually acquires and maintains privileged system access while hiding its presence in the same time. It acts as a conduit by providing the attacker with a backdoor to a system

Other security threats

Spyware

- Spyware is a software that monitors and collects information about a particular user, computer or organization without user's knowledge.
- There are different types of spyware, namely system monitors, trojans (keyloggers, banker trojans, inforstealers), adware, tracking cookies etc.

Tracking cookies

- Tracking cookies are a specific type of cookies that are distributed, shared and read across two or more unrelated websites for the purpose of gathering information or potentially to present.

Other security threats

Riskware

- Riskware is a term used to describe potentially dangerous software whose installation may pose a risk to the computer.

Adware

- Adware in general term adware is software generating or displaying certain advertisements to the user.
- This kind of adware is very common for freeware and shareware software and can analyze end user internet habits and then tailor the advertisements directly to users' interests.

Other Security threats

Creepware

- Creepware is a term used to describe activities like spying others through webcams (very often combined with capturing pictures), tracking online activities of others and listening to conversation over the computer's microphone and stealing passwords and other data.

Blended threat

- Blended threat defines an exploit that combines elements of multiple types of malware components.
- Usage of multiple attack vectors and payload types targets to increase the severity of the damage causes and as well the speed of spreading.

NETWORK ATTACKS

- Network attack is defined as an intrusion on the network infrastructure to first analyze the environment and collect information in order to exploit the existing open ports or vulnerabilities.
- This may include unauthorized access to organization resources.

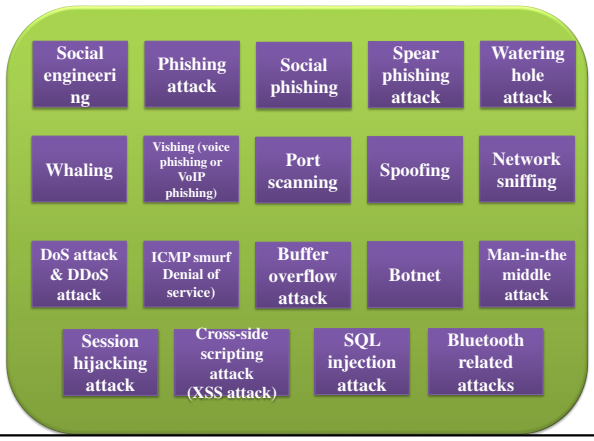
NETWORK ATTACKS

- **Passive attacks:** Refer to attack where the purpose is only to learn and get some information from the system, but the system resources are not altered or disabled in any way.
- **Active attacks:** Type of network attack, the perpetrator accesses and either alters, disables or destroys resources or data.

NETWORK ATTACKS

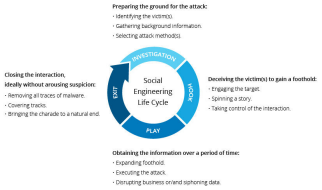
- **Outside attack:**
  - when attack is performed from outside of the organization by unauthorized entity it is said to be an outside attack.
- **Inside attack:**
  - if an attack is performed from within the company by an "insider" that already has certain access to the network it is considered to be an inside attack.
- **Others**
  - such as end users targeted attacks (like phishing or social engineering): these attacks are not directly referred to as network attacks, but are important to know due to their widespread occurrences.

What types of attack are there?



What is social engineering?

- Social engineering attacks come in many different forms and can be performed anywhere where human interaction is involved.
- Social engineering is the term used for a broad range of malicious activities accomplished through human interactions.
- It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.



Social engineering attack techniques

- Social engineering attacks happen in one or more steps.
- A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack.
- Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Social engineering attack techniques

- Baiting
  - As its name implies, baiting attacks use a false promise to pique a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.
  - The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list.
  - Victims pick up the bait out of curiosity and insert it into a work or home computer, resulting in automatic malware installation on the system.
  - Baiting scams don't necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

Social engineering attack techniques

- Pretexting
  - An attacker obtains information through a series of cleverly crafted lies.
  - The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.
  - The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority.
  - The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.
  - All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Social engineering attack techniques

- Phishing
  - As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.
  - An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.
  - Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having access to threat sharing platforms.

Social engineering attack techniques

- Spear phishing
  - This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.
  - A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

Social engineering prevention

- Don't open emails and attachments from suspicious sources – If you don't know the sender in question, you don't need to answer an email.
- Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site.
- Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.
- Use multifactor authentication – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise. Imperva Login Protect is an easy-to-deploy 2FA solution that can increase account security for your applications.
- Be wary of tempting offers – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.
- Keep your antivirus/antimalware software updated – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

Distributed denial of service attack (DDoS)

- A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server.
- DoS and DDoS attacks can be divided into three types:
  - Volume Based Attacks: Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second.
  - Protocol Attacks: Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).
  - Application Layer Attacks: Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second (Rps).

Common DDoS attacks types

- UDP Flood: A UDP flood is any DDoS attack that floods a target with User Datagram Protocol (UDP) packets. The goal of the attack is to flood random ports on a remote host. This causes the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP 'Destination Unreachable' packet. This process saps host resources, which can ultimately lead to inaccessibility.
- ICMP (Ping) Flood: Similar to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown.

Common DDoS attacks types

- SYN Flood: A SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (the "three-way handshake"), wherein a SYN request to initiate a TCP connection with a host must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in denial of service.

Common DDoS attacks types

- Ping of Death: A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size – for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.
- Slowloris: Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server, but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.

Common DDoS attacks types

- NTP Amplification: In NTP amplification attacks, the perpetrator exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm a targeted server with UDP traffic. The attack is defined as an amplification assault because the query-to-response ratio in such scenarios is anywhere between 1:20 and 1:200 or more. This means that any attacker that obtains a list of open NTP servers (e.g., by a using tool like Metasploit or data from the Open NTP Project) can easily generate a devastating high-bandwidth, high-volume DDoS attack.
- HTTP Flood: In an HTTP flood DDoS attack, the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application. HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to every single request.
- Zero-day DDoS Attacks: The "Zero-day" definition encompasses all unknown or new attacks, exploiting vulnerabilities for which no patch has yet been released. The term is well-known amongst the members of the hacker community, where the practice of trading zero-day vulnerabilities has become a popular activity.

Motivation behind DDoS attacks

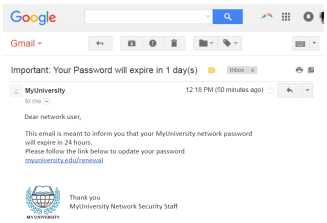
- DDoS attacks are quickly becoming the most prevalent type of cyber threat, growing rapidly in the past year in both number and volume according to recent market research. The trend is towards shorter attack duration, but bigger packet-per-second attack volume.
- Attackers are primarily motivated by:
  - Ideology – So called "hacktivists" use DDoS attacks as a means of targeting websites they disagree with ideologically.
  - Business feuds – Businesses can use DDoS attacks to strategically take down competitor websites, e.g., to keep them from participating in a significant event, such as Cyber Monday.
  - Boredom – Cyber vandals, a.k.a., "script-kiddies" use prewritten scripts to launch DDoS attacks. The perpetrators of these attacks are typically bored, would-be hackers looking for an adrenaline rush.
  - Extortion – Perpetrators use DDoS attacks, or the threat of DDoS attacks as a means of extorting money from their targets.
  - Cyber warfare – Government authorized DDoS attacks can be used to both cripple opposition websites and an enemy country's infrastructure.

What is a phishing attack?

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.
- It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.
- The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.
- An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Phishing attack examples

- The following illustrates a common phishing scam attempt:
  - A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.
  - The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.



Spear phishing

- Spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in-depth version of phishing that requires special knowledge about an organization, including its power structure.
- An attack might play out as follows:
  - A perpetrator researches names of employees within an organization's marketing department and gains access to the latest project invoices.
  - Posing as the marketing director, the attacker emails a departmental project manager (PM) using a subject line that reads, Updated invoice for Q3 campaigns. The text, style, and included logo duplicate the organization's standard email template.
  - A link in the email redirects to a password-protected internal document, which is in actuality a spoofed version of a stolen invoice.
  - The PM is requested to log in to view the document. The attacker steals his credentials, gaining full access to sensitive areas within the organization's network.
  - By providing an attacker with valid login credentials, spear phishing is an effective method for executing the first stage of an APT.

What is a Ping of Death attack?

- Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.
- PoD attacks exploit legacy weaknesses which may have been patched in target systems.
- New type of PoD attack has become popular, known as a Ping flood, the targeted system is hit with ICMP packets sent rapidly via ping without waiting for replies.
- Since sending a ping packet larger than 65,535 bytes violates the Internet Protocol, attackers would generally send malformed packets in fragments.
- When the target system attempts to reassemble the fragments and ends up with an oversized packet, memory overflow could occur and lead to various system problems including crash.

Ping (ICMP) flood attack

- Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings.
- The attack involves flooding the victim's network with request packets, knowing that the network will respond with an equal number of reply packets.
- Additional methods for bringing down a target with ICMP requests include the use of custom tools or code, such as hping and scapy.
- Normally, ping requests are used to test the connectivity of two computers by measuring the round-trip time from when an ICMP echo request is sent to when an ICMP echo reply is received.
- During an attack, they are used to overload a target network with data packets.
- Executing a ping flood is dependent on attackers knowing the IP address of their target.

Ping flood attack Description

- Attacks can be broken down into three categories, based on the target and how its IP address is resolved.
  - **A targeted local disclosed ping flood** targets a single computer on a local network. An attacker needs to have physical access to the computer in order to discover its IP address. A successful attack would result in the target computer being taken down.
  - **A router disclosed ping flood** targets routers in order to disrupt communications between computers on a network. It is reliant on the attacker knowing the internal IP address of a local router. A successful attack would result in all computers connected to the router being taken down.
  - **A blind ping flood** involves using an external program to uncover the IP address of the target computer or router before executing an attack.

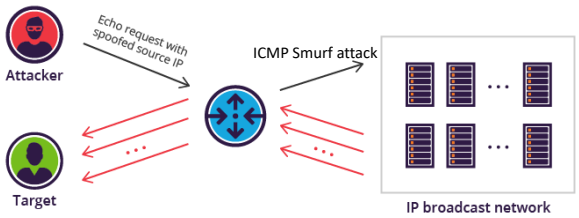
What is a Smurf attack

- Smurf is a network layer distributed denial of service (DDoS) attack, named after the DDoS.
- A Smurf malware enables it execution.
- Smurf attacks are somewhat similar to ping floods, as both are carried out by sending a slews of ICMP Echo request packets.
- Unlike the regular ping flood, however, Smurf is an amplification attack vector that boosts its damage potential by exploiting characteristics of broadcast networks.

ICMP Smurf attack

- A Smurf attack scenario can be broken down as follows:
  - Smurf malware is used to generate a fake Echo request containing a spoofed source IP, which is actually the target server address.
  - The request is sent to an intermediate IP broadcast network.
  - The request is transmitted to all of the network hosts on the network.
  - Each host sends an ICMP response to the spoofed source address.
  - With enough ICMP responses forwarded, the target server is brought down.

ICMP Smurf attack



SPOOFING

It is a technique used to masquerade a person, program or an address as another by falsifying the data with purpose of unauthorized

- **IP Address spoofing**

  – process of creating IP packets with forged source IP address to impersonate legitimate system. This kind of spoofing is often used in DoS attacks (Smurf Attack).

- **ARP spoofing (ARP Poisoning)**

  – process of sending fake ARP messages in the network. The purpose of this spoofing is to associate the MAC address with the IP address of another legitimate host causing traffic redirection to the attacker host. This kind of spoofing is often used in man-in-the-middle attacks.

SPOOFING

- **DNS spoofing (DNS Cache Poisoning)**

  – an attack where the wrong data is inserted into DNS Server cache, causing the DNS server to divert the traffic by returning wrong IP addresses as results for client queries.

- **Email spoofing**

  – a process of faking the email's sender "from" field in order to hide real origin of the email. This type of spoofing is often used in spam mail or during phishing attack.

- **Search engine poisoning**

  – attackers take advantage of high profile news items or popular events that may be of specific interest for certain group of people to spread malware and viruses.

NETWORK SNIFFING (Packet Sniffing)

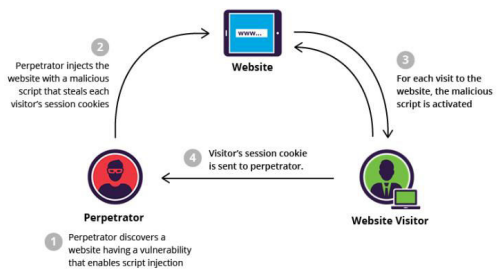
- A process of capturing the data packets travelling in the network.This may include unauthorized access to organization resources.
- Network sniffing can be used both by IT professionals to analyse and monitor the traffic for example, in order to find unexpected suspicious traffic, but as well by perpetrators to collect data send over clear text that is easily readable with use of network sniffers (protocol analysers).
- Best counter measure against sniffing is the use of encrypted communication between the hosts.

Denial of Service Attack (DoS Attack) and Distributed Denial of Service Attack (DDoS Attack)

- An attack designed to cause an interruption or suspension of services of a specific host/ server by flooding it with large quantities of useless traffic or external communication requests.
- When the DoS attack succeeds the server is not able to answer even to legitimate requests anymore, this can be observed in numbers of ways – slow response of the server, slow network performance, unavailability of software or web page, inability to access data, website or other resources.
- Distributed Denial of Service Attack (DDoS) occurs where multiple compromised or infected systems (botnet) flood a particular host with traffic simultaneously.

Common DoS Attack types…

- ICMP flood attack (Ping Flood)
- Ping of Death (PoD)
- Smurf attack
- ICMP Smurf Denial of Service SYN flood attack
- Buffer overflow attack
- Botnet
- Man-in-the-middle attack
- Session hijacking attack
- Cross-side scripting attack (XSS attack)
- SQL injection attack.



Bluetooth related attacks

- Bluesnarfing
- Bluejacking
- Bluebugging

References

- https://blog.finjan.com/tcpip-vulnerabilities/

Module-1

INFORMATION ASSETS & THREATS

Vulnerability Enumeration

Common Vulnerabilities and Exposures (CVE)

- Common Vulnerabilities and Exposures (CVE) is a catalogue of known security threats.
- Threats are divided into two categories:
    - Vulnerabilities and
    - Exposures.

Common Vulnerabilities and Exposures (CVE)

- Common Vulnerabilities and Exposures (CVE) is a dictionary of common names (i.e. CVE Identifiers) for publicly known information/cyber security vulnerabilities.
- CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools.
- If a report from one of your security tools incorporates CVE identifiers, you may then quickly and accurately access fix information in one or more separate CVE compatible databases to remediate the problem.

Common Vulnerability Scoring System (CVSS)

- Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- Its quantitative model ensures repeatable, accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.
- CVSS is well suited as a standard measurement system for industries, organizations and governments that need accurate and consistent vulnerability impact scores.

https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

Common Weakness Enumeration (CWE)

- Common Weakness Enumeration Specification (CWE) provides a common language of discourse for discussing, finding and dealing with the causes of software security vulnerabilities as they are found in code, design or system architecture.
- Each individual CWE represents a single vulnerability type.
- CWEs are used as a classification mechanism that differentiates CVEs by the type of vulnerability they represent.

Module-1

Elements of Information Security

Elements of Information Security

- **Network Security**
  - Network security refers to any activity designed to protect the **usability, reliability, integrity and safety** of your network and data.
  - Network security is accomplished through hardware and software where the software must be constantly updated and managed to protect you from emerging threats.

Elements of Information Security (Network Security)…

- Network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.
- Mobility of Wireless networks adds more challenges to security, namely monitoring and maintenance of secure traffic transport of mobile nodes.
- At Terminal, it is important to protect its resources (battery, disk, CPU) against misuse and ensure the confidentiality of its data.
- Ad hoc or sensor network, it becomes essential to ensure terminal's integrity as it plays a dual role of router and terminal.

Elements of Information Security

Network security components often include:

- Anti-virus and anti-spyware
- Firewall to block unauthorized access into the network
- Intrusion Prevention Systems (IPS) to identify fast-spreading threats, such as zero-day or zero-hour attacks
- Virtual Private Networks (VPNs) to provide secure remote access
- Communication security

Application Security

- Application security encompasses measures taken to improve the security of an application often by **finding, fixing and preventing security vulnerabilities.**
- Different techniques are used to surface such security vulnerabilities at different stages of an applications lifecycle such as **design, development, deployment, upgrade, maintenance.**
- **Terms**
  - **Asset** - Resource of value such as the data in a database, money in an account, file on the file system or any system resource.
  - **Vulnerability** - A weakness or gap in security program that can be exploited by threats to gain unauthorized access to an asset.
  - **Attack (or exploit)** - An action taken to harm an asset.
  - **Threat** - Anything that can exploit a vulnerability and obtain, damage, or destroy an asset.

Application Security

- **Three distinct elements:**
  - Measurable reduction of risk in existing applications
  - Prevention of introduction of new risks
  - Compliance with software security mandates

Application Security Techniques

- Different techniques will find different subsets of the security vulnerabilities lurking in an application and are most effective at different times in the software lifecycle. They each represent different tradeoffs of time, effort, cost and vulnerabilities found.
- **Techniques**
  - **Whitebox security review, or code review.** This is a security engineer deeply understanding the application through manually reviewing the source code and noticing security flaws. Through comprehension of the application vulnerabilities unique to the application can be found.
  - **Blackbox security audit.** This is only through use of an application testing it for security vulnerabilities, no source code required.
  - **Design review.** Before code is written working through a threat model of the application. Sometimes alongside a spec or design document.
  - **Tooling.** There exist many automated tools that test for security flaws, often with a higher false positive rate than having a human involved.
  - **Coordinated vulnerability platforms. H**acker-powered application security solutions offered by many websites and software developers by which individuals can receive recognition and compensation for reporting bugs.
- Utilizing these techniques appropriately throughout the software development life cycle (SDLC) to maximize security is the role of an application security team.

Application Security

- **Application Security market has reached sufficient maturity to allow organizations of all sizes to follow a well-established roadmap:**
  - Begin with software security testing to find and assess potential vulnerabilities
  - Follow remediation procedures to prioritize and fix them.
  - Train developers on secure coding practices.
  - Leverage ongoing threat intelligence to keep up-to-date.
  - Develop continuous methods to secure applications throughout the development life cycle.
  - Instantiate policies and procedures that in still good governance.

Application threats and attacks

- According to the patterns & practices Improving Web Application Security book, the following are classes of common application security threats and attacks:

Category	Threats & Attacks
Input Validation	Buffer overflow; cross-site scripting; SQL injection; canonicalization
Software Tampering	Attacker modifies an existing application's runtime behavior to perform unauthorized actions; exploited via binary patching, code substitution, or code extension
Authentication	Network eavesdropping; Brute force attack; dictionary attacks; cookie replay; credential theft
Authorization	Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
Configuration management	Unauthorized access to administration interfaces; unauthorized access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
Sensitive information	Access sensitive code or data in storage; network eavesdropping; code/data tampering
Session management	Session hijacking; session replay; man in the middle
Cryptography	Poor key generation or key management; weak or custom encryption
Parameter manipulation	Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
Exception management	Information disclosure; denial of service
Auditing and logging	User denies performing an operation; attacker exploits an application without trace; attacker covers his or her tracks

OWASP

- The Open Web Application Security Project (OWASP) is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.
- The OWASP community publishes a list of the top 10 vulnerabilities for web applications
- It outlines best security practices for organizations and while aiming to create open standards for the industry

OWASP

Category	Threats / Attacks
Injection	SQL injection; NoSQL; OS Command; Object-relational mapping; LDAP injection
Broken authentication	Credential stuffing; brute force attacks; weak passwords
Sensitive data exposure	Weak cryptography; un-enforced encryption
XML external entities	XML external entity attack
Broken access control	CORS misconfiguration; force browsing; elevation of privilege
Security misconfiguration	Unpatched flaws; failure to set security values in settings; out of date or vulnerable software
Cross-site scripting (XSS)	Reflected XSS; Stored XSS; DOM XSS
Insecure deserialization	Object and data structure is modified; data tampering
Using components with known vulnerabilities	Out of date software; failure to scan for vulnerabilities; failure to fix underlying platform frameworks; failure to updated or upgraded library compatibility
Insufficient logging & monitoring	Failure to log auditable events; failure to generate clear log messages: inappropriate alerts; failure to detect or alert for active attacks in or near real-time

https://owasp.org/www-project-top-ten/

Communications Security

- Communications Security (COMSEC) ensures the security of telecommunications confidentiality and integrity – the two information assurance (IA) pillars.
- Generally, COMSEC may refer to the security of any information that is transmitted, transferred or communicated.

Five COMSEC Security Types

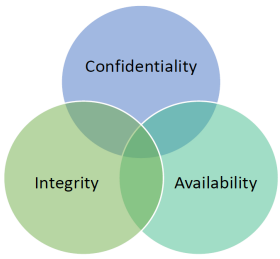
1. **Crypto security:** Encrypts data, rendering it unreadable until the data is decrypted.
2. **Emission Security (EMSEC):** Prevents the release or capture of emanations from equipment, such as cryptographic equipment, thereby preventing unauthorized interception.
3. **Physical Security:** Ensures the safety and prevents unauthorized access to cryptographic information, documents and equipment.
4. **Traffic-Flow Security:** Hides messages and its characteristics while transmitting on a network.
5. **Transmission Security (TRANSEC):** Protects transmissions from unauthorized access, thereby preventing interruption and harm.

Module-1

Principles and Concepts – Data Security

Principles and Concepts – Data Security

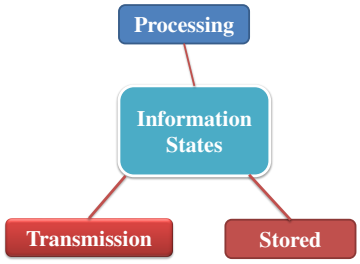
- **Critical Information**
  - Confidentiality
  - Integrity
  - Availability



Principles and Concepts – Data Security

Information States

- Information has three basic states, at any given moment, information is being transmitted, stored or processed.
- Three states exist irrespective of the media in which information resides.



Principles and Concepts – Data Security

Basic information security concepts:

- Identification
- Authentication
- Authorization
- Confidentiality
- Integrity
- Availability
- Non-repudiation

Identification

- **Identification** is the first step in the 'identify-authenticate-authorize' sequence that is performed every day countless times by humans and computers alike when access to information or information processing resources are required.
- While particulars of identification systems differ depending on who or what is being identified, some intrinsic properties of identification apply regardless of these particular.
- Just three of these properties are the ***scope, locality, and uniqueness*** of IDs.

Authentication

- **Authentication** happens right after identification and before authorization.
- It verifies the authenticity of the identity declared at the identification stage.
- At the authentication stage you prove that you are indeed the person or the system you claim to be.
- Three methods of authentication:
  - what you know,
  - what you have and
  - what you are.

Authorization

- **Authorization** is the process of ensuring that a user has sufficient rights to perform the requested operation, and preventing those without sufficient rights from doing the same.
- After declaring identity at the identification stage and proving it at the authentication stage, users are assigned a set of authorizations (also referred to as rights, privileges or permissions) that define what they can do on the system.
- These privileges extremes:
  - "permit nothing"
  - "permit everything" and
  - include anything in between.

Confidentiality

- **Confidentiality** means persons authorized have access to receive or use information, documents etc.
- Unauthorized access to confidential information may have devastating consequences, not only in national security applications, but also in commerce and industry.
- **Mechanisms to assure confidentiality in information systems**
  - Cryptography
  - Access controls

Confidentiality

- Examples of threats to confidentiality:
  - Malware
  - Intruders
  - Social engineering
  - Insecure networks and
  - Poorly administered systems.

Integrity

- **Integrity** is concerned with the trustworthiness, origin, completeness and correctness of information as well as the prevention of improper or unauthorized modification of information.
- Integrity in the information security context refers not only to integrity of information itself but also to the origin integrity i.e. integrity of the source of information.

Integrity

- Integrity protection mechanisms may be grouped into two broad types:
  - **Preventive mechanisms**
    - Access controls prevent unauthorized modification of information
  - **Detective mechanisms**
    - Intended to detect unauthorized modifications when preventive mechanisms have failed

Availability

- **Availability** of information, although usually mentioned last, is not the least important pillar of information security.
- Who needs confidentiality and integrity if the authorized users of information cannot access and use it? Who needs sophisticated encryption and access
- Controls if the information being protected is not accessible to authorized users when they need it?

Availability

- Availability is just as important and as necessary a component of information security as confidentiality and integrity.
- Attacks against availability are known as denial of service (DoS) attacks.
- Natural and manmade disasters obviously may also affect availability as well as confidentiality and integrity of information though their frequency and severity greatly differ.

Non-repudiation

- **Nonrepudiation** is the assurance that someone cannot deny something.
- It refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- In the information security context refers to one of the properties of cryptographic digital signatures that offers the possibility of proving whether a particular message has been digitally signed by the holder of a particular digital signature's private key.

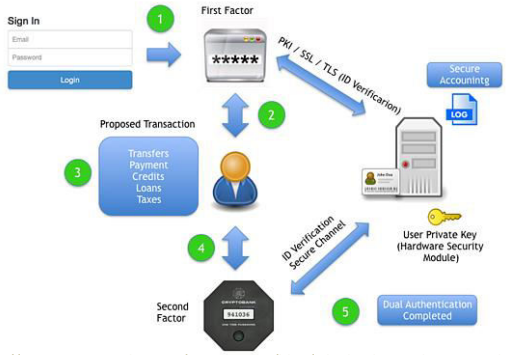
Non-repudiation

- The following types of non-repudiation services are defined in international standard ISO 14516:2002 (guidelines for the use and management of trusted third party services).
  1. **Approval: N**on-repudiation of approval provides proof of who is responsible for approval of the contents of a message.
  2. **Sending: N**on-repudiation of sending provides proof of who sent the message.
  3. **Origin: N**on-repudiation of origin is a combination of approval and sending.
  4. **Submission: N**on-repudiation of submission provides proof that a delivery agent has accepted the message for transmission.

Non-repudiation

- **5. Receipt:** Non-repudiation of receipt provides proof that the recipient received the message.
- **6. Knowledge:** Non-repudiation of knowledge provides proof that the recipient recognized the content of the received message.
- 7. **Delivery:** Non-repudiation of delivery is a combination of receipt and knowledge, as it provides proof that the recipient received and recognized the content of the message.
- **8. Transport:** Non-repudiation of transport provides proof for the message originator that a delivery agent has delivered the message to the intended recipient.

Non-repudiation

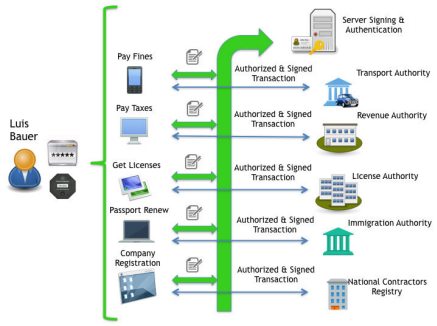


https://www.cryptomathic.com/news-events/blog/why-banks-need-non-repudiation-of-origin-and-non-repudiation-of-emission

NRO and NRE

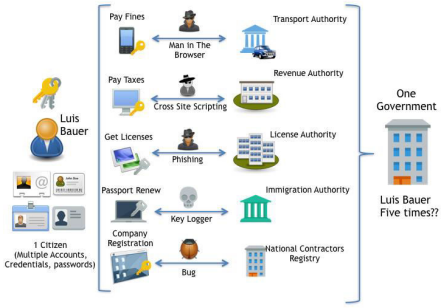
- Non-Repudiation of Origin (NRO) makes a link between the message and the sender of the message. It can provide legal evidence that a person in fact sent the message.
- Non-Repudiation of Emission (NRE) makes a link between the sender of the message and the content of the message. It can provide legal evidence that a person sent that specific message
- From a technical point of view, RFC 4270 (Attacks on Cryptographic Hashes in Internet Protocols) points out that Non-repudiation is “a security service that provides protection against false denial of involvement in a communication”.
- Something You Know, Have, or Are, and then you can sign
  - The knowledge of a unique secret (E.g. password, PIN)
  - Having a unique device that no one else has (E.g. token, card)
  - Being yourself (E.g. fingerprints, DNA)

Threat Scenarios…



https://www.cryptomathic.com/news-events/blog/centralized-authentication-and-signing-for-e-government

Threat Scenarios…



Access control (authorisation) in distributed systems

recall lecture 9 - Introduction to DS: slides 21 to 27
for access control within the overall system architecture:

- as an individual e.g. from home
- within a single administration domain e.g. CL
- using external services from a domain as an individual or group member
- federated domains: inter-domain authorisation

We are concerned with authorisation for service use and/or object access
How is access control policy expressed and enforced?

Authorisation and authentication

Authorisation is built above authentication (proof of identity – proof that you are who you say you are – will someone/something vouch for you?).

Within an administration domain, principals are named and registered as individuals and members of groups.
Principals authenticate in their home domain by means of e.g. passwords.

The aim is to avoid having to have a ***username/password*** for every service.
(.... *How does one remember them all?* .....
....*Use the same one for all? No, break one break all* .....)

A Single Sign On service is needed.

Authentication is covered in Security courses.
For background reading, slides 29-36 outline some single sign on systems for cross-domain service use: Raven, Shibboleth, OpenID

Access control – from first principles

Model: access matrix A (i, j) rows represent principals, columns objects
entry (i, j) contains the rights principal i has to object j

Implementation: since the matrix is sparse (most entries are null)

1. Using access control lists (ACLs): keep non-null entries of column j with object j
   ACL entry = principal name + access rights
   optimisation: group name = list of principals
2. Using capabilities: keep non-null entries of row i with principal i
   a capability (capability list entry) = object name + access rights

Assume managers for the various types of object

On an access request, the manager must check that the requesting principal has the appropriate right to access the object

1. check that the ACL list contains an entry for that principal with the right
2. check that the capability passed by the principal with the request contains the right

ACLs – cf. - capabilities

ACLs

Expressiveness: subtle expression of policy – entries may be for individual principals and groups with individual exceptions.

Revocation: easy to revoke – but ACL changes may not have immediate effect (because the ACL may not be checked on every access once an object is open)

BUT: slow to check - scalability problem
- if expressiveness exploited e.g. negatives and exceptions allowed
- if there are many principals and large groups
- generalisation? multi-domain operation? names outside domain of registration?

AND: awkward to delegate rights e.g. For a file to a printer for a single print job
In a distributed system many services are not part of privileged OSs.

Capabilities

Quick to check – like a ticket – so scale well

Anonymous – knowledge of names not needed – may generalise to multiple domains.
- anonymity may be wanted by some applications for privacy reasons

Problems/issues ... because they are associated with the process rather than the object ...

Capability-based access control - issues

as defined so far, a capability is an object name and some rights

1. protection
   must prevent unauthorised creation, tampering, theft

2. control of propagation
   can principals pass on copies?
   must they ask the object manager? How can this be enforced?

3. delegation
   is an example of propagation
   often with restricted rights for a limited time or action

4. revocation
   - if the access control policy changes, and certain principals should lose their rights, their capabilities should ideally be revoked. Can this be done without revoking all capabilities for the service/object?
   - if a capability is known to have been stolen or tampered with it should be revoked instantly. Will this invalidate all capabilities for this service/object? Anonymity has created revocation problems.

Capabilities in centralised and distributed systems

centralised

Several capability architectures were designed and built e.g. Plessey PP250, CAP
Capabilities can be protected by the hardware and/or the OS
A capability is named via an index into a segment or an OS table.
- held in protected OS space per process
- held in typed capability segments in user space with operations such as
  insert, delete, use-as-argument

distributed

Can't be protected by hardware/OS
Have to be transferred across networks and pass through user space
so must be encryption-protected
Security terminology and implementation:
capability = signed certificate
e.g. X.509 authentication and attribute certificates

Capabilities in distributed systems - design

Must be protected by encryption
The object manager (certificate issuer) keeps a ***SECRET*** (random number, private key) and uses a well-known function ***f***, a one-way function.

A capability is constructed using
check digits = f (SECRET, protected fields)

protected fields	***check digits*** (signature)

When a capability is presented with an operation invocation, the manager checks that:
f (SECRET, protected fields) = check digits
If not, the invocation is rejected.

More generally, the invoked service may not be the capability issuer. The service can check back with the issuer (cf. Certification Authority)

Encryption-protected capabilities – issues?

1. protection
   protect against tampering – adding rights,
   NOT against theft – eavesdropping on the network and replay attacks

2. control of propagation
   still no control over propagation

3. delegation
   object manager must be asked to create a capability with reduced rights to pass to another principal for delegated authority.
   Works indefinitely – duration is not controlled – nor further transfer

4. revocation
   (recall: needed when access control policy changes as well as for stolen capabilities)
   - expiry time as a protected field (like X.509) – crude mechanism
   - hot list of invalid invoking principals per service/object (spoofing? check overhead?)
   - change the SECRET – not selective – all old capabilities will not work and authorised principals will have to request new capabilities.

Principal-specific capabilities

include the name of the principal in the capability for generation and checking as an argument to ***f***, perhaps as a protected field in the capability.

1. protection
   from tampering – YES, from theft – YES: authenticate presenting principal

2. control of propagation
   YES – a capability for the receiving principal can only be created by the object manager

3. delegation
   YES – a capability for the receiving principal must be created by the object manager

4. revocation
   can be more selective – still involves overhead of checking hot list
   e.g. revocation list of principals excluded by policy change
   stolen capabilities should be detected on authenticating the presenting principal unless the presenter is successfully masquerading as the owner.

All the above raise the question of the structure and scope of principal names and how and where principals are authenticated.

ACLs in distributed systems

We first followed the capability thread after slide 11.
We have discussed principal-specific capabilities
Now, return to consider ACLs.
ACLs comprise lists of principals (or groups)
ACL entry = principal (or group) name, rights (from slide 3)
Where principals and groups are defined and registered within some administration domain.

Without group names ACLs may become unmanageable, long lists of principals.
Within the administration domain where a group and its constituent principals are registered, a group name can be expanded into a list of principals, for checking.

How can group names be used outside the domain where the group is registered?

We generalise groups to roles and consider role-based access control (RBAC)

Role-based access control (RBAC)

Services may classify their clients into named roles e.g.
login service: ***logged-in-user*** (after authentication)
patient monitoring service: ***surgeon, doctor, nurse, patient***
online exam service: ***candidate, examiner, chief examiner***
digital library service: ***reader, librarian, administrator***

Access rights (privileges) are assigned to roles for use of services (method invocation) or more fine-grained access to individual objects or broad categories of object managed by a service

Scope of role names may be the local domain of the service, or some role names may be organisation-wide, across federated domains
e.g. ***sales-manager*** used in all branches of a world-wide company
police-sergeant used in all of the 52 UK county police forces
NHS-doctor used throughout the UK NHS

RBAC - 2

Administration: note the separation:
principals –> ***roles***, ***roles*** –> ***privileges***

Service developers need only specify authorisation in terms of roles, independently of the administration of principals
e.g. annual student cohort, staff leaving and joining

Principals are authenticated, as always, and must also prove their right to acquire/activate a role. They thus prove they are authorised to use a service

Compare with ACLs – like ACLs containing only group names.
Compare with capabilities – can a capability that proves role membership be engineered?
RBAC seems promising for fast authorisation checking.

RBAC – 3: Parametrised roles

Roles may be parametrised for fine-grained access control to capture:
- relationships between principals:
Policy: "*only the doctor treating a patient may access the medical record*"
e.g. ***treating-doctor (hospital-ID, doctor-ID, patient-ID)***

- patients and others may express exclusions as authorisation policy
e.g. ***doctor (doctor-ID)***
Policy: "*where doctor is not Shipman*", "*where doctor is not <x> (a relative)*"

Compare with ACLs containing only groups, with exclusions of individual members – semantics of precedence of evaluation in ACLs has always been a difficult area.

RBAC – 4: Role hierarchies

Some RBAC systems define role hierarchies with privilege inheritance up the hierarchy.
The hierarchy may mirror organisational structure, which reflects power and responsibility rather than functional competence.
Privilege inheritance is even less defensible for functional roles.

Also: privilege inheritance violates the *principle of minimum necessary privilege* and makes reasoning about privileges difficult
– see many ACM SACMAT papers)

Role hierarchies are defined in the later NIST RBAC standards.

Our work has avoided privilege inheritance (see OASIS case study).

RBAC – 5: Inter-domain authorisation

RBAC eases authorisation outside principals' home domains, because:

- Roles change less frequently than principals leave and join them
- Administration of users and role membership is separate from service development and use.
- Negotiation on use of services external to domains can be in terms of roles, e.g. payment for a role to use a service
- Federated domains may contain agreed role names in each domain.
  Makes policy easier to negotiate and express.
  e.g. ***sales-department-staff, sales-manager, salesman***

RBAC – 6: Authorisation context

Authorisation policy could include other constraints on use of a role
e.g. time of day, as well as relationships and exclusions.
see OASIS case study – environmental constraints

The privileges associated with a role might not be static.
e.g. ***student (course-ID, student-ID)*** may read solutions to exercises only after marked work has been returned.

e.g. Conference management system – a small-scale example follows of use of an external service from a number of domains.

Example: conference management (e.g. Easychair, CMT, EDAS, ...) selection from workflow and policy

Program chair registers names, email addresses, initial password, and roles of the programme committee: roles ***PC-chair(s), PC-member***
all are sent an email asking them to register their account, change their password

Authors submit papers, acquiring role ***contact-author***, returned a UID for the paper
contact-author may submit new versions up to the deadline
PC-members are assigned papers to review. They may delegate some reviews:
role ***reviewer*** per paper, separate from ***PC-member***
Conflicts of interest must be expressed by submitting-authors and PC members, and enforced by the system
PC members must never be able to know the reviewers and see the reviews of their own papers
PC members can see only their own reviews until after the review deadline.
After this, in a discussion phase, PC members may be able to see the ranked order and other reviews (except for their own papers). Systems vary in this respect.
Note: small scale example e.g. 50 PC members, 200 papers
Note: rights will change after deadlines (an example of context)

Design of capabilities/certificates can incorporate RBAC

Traditional capabilities in centralised systems:

object-ID	***rights***

proves the presenter has the rights to the object

RBAC

role	***parameters***

proves the presenter holds the role + parameters must be checked against access control policy

Capabilities/certificates in distributed systems
check digits = *f* (SECRET, protected fields)

protected fields (***object-ID, rights***)	***check digits*** (signature)

RBAC in distributed systems
check digits = *f* (SECRET, protected fields)

protected fields (***role, parameters***)	***check digits*** (signature)

RBAC - discussion

RBAC provides:

1. Expressiveness
   - subtle expression of access control policy.
   - if roles are parametrised, exclusions and relationships can be captured.
   - environmental/context checks (time/place) can also be included.

2. Efficiency
   - checking faster than ACLs
   - use of certificate technology comparable with capabilities
   - or use a secure channel and role authentication in source domain

3 Cross-domain interworking
   - easy to negotiate
   - authorisation policy expressible and enforceable
   - heterogeneity of certificates – can check back with issuing domain

OASIS RBAC

Open Architecture for Securely Interworking Services
Case study from Opera Group research

- OASIS services name their clients in terms of **roles**
- OASIS services specify **policy** in terms of **roles**
  - for **role entry** (activation)
  - for **service invocation** (authorisation, access control)

  both in Horn clause form

see: *www.cl.cam.ac.uk/Research/SRG/opera*
for people, projects, publications for download

OASIS model of **role activation**

a role activation rule is of the form:

condition1, condition2, ….. |- target role

where the conditions can be

- prerequisite role
- appointment credential
- environmental constraint

all are parametrised

OASIS (continued) **membership** rules

as we have seen, a role activation rule:

cond1*, cond2, cond3*, ….. |- target role

role membership rule:

the role activation conditions that must **remain true**, e.g.*
for the principal to remain active in the role

monitored using **event-based middleware**
another contributor to an **active security environment**

OASIS model of **authorisation**

An authorisation rule is of the form:

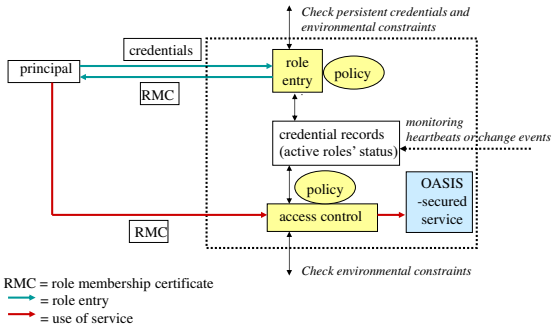
condition1, condition2, ….. |- access

where the conditions can be

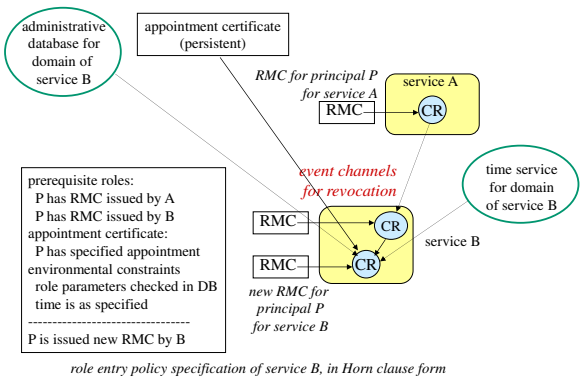
- an active role
- an environmental constraint

all are parametrised

A Service Secured by OASIS Access Control

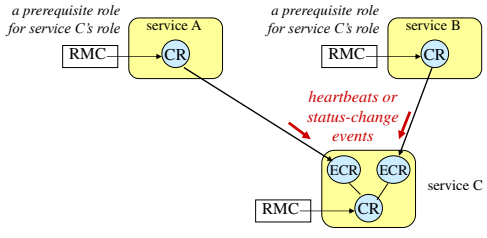


OASIS role activation illustrated



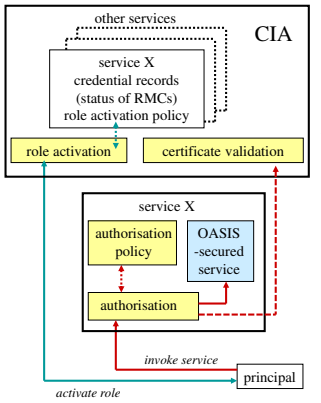
role entry policy specification of service B, in Horn clause form
conditions for principal P to activate some role

Active Security Environment
Monitoring membership rules of active roles



RMC = role membership certificate
CR = credential record
ECR = external credential record

Engineering per-domain certificate issuing and authentication



It is not realistic for every service to manage secrets and issue certificates

The CIA service, for services in its domain:
- keeps the activation polices
- activates roles
- issues and validates certificates
- maintains credential record structures for active roles
-handles revocation via event channels

The CIA service, for services in other domains:
-validates certificates it has issued
- handles revocation of its certificates

OASIS philosophy and characteristics

- Distributed architecture, not a single organisation. Incremental deployment of independently developed services in independent administration domains.
- RBAC for scalability, parametrised roles for expressiveness of policy (e.g. exclusion of values, relationships between parameters).
- Policy expression is per service, per domain
- Roles are activated within sessions. Persistent credentials may be required for role activation.
- Independent designs of RMCs may coexist – service at which RMC is presented checks back with issuer for RMC validation
- Service (domain) level agreements on use of others' RMCs
- Anonymity if and when required
- Immediate revocation on an individual basis
- No role hierarchies with inheritance of privileges

Background on cross-domain authentication

(From slide 2) – here is an outline of some single sign on systems

Raven for use of websites across all the domains of Cambridge University
- common naming of principals (CRSIDs, nested domains)
- authentication is sufficient for authorisation

Shibboleth organisation-centric.
organisation negotiates use by its members of external services

OpenID user-centric
used by many large websites (BBC, Google, MySpace, PayPal, ...)

Raven

- Aim: avoid proliferation of passwords for UCam web services
  - Raven is a Ucam-webauth Single Sign On system instance
  - Developed within Cambridge (by Jon Warbrick)
- Three parties in the Ucam_webauth protocol:
  - User's web-browser
  - Target web-server
  - Raven web-server
- Authentication token passed as an HTTP cookie
  - Thus should be passed using HTTPS… but often isn't

Example Raven dialogue

- User requests protected page
- Target web-server checks for Ucam-WLS-Session cookie
- If found, and decodes correctly, page is returned. Done.

- Otherwise, redirect client browser to Raven server
  - Encodes information about the requested page in the URL
- Raven inputs and checks credentials
  - (Also permits users to "cancel")
- Raven redirects client browser to the protected page. Done.
  - (An HTTP 401 error will be generated if users cancelled)

Raven coordinates participants using time

- Target web-server verifies Ucam-WLS-Session cookie
  - Public-key of Raven server pre-loaded on target web-server
- Target web-server and Raven do not interact directly
  - Client browser receives, stores and resends cookies
- What about malicious client behaviour or interception?
  - e.g. replay attacks?
- Raven requires time-synchronisation
  - A site-specific clock-skew margin can be configured

Shibboleth provides federated authentication

- System for federated authentication and authorisation
  - Internet2 middleware group standard
  - Implements SAML: Security Assertion Markup Language
  - Facilitates single-sign-on across administrative domains
- Raven actually speaks both Ucam-webauth and Shibboleth
  - Shibboleth has the advantage of wider software support
- Identity providers (IdPs) supply user information
- Service providers (SPs) consume this information and get access to secure content

Shibboleth exchange

- Similar to Raven, but with some extra indirection
  - User requests protected resource from SP
  - SP crafts authentication request
  - User redirected to IdP or 'Where Are You From' service
    - E.g. UK Federation WAYF service
  - User authenticates (external to Shibboleth)
  - Shibboleth generates SAML authentication assertion handle
  - User redirected to SP
  - SP may issue AttributeQuery to IdP's attribute service
  - SP can make access control decision

OpenID

- Another cross-domain single-sign-on system
- Shibboleth is organisation-centric
  - Organisations must agree to accept other organisations' statements regarding foreign users
  - Lots of support within the UK Joint Information Systems Committee (JISC) for accessing electronic resources
- OpenID is user-centric
  - Primarily about identity
  - OpenIDs are permanent URI or XRI structures

OpenID (cont)

- User provides their ID to relying party web site
  - OpenID 1.0 retrieves URL, learns identity provider
  - OpenID 2.0 retrieves XRDS, learns identity provider
    - XRDS/Yadis indirection affords greater flexibility
- Many big commercial players offer OpenID assertions
- Lots of open source software support for OpenID also
- In terms of responsibility, consider use for:
  - Access to a web resource
  - Access to a wireless network

Access Control

Access Control

- Access control is a method of limiting access to a system or to physical or virtual resources.
- It is a process by which users can access and are granted certain prerogative to systems, resources or information.
- Access control is a security technique that has control over who can view different aspects, what can be viewed and who can use resources in a computing environment.
- It is a fundamental concept in security that reduces risk to the business or organization.
- To establish a secure system, electronic access control systems are used that depend on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and areas.
- These systems include access control panels to prohibit entry to sensitive areas like alarms and lock down areas to prevent unauthorized access or operations.

Access Control

- Access control systems perform identification, authentication, and authorization of users and entities by evaluating required login credentials that may include passwords, pins, bio-metric scans or other authentication factors.
- There is multi-factor authentication which requires two or more authentication factors which is often an important part of the layered defense to protect access control systems.
- Authentication Factors:
  - Password or PIN
  - Bio-metric measurement (fingerprint & ratina scan)
  - Card or Key

Access Control

- Different access control models are used depending on the compliance requirements and the security levels of information technology that is to be protected.
- Basically access control is of 2 types:
  - Physical Access Control: Physical access control restricts entry to campuses, buildings, rooms and physical IT assets.
  - Logical Access Control: Logical access control limits connections to computer networks, system files and data.

Access Control Model

- Attribute-based Access Control (ABAC):
  - Access is granted or declined by evaluating a set of rules, policies, and relationships using the attributes of users, systems and environmental conditions.
- Discretionary Access Control (DAC):
  - The owner of data determines who can access specific resources.
- History-Based Access Control (HBAC):
  - Access is granted or declined by evaluating the history of activities of the inquiring party that includes behavior, the time between requests and content of requests.
- Identity-Based Access Control (IBAC):
  - By using this model network administrators can more effectively manage activity and access based on individual requirements.

https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria

Access Control Model

- Mandatory Access Control (MAC):
  - A control model in which access rights are regulated by a central authority based on multiple levels of security. Security Enhanced Linux is implemented using MAC on the Linux operating system.
- Organization-Based Access control (OrBAC):
  - This model allows the policy designer to define a security policy independent of the implementation.
- Role-Based Access Control (RBAC):
  - RBAC allows access based on the job title. RBAC eliminates discretion on a large scale when providing access to objects. For example, there should not be permissions for human resources specialist to create network accounts.
- Rule-Based Access Control (RAC):
  - RAC method is largely context based. Example of this would be only allowing students to use the labs during a certain time of day.

Attribute-based Access Control

- ABAC comes with a recommended architecture which is as follows:
  - The PEP or Policy Enforcement Point: it is responsible for protecting the apps & data you want to apply ABAC to. The PEP inspects the request and generates an authorization request from it which it sends to the PDP.
  - The PDP or Policy Decision Point is the brain of the architecture. This is the piece which evaluates incoming requests against policies it has been configured with. The PDP returns a Permit / Deny decision. The PDP may also use PIPs to retrieve missing metadata
  - The PIP or Policy Information Point bridges the PDP to external sources of attributes e.g. LDAP or databases.

Attribute-based Access Control

- Attributes tend to fall into 4 different categories:
  - Subject attributes: attributes that describe the user attempting the access e.g. age, clearance, department, role, job title...
  - Action attributes: attributes that describe the action being attempted e.g. read, delete, view, approve...
  - Object attributes: attributes that describe the object (or resource) being accessed e.g. the object type (medical record, bank account...), the department, the classification or sensitivity, the location...
  - Contextual (environment) attributes: attributes that deal with time, location or dynamic aspects of the access control scenario

Attribute-based Access Control

- Policies
  - Policies are statements that bring together attributes to express what can happen and is not allowed.
  - Policies in ABAC can be granting or denying policies.
  - Policies can also be local or global and can be written in a way that they override other policies.
  - Examples include:
    - A user can view a document if the document is in the same department as the user
    - A user can edit a document if they are the owner and if the document is in draft mode
    - Deny access before 9am
    - With ABAC you can have as many policies as you like that cater to many different scenarios and technologies.

Role-Based Access Control

When defining an RBAC model, the following conventions are useful:

- S = Subject = A person or automated agent
- R = Role = Job function or title which defines an authority level
- P = Permissions = An approval of a mode of access to a resource
- SE = Session = A mapping involving S, R and/or P
- SA = Subject Assignment
- PA = Permission Assignment
- RH = Partially ordered Role Hierarchy. RH can also be written: ≥ (The notation: x ≥ y means that x inherits the permissions of y.)
  - A subject can have multiple roles.
  - A role can have multiple subjects.
  - A role can have many permissions.
  - A permission can be assigned to many roles.
  - An operation can be assigned to many permissions.
  - A permission can be assigned to many operations.

A constraint places a restrictive rule on the potential inheritance of permissions from opposing roles, thus it can be used to achieve appropriate separation of duties. For example, the same person should not be allowed to both create a login account and to authorize the account creation.

Thus, using set theory notation:

- $PA \subseteq P \times R$ and is a many to many permission to role assignment relation.
- $SA \subseteq S \times R$ and is a many to many subject to role assignment relation.
- $RH \subseteq R \times R$

A subject may have *multiple* simultaneous sessions with/in different roles.

References

- http://web.archive.org/web/20160429011917/http://www.cgisecurity.com/owasp/html/ch08s02.html
- https://en.wikipedia.org/wiki/Role-based_access_control
- https://en.wikipedia.org/wiki/Attribute-based_access_control
- https://en.wikipedia.org/wiki/Organisation-based_access_control
- https://en.wikipedia.org/wiki/Discretionary_access_control
- https://en.wikipedia.org/wiki/Mandatory_access_control
- https://en.wikipedia.org/wiki/Graph-based_access_control

Module-1

Fundamentals: Information Security and Threats

Types of Security Attacks

- Virus
- Worm
- Trojan

Virus

- Virus is a malicious program able to inject its code into other programs/ applications or data files and the targeted areas become "infected".
- Installation of a virus is done without user's consent, and spreads in form of executable code transferred from one host to another.

Types of viruses

- Resident virus;
- Non-resident virus;
- Boot sector virus;
- Macro virus;
- File-infecting virus (file-infector);
- Polymorphic virus;
- Metamorphic virus;
- Stealth virus;
- Companion virus
- Cavity virus.

Worm

- Worm is a malicious program category, exploiting operating system vulnerabilities to spread itself.
- In its design, worm is quite similar to a virus - considered even its sub-class.
- Unlike the viruses though worms can reproduce/ duplicate and spread by itself.

Types of Worms

Email worms:

- spread through email messages, especially through those with attachments.

Internet worms:

- spread directly over the internet by exploiting access to open ports or system vulnerabilities**.**

Network worms:

- spread over open and unprotected network shares.

Multi-vector worms:

- having two or more various spread capabilities.

Trojan

- Trojans are a type of malware software that masquerades itself as a not-malicious even useful application but it will actually do damage to the host computer after its installation.
- Unlike virus, Trojans do not self-replicate unless end user intervene to install.

Types of Trojan

- Remote Access Trojans (RAT) aka Backdoor Trojan
- Trojan-DDoS
- Trojan-Proxy
- Trojan-FTP
- Destructive Trojan
- Security Software Disabler Trojan
- Info Stealer (Data Sending/ Stealing Trojan)
- Keylogger Trojan
- Trojan-PSW (Password Stealer)
- Trojan-Banker
- Trojan-IM,.. etc..

Other security threats

Malware

- Malware refers to software viruses, spyware, adware, worms, Trojans, ransomeware etc.
- They are designed to cause damage to a targeted computer or cause a certain degree of operational disruption.

Rootkit

- Rootkit are malicious software designed to hide certain processes or programs from detection.
- Usually acquires and maintains privileged system access while hiding its presence in the same time. It acts as a conduit by providing the attacker with a backdoor to a system

Other security threats

Spyware

- Spyware is a software that monitors and collects information about a particular user, computer or organization without user's knowledge.

Riskware

- Riskware is a term used to describe potentially dangerous software whose installation may pose a risk to the computer.

Other security threats

Adware

- Adware in general term adware is software generating or displaying certain advertisements to the user.
- This kind of adware is very common for freeware and shareware software and can analyze end user internet habits and then tailor the advertisements directly to users' interests.

Other security threats

Creepware

• Creepware is a term used to describe activities like spying others through webcams (very often combined with capturing pictures), tracking online activities of others and listening to conversation over the computer's microphone and stealing passwords and other data.

Blended threat

- Blended threat defines an exploit that combines elements of multiple types of malware components.
- Usage of multiple attack vectors and payload types targets to increase the severity of the damage causes and as well the speed of spreading.

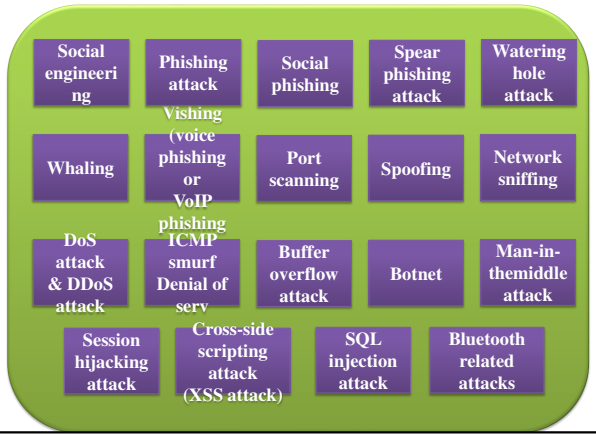
NETWORK ATTACKS

- Network attack is usually defined as an intrusion on the network infrastructure that will first analyze the environment and collect information in order to exploit the existing open ports or vulnerabilities.
- This may include unauthorized access to organization resources.

NETWORK ATTACKS

- **Outside attack:**
  - when attack is performed from outside of the organization by unauthorized entity it is said to be an outside attack.
- **Inside attack:**
  - if an attack is performed from within the company by an "insider" that already has certain access to the network it is considered to be an inside attack.
- **Others**
  - such as end users targeted attacks (like phishing or social engineering): these attacks are not directly referred to as network attacks, but are important to know due to their widespread occurrences.

What types of attack are there?



Spoofing

It is a technique used to masquerade a person, program or an address as another by falsifying the data with purpose of unauthorized

- **IP Address spoofing**

  – process of creating IP packets with forged source IP address to impersonate legitimate system. This kind of spoofing is often used in DoS attacks (Smurf Attack).

- **ARP spoofing (ARP Poisoning)**

  – process of sending fake ARP messages in the network. The purpose of this spoofing is to associate the MAC address with the IP address of another legitimate host causing traffic redirection to the attacker host. This kind of spoofing is often used in man-in-the-middle attacks.

Spoofing

- **DNS spoofing (DNS Cache Poisoning)**

  – an attack where the wrong data is inserted into DNS Server cache, causing the DNS server to divert the traffic by returning wrong IP addresses as results for client queries.

- **Email spoofing**

  – a process of faking the email's sender "from" field in order to hide real origin of the email. This type of spoofing is often used in spam mail or during phishing attack.

- **Search engine poisoning**

  – attackers take advantage of high profile news items or popular events that may be of specific interest for certain group of people to spread malware and viruses.

Network Sniffing (Packet Sniffing)

- A process of capturing the data packets travelling in the network.This may include unauthorized access to organization resources.

Denial of Service Attack (DoS Attack) and Distributed Denial of Service Attack (DDoS Attack

- An attack designed to cause an interruption or suspension of services of a specific host/ server by flooding it with large quantities of useless traffic or external communication requests.
- When the DoS attack succeeds the server is not able to answer even to legitimate requests anymore, this can be observed in numbers of ways – slow response of the server, slow network performance, unavailability of software or web page, inability to access data, website or other resources.
- Distributed Denial of Service Attack (DDoS) occurs where multiple compromised or infected systems (botnet) flood a particular host with

DoS attack types:

- ICMP flood attack (Ping Flood)
- Ping of Death (PoD)
- Smurf attack
- ICMP Smurf Denial of Service SYN flood attack
- Buffer overflow attack
- Botnet
- Man-in-the-middle attack
- Session hijacking attack
- Cross-side scripting attack (XSS attack)
- SQL injection attack.

Bluetooth related attacks

- Bluesnarfing
- Bluejacking
- Bluebugging

Module-1

Types of Controls in Information Security

Controls in Information Security

- Once an organization defines control objectives, it can assess the risk to individual assets and then choose the most appropriate security controls to put in place.

Control Types

- Physical controls
- Technical controls
- Administrative controls

Control Types

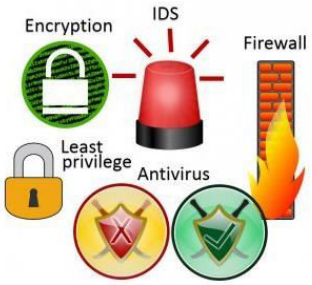
- Physical controls

Control Types

- Physical controls
  - It describe anything tangible that's used to prevent or detect unauthorized access to physical areas, systems, or assets.
  - This includes things like fences, gates, guards, security badges and access cards, biometric access controls, security lighting, CCTVs, surveillance cameras, motion sensors, fire suppression, as well as environmental controls like HVAC and humidity controls.

Control Types

- Technical controls



Control Types

- Technical controls
  - (also known as logical controls) include hardware or software mechanisms used to protect assets.
  - Some common examples are authentication solutions, firewalls, antivirus software, intrusion detection systems (IDSs), intrusion protection systems (IPSs), constrained interfaces, as well as access control lists (ACLs) and encryption measures.

Control Types

- Administrative controls

Control Types

- Administrative controls
  - It refer to policies, procedures, or guidelines that define personnel or business practices in accordance with the organization's security goals.
  - These can apply to employee hiring and termination, equipment and Internet usage, physical access to facilities, separation of duties, data classification, and auditing.
  - Security awareness training for employees also falls under the umbrella of administrative controls.

Security Control Functions

- Preventative controls
- Detective controls
- Corrective controls
- Recovery controls
- Compensation controls

Security Control Functions

- Preventative controls
  - It describe any security measure that's designed to stop unwanted or unauthorized activity from occurring.
  - Examples include physical controls such as fences, locks, and alarm systems;
  - technical controls such as antivirus software, firewalls, and IPSs; and
  - administrative controls like separation of duties, data classification, and auditing.

Security Control Functions

- Detective controls
  - It describe any security measure taken or solution that's implemented to detect and alert to unwanted or unauthorized activity in progress or after it has occurred.
  - Physical examples include alarms or notifications from physical sensor (door alarms, fire alarms) that alert guards, police, or system administrators.
  - Honeypots and IDSs are examples of technical detective controls.

Security Control Functions

- Corrective controls
  - It include any measures taken to repair damage or restore resources and capabilities to their prior state following an unauthorized or unwanted activity.
  - Examples of technical corrective controls include patching a system, quarantining a virus, terminating a process, or rebooting a system.
  - Putting an incident response plan into action is an example of an administrative corrective control.

Security Control Functions

- Recovery controls
  - Recovery controls are somewhat like corrective controls, but they are applied in more serious situations to recover from security violations and restore information and information processing resources.
  - Recovery controls may include,
    - disaster recovery and business continuity mechanisms
    - backup systems and data
    - emergency key management arrangements and similar controls.

Security Control Functions

- Compensation controls
  - Compensating controls are intended to be alternative arrangements for other controls when the original controls have failed or cannot be used.
    - When a second set of controls addresses the same threats that are addressed by another set of controls, it acts as a compensating control.

Access Control Models

- The term 'access control' refers to "the control of access to system resources after a user's account credentials and identity have been authenticated and access to the system has been granted".

Access Control Models

- Access control is used to identify a subject (user/human) and to authorize the subject to access an object (data/resource) based on the required task.
- These controls are used to protect resources from unauthorized access and are put into place to ensure that subjects can only access objects using secure and pre-approved methods.

Access Control Models

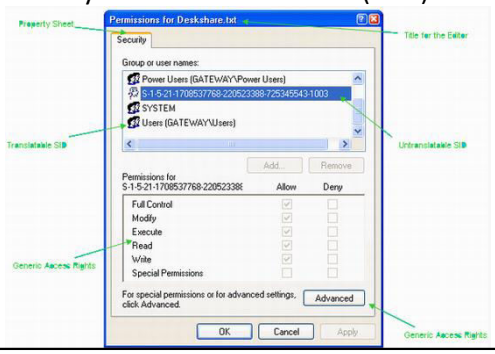
- Logical access control models are the abstract foundations upon which actual access control mechanisms and systems are built.
- Access control is among the most important concepts in computer security.
- Access control models define how computers enforce access of subjects (such as users, other Computers, applications and so on) to objects (such as computers, files, directories, applications, servers and devices).

Access Control Models

- Discretionary Access Control Model
- Mandatory Access Control Model
- Role based Access Control Model

Access Control Models

- Discretionary Access Control Model(DAC)



Access Control Models

- Discretionary Access Control(DAC)
  - DAC is a type of access control system that assigns access rights based on rules specified by users. The principle behind DAC is that subjects can determine who has access to their objects.

Access Control Models

- Mandatory Access Control Model(MAC)
  - The design and implementation of MAC is commonly used by the government. It uses a hierarchical approach to control access to files/resources. Under a MAC environment, access to resource objects is controlled by the settings defined by a system administrator.

Access Control Models

- Mandatory Access Control Model(MAC)
  - This means access to resource objects is controlled by the operating system based on what the system administrator configured in the settings. It is not possible for users to change access control of a resource.

Access Control Models

- Mandatory Access Control Model(MAC)
  - Each user account is also assigned classification and category properties.
  - This system provides users access to an object if both properties match. If a user has high classification but is not part of the category of the object, then the user cannot access the object.

Access Control Models

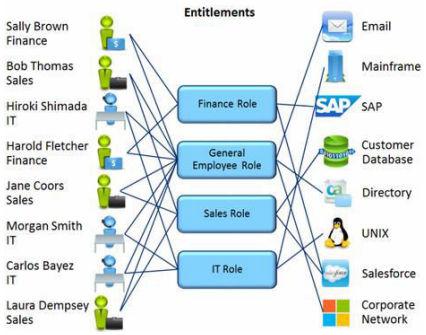
- Mandatory Access Control Model(MAC)

Access Control Models

- Role-Based Access Control (RBAC)
  - RBAC, also known as a non-discretionary access control, is used when system administrators need to assign rights based on organizational roles instead of individual user accounts within an organization.
  - It presents an opportunity for the organization to address the principle of 'least privilege'. This gives an individual only the access needed to do their job, since access is connected to their job.

Access Control Models

- Role-Based Access Control (RBAC)



Module-1

Security Policies

- An information security policy (ISP) is a set of rules, policies and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements.

Security Policies

- What is the purpose of an information security policy?
  - An information security policy aims to enact protections and limit the distribution of data to only those with authorized access.
  - Organizations create ISPs to:
    - Establish a general approach to information security
    - Document security measures and user access control policies
    - Detect and minimize the impact of compromised information assets such as misuse of data, networks, mobile devices, computers and applications
    - Protect the reputation of the organization

Security Policies

- What is the purpose of an information security policy?
  - An information security policy aims to enact protections and limit the distribution of data to only those with authorized access.
  - Organizations create ISPs to:
    - Comply with legal and regulatory requirements like NIST, GDPR, HIPAA and FERPA
    - Protect their customer's data, such as credit card numbers
    - Provide effective mechanisms to respond to complaints and queries related to real or perceived cyber security risks such as phishing, malware and ransomware
    - Limit access to key information technology assets to those who have an acceptable use

Security Policies

- Why is an information security policy is important?
  - Creating an effective information security policy and that meets all compliance requirements is a critical step in preventing security incidents like data leaks and data breaches.
  - ISPs are important for new and established organizations.
  - Increasing digitalization means every employee is generating data and a portion of that data must be protected from unauthorized access.
  - Depending on your industry, it may even be protected by laws and regulations.

Security Policies

- Why is an information security policy is important?
  - Sensitive data, personally identifiable information (PII), and intellectual property must be protected to a higher standard than other data.
  - Whether you like it or not, information security (InfoSec) is important at every level of your organization and outside of your organization.
  - Increased outsourcing means third-party vendors have access to data too.
  - Third-party risk management and vendor risk management is part of any good ISP.
  - Third-party risk, fourth-party risk and vendor risk are equally important.

Security Policies

- What are the key elements of an information security policy?
  1. Purpose
  2. Audience
  3. Information security objectives
  4. Authority and access control policy
  5. Data classification
  6. Data support and operations
  7. Security awareness training
  8. Responsibilities and duties of employees

Security Policies

- What are the key elements of an information security policy?
  - 1. Purpose
    - Preserve your organization's information security.
    - Detect and preempt information security breaches caused by third-party vendors, misuse of networks, data, applications, computer systems and mobile devices.
    - Protect the organization's reputation
    - Uphold ethical, legal and regulatory requirements
    - Protect customer data and respond to inquiries and complaints about non-compliance of security requirements and data protection.

Security Policies

- What are the key elements of an information security policy?
  - 2. Audience
    - Define who the information security policy applies to and who it does not apply to.
    - You may be tempted to say that third-party vendors are not included as part of your information security policy.

Security Policies

- What are the key elements of an information security policy?
  - 3. Information security objectives
    - **Confidentiality:** data and information are protected from unauthorized access
    - **Integrity:** Data is intact, complete and accurate
    - **Availability:** IT systems are available when needed

Security Policies

- What are the key elements of an information security policy?
  - 4. Authority and access control policy
    - This part is about deciding who has the authority to decide what data can be shared and what can't.
    - Remember, this may not be always up to your organization.
    - For example, if you are the CSO at a hospital. You likely need to comply with HIPAA and its data protection requirements. If you store medical records, they can't be shared with an unauthorized party whether in person or online.

Security Policies

- What are the key elements of an information security policy?
  - 5. Data classification
    - An information security policy must classify data into categories. A good way to classify the data is into five levels that dictate an increasing need for protection:
      - **Level 1:** Public information
      - **Level 2:** Information your organization has chosen to keep confidential but disclosure would not cause material harm
      - **Level 3:** Information has a risk of material harm to individuals or your organization if disclosed
      - **Level 4:** Information has a high risk of causing serious harm to individuals or your organization if disclosed
      - **Level 5:** Information will cause severe harm to individuals or your organization if disclosed

Security Policies

- What are the key elements of an information security policy?
  - 6. Data support and operations
    - Once data has been classified, you need to outline how data is each level will be handled.
    - There are generally three components to this part of your information security policy:
      - **Data protection regulations:**
        - » Organizations that store personally identifiable information (PII) or sensitive data must be protected according to organizational standards, best practices, industry compliance standards and regulation
      - **Data backup requirements:**
        - » Outlines how data is backed up, what level of encryption is used and what third-party service providers are used
      - **Movement of data:**
        - » Outlines how data is communicated. Data that is deemed classified in the above data classification should be securely communicated with encryption and not transmitted across public networks to avoid man-in-the-middle attacks

Security Policies

- What are the key elements of an information security policy?
  - 7. Security awareness training
    - Security training should include:
      - **Social engineering:**
        - » Teach your employees about phishing, spearphishing and other common social engineering cyber attacks
      - **Clean desk policy:**
        - » Laptops should be taken home and documents shouldn't be left on desks at the end of the work day
      - **Acceptable usage:**
        - » What can employees use their work devices and Internet for and what is restricted?

Security Policies

- What are the key elements of an information security policy?
  - 8. Responsibilities and duties of employees
    - This is where you operationalize your information security policy. This part of your information security policy needs to outline the owners of:
      - Security programs
      - Acceptable use policies
      - Network security
      - Physical security
      - Business continuity
      - Access management
      - Security awareness
      - Risk assessments
      - Incident response
      - Data security
      - Disaster recovery
      - Incident management

Basic Terminologies in Cryptography

- Plaintext
- Ciphertext
- Encryption
- Decryption
- Keys
- Hash
- Salt
- Symmetric and Asymmetric Algorithms
- Public and Private Keys
- HTTPS
- End-to-End Encryption

Basic Terminologies in Cryptography

- Plaintext
  - which is simple but just as important as the others: **plaintext** is an unencrypted, readable, plain message that anyone can read.

Basic Terminologies in Cryptography

- **Ciphertext**
  - **Ciphertext** is the result of the encryption process.
  - The encrypted plaintext appears as apparently random strings of characters, rendering them useless.
  - A cipher is another way of referring to the encryption algorithm that transforms the plaintext, hence the term ciphertext.

Basic Terminologies in Cryptography

- **Encryption**
  - **Encryption** is the process of applying a mathematical function to a file that renders its contents unreadable and inaccessible---unless you have the decryption key.
  - For instance, let's say you have a Microsoft Word document.
  - You apply a password using Microsoft Office's inbuilt encryption function.
  - The file is now unreadable and inaccessible to anyone without the password. You can even encrypt your entire hard drive for security.

Basic Terminologies in Cryptography

- **Decryption**
  - If encryption locks the file, then decryption reverses the process, turning ciphertext back to plaintext.
  - **Decryption** requires two elements: the correct password and the corresponding decryption algorithm.

Basic Terminologies in Cryptography

- **Keys**
  - The encryption process requires a **cryptographic key** that tells the algorithm how to transform the plaintext into ciphertext.
  - **Kerckhoffs's principle** states that "only secrecy of the key provides security," while Shannon's maxim continues "the enemy knows the system."

Basic Terminologies in Cryptography

- **Keys**
  - These two statements influence the role of encryption, and keys within that.
  - Keeping the details of an entire encryption algorithm secret is extremely difficult; keeping a much smaller key secret is easier.
  - The key locks and unlocks the algorithm, allowing the encryption or decryption process to function.

Basic Terminologies in Cryptography

- **Keys**
  - **Is a Key a Password?**
    - No. Well, at least not entirely. Key creation is a result of using an algorithm, whereas a password is usually a user choice.
    - The confusion arises as we rarely specifically interact with a cryptographic key, whereas passwords are part of daily life.
    - Passwords are at times part of the key creation process. A user enters their super-strong password using all manner of characters and symbols, and the algorithm generates a key using their input.

Basic Terminologies in Cryptography

- **Hash**
  - When a website encrypts your password, it uses an encryption algorithm to convert your plaintext password to a hash.
  - A **hash** is different from encryption in that once the data is hashed, it cannot be unhashed. Or rather, it is extremely difficult.
  - Hashing is really useful when you need to verify something's authenticity, but not have it read back. In this, password hashing offers some protection against **brute-force attacks** (where the attacker tries every possible password combination).

Basic Terminologies in Cryptography

- **Hash**
  - You might have even heard of some of the common hashing algorithms, **such as MD5, SHA, SHA-1, and SHA-2**. Some are stronger than others, while some, such as MD5, are outright vulnerable.
  - For instance, if you head to the site **MD5 Online**, you'll note they have 123,255,542,234 words in their MD5 hash database.

Basic Terminologies in Cryptography

- **Salt**
  - When passwords are part of key creation, the encryption process requires additional security steps.
  - One of those steps is **salting** the passwords.
  - At a basic level, a salt adds random data to a one-way hash function.

Basic Terminologies in Cryptography

- **Salt**
  - There are two users with the exact same password: **hunter2**.
  - We run **hunter2** through an SHA256 hash generator and receive f52fbd32b2b3b86ff88ef6c490628285f482af15ddcb29541f94bcf526a3f6c7.
  - Someone hacks the password database and they check this hash; each account with the corresponding hash is immediately vulnerable.

Basic Terminologies in Cryptography

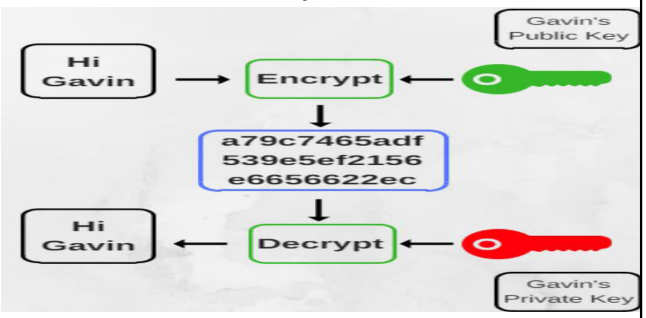
- **Symmetric and Asymmetric Algorithms**
  - In modern computing, there are two primary encryption algorithm types: symmetric and asymmetric. They both encrypt data, but function in a slightly different manner.
    - **Symmetric algorithm:**
      - Uses the same key for both encryption and decryption. Both parties must agree on the algorithm key before commencing communication.
    - **Asymmetric algorithm:**
      - Uses two different keys: a public key and a private key. This enables secure encryption while communicating without previously establishing a mutual algorithm. This is also known as **public key cryptology**

Basic Terminologies in Cryptography

- **Public and Private Keys**
  - An asymmetric algorithm uses two keys: a **public key** and a **private key**.
  - The public key can be sent to other people, while the private key is only known by the owner.
  - What's the purpose of this?
    - Well, anyone with the intended recipient's public key can encrypt a private message for them, while the recipient can only read the contents of that message provided they have access to the paired private key. Check out the below image for more clarity.

Basic Terminologies in Cryptography

- **Public and Private Keys**



Basic Terminologies in Cryptography

- **Public and Private Keys**
  - Public and private keys also play an essential role in **digital signatures**, whereby a sender can sign their message with their private encryption key.
  - Those with the public key can then verify the message, safe in the knowledge that the original message came from the sender's private key.
  - A **key pair** is the mathematically linked public and private key generated by an encryption algorithm.

Basic Terminologies in Cryptography

- **HTTPS**
  - **HTTPS (HTTP Secure)** is a now widely implemented security upgrade for the HTTP application protocol that is a foundation of the internet as we know it.
  - When using a HTTPS connection, your data is encrypted using Transport Layer Security (TLS), protecting your data while in transit.
  - HTTPS generates long-term private and public keys that in turn are used to create a short-term session key.

Basic Terminologies in Cryptography

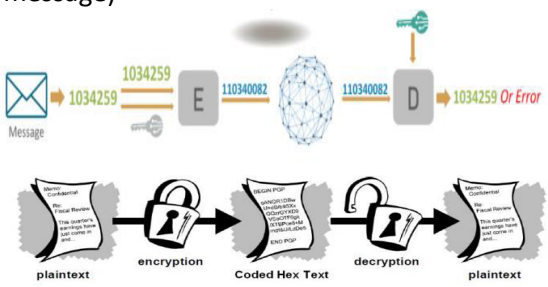
- **HTTPS**
  - The session key is a single-use symmetric key that the connection destroys once you leave the HTTPS site (closing the connection and ending its encryption).
  - However, when you revisit the site, you will receive another single-use session key to secure your communication.
  - A site must completely adhere to HTTPS to offer users complete security.
  - Since 2018 the majority of sites online began offering HTTPS connections over standard HTTP.

Basic Terminologies in Cryptography

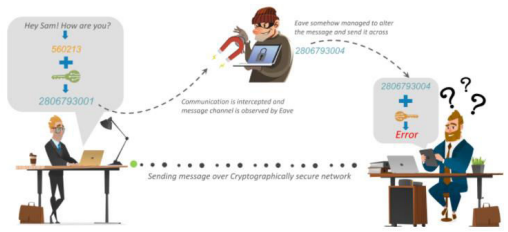
- **End-to-End Encryption**
  - One of the biggest encryption buzzwords is that of **end-to-end encryption**.
  - Social messaging platform service WhatsApp began offering its users end-to-end encryption (E2EE) in 2016, making sure their messages are private at all times.
  - WhatsApp isn't the first, or even the only **messaging service to offer end to end encryption**.
  - Idea of mobile message encryption further into the mainstream - much to the ire of myriad government agencies around the world.

Encryption (Cryptography)

- "hidden writing" (hiding the meaning of the message)



Encryption (Cryptography)



Encryption (Cryptography)

- Basic security goals:
  - privacy (secrecy, confidentiality)
    - only the intended recipient can see the communication
  - authenticity (integrity)
    - the communication is generated by the alleged sender

Types of Encryption Algorithms