R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K
GROUP OF INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

22CS701- CRYPTOGRAPHY AND CYBER SECURITY (Lab Integrated)

Unit-V

Department: Computer Science and Engineering

Batch/Year : 2022-2026/IV

Created by:

Dr. A.Thilagavathy/ Associate Professor/CSE/RMKEC

Dr.D.Naveen Raju /Associate Professor/CSE/RMKEC

Ms.K.Padmapriya/ Associate Professor/CSE/RMDEC

Dr. J. Sherine Glory/Assistant Professor/CSE/RMDEC

Dr.Anish T P/Associate Professor/CSE/RMKCET

Mr.Antony Vijay/ Assistant Professor/CSE/RMKCET

Mr.Vinoth Kumar V/ Assistant Professor/CSE(CS)/RMKCET

Date: 04.10.2025

R.M.K GROUP OF INSTITUTIONS

Table of Contents

22CS701-CRYPTOGRAPHY AND CYBER SECURITY
(Lab Integrated)

COURSE OBJECTIVES

The Course will enable learners to:

- Understand the fundamentals of network security and security architecture.
- Learn the different symmetric key cryptographic algorithms.
- Study the various asymmetric key cryptographic algorithms and techniques.
- Know the importance of message authentication and integrity.
- Learn the various cyber-crimes and cyber security

PREREQUISITE

- 22MA201 Transforms and Numerical Methods
- 22CS501 Computer Networks

22CS701 CRYPTOGRAPHY AND CYBER SECURITY (Lab Integrated)

SYLLABUS

22CS701 CRYPTOGRAPHY AND CYBER SECURITY 3 0 2 4

UNIT I INTRODUCTION TO SECURITY 9+6

Computer Security Concepts – The OSI Security Architecture – Security Attacks – Security Services and Mechanisms – A Model for Network Security – Classical encryption techniques: Substitution techniques, Transposition techniques, Steganography –Foundations of modern cryptography: Perfect security – Information Theory – Product Cryptosystem – Cryptanalysis.

List of Exercise/Experiments:

1. Perform encryption, decryption using the following substitution techniques
(i) Ceaser cipher, (ii) playfair cipher iii) Hill Cipher iv) Vigenere cipher
2. Perform encryption and decryption using following transposition techniques
i) Rail fence ii) row & Column Transformation

UNIT II SYMMETRIC CIPHERS 9+6

Number theory – Algebraic Structures – Modular Arithmetic - Euclid‘s algorithm – Congruence and matrices – Group, Rings, Fields, Finite Fields SYMMETRIC KEY CIPHERS: SDES – Block Ciphers – DES, Strength of DES – Differential and linear cryptanalysis – Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Pseudorandom Number Generators – RC4 – Key distribution.

List of Exercise/Experiments:

1. Apply DES algorithm for practical applications.
2. Apply AES algorithm for practical applications.

UNIT III ASYMMETRIC CRYPTOGRAPHY 9+6

MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler’s totient function, Fermat’s and Euler’s Theorem – Chinese Remainder Theorem – Exponentiation and logarithm ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange -– Elliptic curve arithmetic – Elliptic curve cryptography.

List of Exercise/Experiments:

1. Implement RSA Algorithm using HTML and JavaScript.
2. Implement the Diffie-Hellman Key Exchange algorithm for a given problem.
3. Calculate the message digest of a text using the SHA-1 algorithm.

22CS701 CRYPTOGRAPHY AND CYBER SECURITY (Lab Integrated)

SYLLABUS

22CS701 CRYPTOGRAPHY AND CYBER SECURITY 3 0 2 4

UNIT IV INTEGRITY AND AUTHENTICATION ALGORITHMS 9+6

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function: HMAC, CMAC – SHA – Digital signature and authentication protocols – DSS – Schnorr Digital Signature Scheme – ElGamal cryptosystem – Entity Authentication: Biometrics, Passwords, Challenge Response protocols – Authentication applications – Kerberos MUTUAL TRUST: Key management and distribution – Symmetric key distribution using symmetric and asymmetric encryption – Distribution of public keys – X.509 Certificates

List of Exercise/Experiments:

1. Implement the SIGNATURE SCHEME - Digital Signature Standard.
2. Demonstrate intrusion detection system (ids) using any tool eg. Snort or any other s/w

UNIT V CYBER CRIMES AND CYBER SECURITY 9+6

Cyber Crime and Information Security – classifications of Cyber Crimes – Tools and Methods – Password Cracking, Keyloggers, Spywares, SQL Injection – Network Access Control – Cloud Security – Web Security – Wireless Security

List of Exercise/Experiments:

1. Automated Attack and Penetration Tools

a.Exploring N-Stalker, a Vulnerability Assessment Tool

2. Defeating Malware

i) Building Trojans ii) Rootkit Hunter

COURSE OUTCOMES

CO1	Understand cryptographical concepts.
CO2	Implement various cryptographic algorithms
CO3	Evaluate and apply network security protocols, to secure communications over networks
CO4	Identify common security threats and vulnerabilities and assess their impact on network security
CO5	Implement access control mechanisms and authentication techniques to protect information systems.
CO6	Develop and propose security policies and best practices for securing networks and information systems

CO-PO MAPPING

COs	PO's/PSO's														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO2	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO3	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO4	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO5	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1
CO6	3	3	3	2	2	-	-	2	2	1	-	2	2	2	1

1 – Low, 2 – Medium, 3 – Strong

LECTURE PLAN

S No	Topics	No of periods	Proposed date	Actual Lecture Date	Pertaining CO	Taxo nomy level	Mode of delivery
1	Course objective, course outcome delivery & Course introduction	1	06-10-2025	06-10-2025	CO5, C06	K3, K4	ICT Tools
2	Cyber Crime and Information Security	1	06-10-2025	06-10-2025	CO6	K3	ICT Tools
3	Classifications of Cyber Crimes–	1	07-10-2025	07-10-2025	CO6	K3	ICT Tools
4	Password Cracking, Keyloggers	1	08-10-2025	08-10-2025	CO6	K3	ICT Tools
5	Tools and Methods	1	09-10-2025	09-10-2025	CO6	K3	ICT Tools
6	Spywares, SQL Injection	1	10-10-2025	10-10-2025	CO6	K3	ICT Tools
7	Network Access Control	1	11-10-2025	11-10-2025	CO5	K3	ICT Tools
8	Cloud Security	1	07-10-2025	07-10-2025	CO5	K3	ICT Tools
9	Web Security	2	07-10-2025	07-10-2025	CO5	K3	ICT Tools

LECTURE PLAN

S No	Topics	No of periods	Proposed date	Actual Lecture Date	Pertaining CO	Taxonomy level	Mode of delivery
10	Wireless Security	1	15-10-2025	15-10-2025	CO5	K4	ICT Tools
11	Lab Exercise-N-Stalker, Vulnerability Assessment Tool	1	16-10-2025	16-10-2025	CO5	K3	ICT Tools
12	Lab Exercise-N-Stalker, Vulnerability Assessment Tool	1	17-10-2025	17-10-2025	CO5	K3	ICT Tools
13	Lab Exercise-Defeating Malware ii) Rootkit Hunter	1	22-10-2025	22-10-2025	CO5	K3	ICT Tools
14	Lab Exercise-Defeating Malware ii) Rootkit Hunter	1	24-10-2025	24-10-2025	CO5	K3	ICT Tools
15	Lab Exercise-Defeating Malware ii) Rootkit Hunter	1	25-10-2025	25-10-2025	CO5	K2	ICT Tools

ACTIVITY BASED LEARNING

S NO	TOPICS	Link
1	Classifications of Cyber Crimes	https://www.youtube.com/watch?v=A-eAHB7oXLQ
2	Network Access Control	https://www.youtube.com/watch?v=Oh0su6tQSVQ
3	Keyloggers	https://www.youtube.com/watch?v=3zrBhMB4CU8
4	Web Security	https://www.youtube.com/watch?v=tH5BXm_rVSg

Cyber Crime

Cybercrime refers to criminal activities carried out using computers and the internet, including hacking, data theft, malware attacks, and financial fraud. With businesses, governments, and individuals relying heavily on digital platforms,
cyber threats have escalated, leading to billions in financial losses worldwide. In **2023 alone, cybercrime caused over $8 trillion in damages**, impacting online security on a massive scale.

From phishing scams to ransomware attacks, cybercriminals exploit vulnerabilities to steal sensitive information and disrupt systems.
This article explores the **types of cybercrime with examples**, real-world cases, **cybercrime laws**, and **effective prevention measures** to stay protected in the digital world.
Cybercrime refers to **illegal activities involving computers, networks, or the internet** as a tool to commit offenses. These crimes include:

- **Identity Theft** – Stealing personal information to commit fraud.
- **Financial Fraud** – Online scams, fake transactions, and credit card fraud.
- **Cyberbullying**– Harassment or threats through digital platforms.
- **Phishing Attacks** – Deceptive emails or websites tricking users into revealing sensitive data.
- **Hacking** – Unauthorized access to systems and data breaches.

Malware Attacks – Spreading viruses, ransomware, and trojans to damage or steal data.

Cybercriminals target individuals, businesses, and even government systems, leading to significant financial losses, data breaches, and security threats.

As the internet becomes an essential part of daily life, from online shopping to business operations and communication, **cybercrime cases have surged** globally. Criminals exploit system vulnerabilities to steal personal data, manipulate financial transactions, and disrupt critical services

It's very important to know and protect ourself against the cyber crime. We can avoid these by use of secure networks, frequent updating of software, and not to engage in activities that may appear suspicious online. Cybercrime, especially through the Internet, has grown as the computer has become central to every field like commerce, entertainment, and government. Cybercrime may endanger a person or a nation security and financial health.

Types of Cyber Crime

Cybercrime includes a **wide range of illegal activities** that exploit computers, networks, and the internet. These crimes can be categorized into **two main types**:

1. Cyber Crimes Targeting Computer Networks or Devices

   These crimes involve **direct attacks on computers, servers, or digital infrastructure** to steal data, cause disruption, or damage systems. It involves different threats like- **viruses, bugs, etc.** and **(DoS) denial-of-service attacks.**

MalwareAttacks: This kind ofcyber threat relates to malware viruses, worms, Trojans, etc. for interfering, damaging, or unauthorized access to computer systems.

For example, ransomware encrypts files and then later demands ransom for decryption.

Denial-of-Service (DoS) Attacks: Here, the attackers focus on a system and flood it with high traffic, hence making it inaccessible to the users. Another dangerous variant of DoS is DDoS, wherein many compromised systems target one, thus, much difficult to defend against.

For example, A DDoS attack crashes an e-commerce website by overwhelming its server with traffic.

Phishing Attacks: These are masqueraded e-mails or messages claiming to be from a formal web but only request that the user grantaccess to sensitiveinformation like password points for an account or credit card numbers. Phishing can be described as an outstanding one of the most common cyber threats.

Botnets (Zombie Networks): A number of hijacked computers can become a "botnet" of malware that can be used by an attacker for coordinated attacks or spamming.

For example, Hackers use botnets to send **millions of spam emails** in a single day.

Exploits and Vulnerabilities: The typical area through which cyber-thieves exploit software weakness is the application or operating system vulnerability in order to access it illegally.

For example, Exploiting an outdated banking app to steal user financial details.

2. Crimes Using Computer Networks to Commit Other Criminal Activities

These types of crimes include cyberstalking, financial fraud, or identity thief.

Cyberstalking: This is considered as that crime in the nature of threatening or frightening a person on-line and spreading fear and emotional distress. This can be termed as involving threats, constant monitoring, or receiving repeated unwanted messages.

For example, Sending **threatening messages** to a person via email or social media.

Financial Fraud: This is an example of a cybercrook manipulating the victim online to proceed with stealing money, such as fake investment opportunities, hacking a business email, and using someone else's credit card details.

For example, A fake online store that steals credit card details without delivering products.

Identity Theft: It is normally the identity of people whose information is stolen with the intention of only acting like them either to misuse their cash or money from their account or even to do malicious reasons. It always lowers the credit score of the victim and in the worst case scenario, misused the account/loan financially with incorrect transactions.

For example, A hacker using stolen credentials to **apply for credit cards and loans**.

Online Harassment and Hate Crimes: When people use the internet to discriminate against a particular person based on his or her racial background, gender, religion, or whatever, which can psychologically disturb the harassed person.

For example, Cyberbullying campaigns that target individuals based on race, gender, or religion.

Intellectual Property Theft: Intellectual property theft refers to the theft of copyrighted content or business secrets through the internet, thereby financially and competitively hurting individuals and companies.

For example, A software company illegally using another firm's **source code** to create a competing product.

Cyber Criminals and its types

Examples of Cyber Crime

Cybercrime includes a wide range of illegal activities that exploit the internet, computer systems, and networks for **financial, political, or personal gain**. Here are some of the **most common cybercrime examples**:

1. Cyber Terrorism:

Cyber terrorism involves using the internet to **carry out violent threats, disrupt essential services, or spread fear** among people. Cyber terrorists target **critical infrastructure, government systems, or financial institutions** to cause panic or damage.

Example: Hacking into power grids or communication networks to create widespread disruption

2. Cyber Extortion (Ransomware Attackes):

Cyber extortion happens when hackers attack websites or computer systems and demand money to stop the attacks. They threaten to keep attacking unless they receive a large payment.

Example: A ransomware attack on a hospital system, blocking access to patient records until a ransom is paid

3. Cyber Warfare:

Cyber warfare is when countries use computers and networks as part of their battles. It includes both attacking and defending against cyber threats, like hacking and spying.

Example: A government hacking another country's defense networks to steal classified information.

4. Internet Fraud:

This type of fraud occurs when someone tricks others on internet to steal money or private information. It involves hiding or giving false information to deceive people and covers many different illegal actions.

Example: A scam website pretending to sell products but stealing users' payment details instead

5. Cyber Stalking and Online Harassement

Cyber stalking is a form of online harassment where someone sends threatening messages or emails to a victim they know. If the stalker feels it's not working, they may also start following the victim in real life to make their life more difficult.

Example: An ex-partner repeatedly sending threatening messages and tracking a victim's online activity

6. Financial Fraud:

Cybercriminals steal **personal and financial data** to commit fraud, open fake bank accounts, or make unauthorized transactions. **Phishing attacks** are one of the most common methods used to trick victims into providing sensitive information.

Example: A phishing email pretending to be from a bank, asking users to enter their login details on a fake website.

7. Cyber Espionage:

Cyber espionage refers to **hacking into government agencies, businesses, or corporations to steal confidential data or trade secrets**. It is often used by **competitor businesses or state-sponsored hackers**.

Example: A company stealing another firm's product designs through hacking.

Challenges of Cyber Crime

People are unaware of their cyber rights: The Cybercrime usually happen with illiterate people around the world who are unaware about their cyber rights implemented by the government of that particular country.

Anonymity: Those who Commit cyber crime are **anonymous** for us so we cannot do anything to that person.

Less numbers of case registered: Every country in the world faces the challenge of cyber crime and the rate of cyber crime is increasing day by day because the people who even don't register a case of cyber crime and this is major challenge for us as well as for authorities as well.

Mostly committed by well educated people: Committing a cyber crime is not a cup of tea for every individual. The person who commits cyber crime is a very technical person so he knows how to commit the crime and not get caught by the authorities.

No harsh punishment: In Cyber crime there is no harsh punishment in every cases. But there is harsh punishment in some cases like when somebody commits cyber terrorism in that case there is harsh punishment for that individual. But in other cases there is no harsh punishment so this factor also gives encouragement to that person who commits cyber crime.

Impact of Cyber Crimes

Financial Losses: The fraud and theft can cause great losses not only for the given organizations but for individuals also.

Reputational Damage: Some people may realize that reputation becomes an issue they may lose depending on the legal outcomes resulting from lawsuits.

Operational Disruption: As will be highlighted later, such an occurrence leads to a shutdown and consequently a loss of productivity.

Legal Consequences: In the cases where clients have been involved in some legal cases or even regulatory fines, they may have to go through another phase of legal activities, clients have to spend considerable amount of money on protecting their data.

How to Protect Yourself Against Cybercrime?

Use strong password: Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc, So make them complex. That means combination of letters, numbers and special characters.

Use trusted antivirus in devices: Always use trustworthy and highly advanced antivirus software in mobile and personal computers. This leads to the prevention of different virus attack on devices.

Enable Two-Factor Authentication: Activate two-factor authentication on your accounts for an extra layer of security, which requires a second verification step.

Keep your device software updated: Whenever you get the updates of the system software update it at the same time because sometimes the previous version can be easily attacked.

Use secure network: Public Wi-Fi are vulnerable. Avoid conducting financial or corporate transactions on these networks.

Never open attachments in spam emails: A computer get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

Software should be updated: operating system should be updated regularly when it comes to internet security. This can become a potential threat when cybercriminals exploit flaws in the system.

Information Security

Information Security refers to the process and methodologies involved in protecting sensitive data from unauthorized access, disclosure, disruption, modification, or destruction. In today's digital era, where data is considered one of the most valuable assets, information security has become critically important for individuals, organizations, and governments.

Information security ensures three main objectives, collectively known as the CIA Triad: Confidentiality, Integrity, and Availability. These principles form the foundation of all security practices.

Objectives of Information Security

➢Confidentiality

Confidentiality ensures that information is accessible only to those authorized to have access. It prevents sensitive data from being accessed or disclosed without permission. Techniques used include:

- Encryption
- Access control
- Authentication mechanisms

➢Integrity

Integrity ensures the accuracy and completeness of information. It protects data from being altered by unauthorized entities and ensures that it remains unchanged during storage or transmission.

- Hash functions (e.g., SHA-256)
- Digital signatures
- Checksums

➢Availability

Availability ensures that information and resources are available to authorized users when needed. Downtime or Denial-of-Service (DoS) attacks can affect availability.

Redundancy (e.g., RAID)

Backup solutions

Network security controls

Types of Threats in Information Security

1.Malware

Malicious software like viruses, worms, trojans, and ransomware can damage systems, steal data, or lock files.

- **Phishing**

Phishing is a social engineering attack where attackers impersonate legitimate sources to trick users into revealing personal information.

- **Man-in-the-Middle (MitM) Attacks**

In MitM attacks, the attacker intercepts communication between two parties without their knowledge, often stealing login credentials or sensitive data.

- **Denial-of-Service (DoS) Attacks**

DoS or Distributed DoS (DDoS) attacks flood systems or networks with traffic, making services unavailable to legitimate users.

Insider Threats

These are security breaches caused by employees or people within the organization who have access to critical data and misuse it.

2. **Security Measures and Controls**

- **Physical Security**

Physical measures like CCTV, biometric locks, and secure server rooms protect against unauthorized physical access to IT systems.

- **Technical Controls**

These include firewalls, intrusion detection/prevention systems (IDS/IPS), antivirus software, encryption, and secure protocols like HTTPS and SSH.

- **Administrative Controls**

Policies and procedures such as information classification, training programs, and incident response plans are essential for managing and monitoring security.

3.Cryptography in Information Security

Cryptography plays a central role in information security. It involves encoding information in such a way that only authorized parties can decode and understand it.

Symmetric Encryption: Uses a single key for both encryption and decryption (e.g., AES).

Asymmetric Encryption: Uses a pair of public and private keys (e.g., RSA).

Digital Signatures: Used for authentication and non-repudiation.

Hashing: Used to verify data integrity (e.g., SHA-256, MD5).

4.Authentication and Authorization

Authentication is the process of verifying the identity of a user or system. Common methods include:

- Passwords
- Biometrics (fingerprint, retina scan)
- Two-Factor Authentication (2FA)

Authorization is the process of granting an authenticated user permission to access specific resources.

5.Cybersecurity Policies and Standards

To enforce information security, various frameworks and standards are adopted globally, such as:

- ISO/IEC 27001: Information security management system (ISMS)
- NIST Cybersecurity Framework
- GDPR (General Data Protection Regulation)

These help organizations to design policies, assess risks, and implement best practices.

6.Emerging Trends and Challenges

- Cloud Security: As data moves to cloud platforms, securing cloud storage and virtual machines is critical.
- IoT Security: Connected devices increase the attack surface, requiring strict access control and network segmentation.
- AI in Cybersecurity: AI is used to detect anomalies and automate threat detection.
- Zero Trust Architecture: Trust no device or user by default; every access request must be authenticated and authorized.

Classifications of Cyber Crimes

Cyber crimes are majorly of 4 types:

1. **Against Individuals:** These include e-mail spoofing, spamming, cyber defamation, cyber harassments and cyber stalking.

2. **Against Property**: These include credit card frauds, internet time theft and intellectual property crimes.

3**. Against Organizations**: These include unauthorized accessing of computer, denial Of service, computer contamination / virus attack, e-mail bombing, salami attack, logic bomb, trojan horse and data diddling.

4. **Against Society**: These include Forgery, Cyber Terrorism, Web Jacking.

Classification Of Cyber Crimes Cyber crimes can be classified in to 4 major categories as the following:

(1) Cyber crime against Individual

(2) Cyber crime Against Property

(3) Cyber crime Against Organization

(4)CyberCrimeAgainstSociety

(1) Against Individuals

(i) Email spoofing : A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.

(ii) Spamming : Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

(iii) Cyber Defamation : This occurs when defamation takes place with the help of computers and/or the Internet.

For instance, someone publishes defamatory matter about another person on a website or sends e-mails containing defamatory information. In such cases, determining the truthfulness of the accused's statements can be challenging, and authorities might consider using a polygraph test as part of the investigation.

(iv) Harassment & Cyber stalking : Cyber Stalking Means following an individual's activity over internet. It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

(2) Against Property

(i) Credit Card Fraud : As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.

(ii) Intellectual Property crimes : These include Software piracy: Illegal copying of programs, distribution of copies of software. Copyright infringement: Using copyrighted material without proper permission. Trademarks violations: Using trademarks and associated rights without permission of the actual holder. Theft of computer source code: Stealing, destroying or misusing the source code of a computer. (iii) Internet time theft : This happens by the usage of the Internet hours by an unauthorized person which is actually paid by anotherPerson.

(3) Against Organisations

(i) Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner. It can be of 2 forms:

a) Changing/deleting data: Unauthorized changing of data.

b) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

(ii) Denial Of Service : When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

(iii) Computer contamination / Virus attack : A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

(iv) Email Bombing : Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

(v) Salami Attack : When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.

(vi) Logic Bomb : It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

(vii) Trojan Horse : This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

(viii) Data diddling : This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

(4) Against Society

(i)Forgery : Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.

(ii) Cyber Terrorism : Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.

(iii) Web Jacking : Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money

TOOLS AND METHODS USED IN CYBER CRIME

Network attack incidents reveal that attackers are often very systematic in launching their attacks. The basic stages of an attack are described here to understand how an attacker can compromise a network here

1. Initial Uncovering
2. Network probe
3. Crossing the line toward electronic crime (E-crime)
4. Capturing the network
5. Grab the data
6. Covering tracks

1. Initial Uncovering

Two steps are involved here. In the first step called as reconnaissance, the attacker gathers information, as much as possible, about the target by legitimate means – searching the information about the target on the Internet by Googling social networking websites and people finder websites.

2. Network probe

At the network probe stage, the attacker uses more invasive techniques to scan the information. Usually, a "ping sweep" of the network IP addresses is performed to seek out potential targets, and then a "port scanning" tool.

3. Crossing the line toward electronic crime (E-crime)

Now the attacker is toward committing what is technically a "computer crime." He/she does this by exploiting possible holes on the target system.

4. Capturing the network

At this stage, the attacker attempts to "own" the network. The attacker gains a foothold in the internal network quickly and easily, by compromising low-priority target systems. The next step is to remove any evidence of the attack.

5. Grab the data

Now that the attacker has "captured the network" he/she takes advantage of his/her position to steal confidential data, customer credit card information, deface web pages, alter processes and even launch attacks at other sites from your network, causing a potentially expensive and embarrassing situation for an individual and/or for an organization.

6. Covering tracks

This is the last step in any cyber-attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.

PASSWORD CRACKING

Password is like a key to get an entry into computerized systems like a lock. Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.

The purpose of password cracking is as follows:

1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to a system.

Manual password cracking is to attempt to logon with different passwords.

The attacker follows the following steps

1. Find a valid user account such as an administrator or guest;
2. Create a list of possible passwords;
3. Rank the passwords from high to low probability;
4. Key-in each password;
5. Try again until a successful password is found.

Passwords can be guessed sometimes with knowledge of the user's personal information:

1. Blank (none);
2. The words like "password," "passcode" and "admin";
3. Series of letters from the "qwerty" keyboard, for example, qwerty, asdf or qwertyuiop.
4. User's name or login name;
5. Name of user's friend/relative/pet;
6. User's birthplace or date of birth, or a relative's or a friend's;
7. User's vehicle number, office number, residence number or mobile number;
8. Name of a celebrity who is considered to be an idol by the user;
9. Simple modification of one of the preceding, such as suffixing a digit, particularly 1, or reversing the order of letters.

Online Attacks

An attacker can create a script file (i.e., automated program) that will be executed to try each password in a list and when matches, an attacker can gain the access to the system. The most popular online attack is man-in-the middle (MITM) attack, also termed as "bucket-brigade attack" or sometimes "Janus attack."

Offline Attacks

Mostly offline attacks are performed from a location other than the target (i.e., either a computer system or while on the network) where these passwords reside or are used.

Strong, Weak and Random Passwords

A weak password is one, which could be easily guessed, short, common and a system default password that could be easily found byexecuting a brute force attack and byusing a subset of all possible passwords.

Here are some of the examples of "weak passwords":

1. Susan: Common personal name;
2. aaaa: repeated letters, can be guessed;
3. rover: common name for a pet, also a dictionary word;
4. abc123: can be easily guessed;
5. admin: can be easily guessed;
6. 1234: can be easily guessed;
7. QWERTY: a sequence of adjacent letters on many keyboards;
8. 12/3/75: date, possibly of personal importance;
9. nbusr123: probably a username, and if so, can be very easily guessed;
10. p@$$\/\/0rd: simple letter substitutions are preprogrammed into password cracking tools;
11. password: used very often – trivially guessed;
12. December12: using the date of a forced password change is very common.

Here are some examples of strong passwords:

1. Convert_£100 to Euros!: Such phrases are long, memorable and contain an extended symbol to increase the strength of the password.

2. 382465304H: It is mix of numbers and a letter at the end, usually used on mass user accounts and such passwords can be generated randomly.

3. 4pRte!ai@3: It is not a dictionary word; however it has cases of alpha along with numeric and punctuation characters.

4. MoOoOfIn245679: It is long with both alphabets and numerals.

5. t3wahSetyeT4: It is not a dictionary word; however, it has both alphabets and numerals.

Random Passwords

We have explained in the previous section how most secure passwords are long with random strings of characters and how such passwords are generally most difficult to remember. Password is stronger if it includes a mix of upper-case and lower-case letters, numbers and other symbols, when allowed, for the same number of characters.

The general guidelines applicable to the password policies, which can be implemented organization-wide, are as follows:

1. Passwords and user logon identities (IDs) should be unique to each authorized user.

2. Passwords should consist of a minimum of eight alphanumeric characters.

3. There should be computer-controlled lists of prescribed password rules and periodic testing to identify any password weaknesses.

4. Passwords should be kept private, that is, not shared with friends, colleagues.

5. Passwords shall be changed every 30/45 days or less.

6. User accounts should be frozen after five failed logon attempts.

7. Sessions should be suspended after 15 minutes (or other specified period) of inactivity and require the passwords to be re-entered.

8. Successful logons should display the date and time of the last logon and logoff.

9. Logon IDs and passwords should be suspended after a specified period of non-use.

10. For high-risk systems, after excessive violations, the system should generate an alarm and be able to simulate a continuing session (with dummy data) for the failed user.

KEYLOGGERS

Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.

1. Software Keyloggers

Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded.

SC-KeyLog PRO

It allows to secretly record computer user activities such as E-Mails, chat conversations, visited websites, clipboard usage, etc. in a protected log file.

Spytech SpyAgent Stealth

It provides a large variety of essential computer monitoring features as well as website and application filtering, chat blocking and remote delivery of logs via E-Mail or FTP.

All in one Keylogger

It is an invisible keystrokes recorder and a spy software tool that registers every activity on the PC to encrypted logs.

- Stealth Keylogger
- Perfect Keylogger
- KGB Spy
- Spy Buddy
- Elite Keylogger
- CyberSpy
- Powered Keylogger

2. Hardware Keyloggers

To install these keyloggers, physical access to the computer system is required. Hardware keyloggers are small hardware devices. Listed are few websites where more information about hardware keyloggers can be found:

1. http://www.keyghost.com
2. http://www.keelog.com
3. http://www.keydevil.com
4. http://www.keykatcher.com

3. Antikeylogger

Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool.

Advantages of using Antikeylogger are as follows:

1. Firewalls cannot detect the installations of keyloggers on the systems; hence, Antikeylogger can detect installations of keylogger.

2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs..

3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.

4. It prevents ID theft

5. It secures E-Mail and instant messaging/chatting.

SPYWARES

Spyware is a type of malware that is installed on computers which collects information about users without their knowledge.

The features and functions of such Spywares are beyond simple monitoring.

1. 007 Spy:

It has following key features:

- Capability of overriding "antispy" programs like "ad-aware";
- Record all websites url visited in internet;
- Powerful keylogger engine to capture all passwords;
- View logs remotely from anywhere at any time;
- Export log report in html format to view it in the browser;
- Automatically clean-up on outdated logs;
- Password protection.

2. Spector Pro:

It has following key features:

- Captures and reviews all chats and instant messages;
- Captures E-Mails (read, sent and received);
- Captures websites visited;
- Captures activities performed on social networking sites such as Myspace and Facebook;

• Enables to block any particular website and/or chatting with anyone;

• Acts as a keylogger to capture every single keystroke (including usernames and passwords).

3. **eBlaster:**

Besides keylogger and website watcher, it also records E-Mails sent and received, files uploaded/downloaded, logging users' activities, record online searches, recording Myspace and Facebook activities and any other program activity.

4. Remotespy:

Besides remote computer monitoring, silently and invisibly, it also monitors and records users' PC without any need for physical access. Moreover, it records keystrokes (keylogger), screenshots, E-Mail, passwords, chats, instant messenger conversations and websites visited.

5. Stealth Recorder Pro:

It is a new type of utility that enables to record a variety of sounds and transfer them automatically through Internet without being notified by original location or source. It has following features:

• Real-time mp3 recording via microphone, cd, line-in and stereo mixer as mp3, wma or wav formatted files;

• Transferring via e-mail or ftp, the recorded files to a user-defined e-mail address or ftp automatically;

• Controlling from a remote location;

• Voice mail, records and sends the voice messages.

6. Stealth Website Logger:

It records all accessed websites and a detailed report can be available on a specified E-Mail address. It has following key features:

• Monitor visited websites;

• Reports sent to an E-Mail address;

• Daily log;

• Global log for a specified period;

• Log deletion after a specified period;

• Hotkey and password protection;

• Not visible in add/remove programs or task manager.

7. Flexispy:

It is a tool that can be installed on a cell/mobile phone. After installation, Flexispy secretly records coversation that happens on the phone and sends this information to a specified E-Mail address.

8. Wiretap Professional:

It is an application for monitoring and capturing all activities on the system. It can capture the entire Internet activity. ftis spy software can monitor and record E-Mail, chat messages and websites visited. In addition, it helps in monitoring and recording of keystrokes, passwords entered and all documents, pictures and folders viewed.

9. PC Phone Home:

It is a software that tracks and locates lost or stolen laptop and desktop computers. Every time a computer system on which PC Phone Home has been installed, connected to the Internet, a stealth E-Mail is sent to a specified E-Mail address of the user's choice.

10. SpyArsenal Print Monitor Pro:

It has following features:

- Keep track on a printer/plotter usage;
- Record every document printed;
- Find out who and when certain paper printed with your hardware.

SQL INJECTION

Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS). SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.

The vulnerability is present when user input is either filtered incorrectly for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL injection attacks are also known as SQL insertion attacks

1. Steps for SQL Injection Attack

Following are some steps for SQL injection attack:

1. The attacker looks for the webpages that allow submitting data, that is, login page, search page, feedback, etc.

2. To check the source code of any website, right click on the webpage and click on "view source" (if you are using IE – Internet Explorer) – source code is displayed in the notepad. The attacker checks the source code of the HTML, and look for "FORM" tag in the HTML code. Everything between the <FORM< and </FORM> have potential parameters that might be useful to find the vulnerabilities.

<FORM action=Search/search.asp method=post>

<input type=hidden name=A value=C></FORM>

3. The attacker inputs a single quote under the text box provided on the webpage to accept the user- name and password. This checks whether the user-input variable is sanitized or interpreted literally by the server.

4. The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

2. Blind SQL Injection

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be the one that displays data.

Using SQL injections, attackers can:

1. Obtain some basic information if the purpose of the attack is reconnaissance.
2. May gain access to the database by obtaining username and their password.
3. Add new data to the database.
4. Modify data currently in the database.

3. Tools used for SQL Server penetration

1. AppDetectivePro
2. DbProtect
3. Database Scanner
4. SQLPoke
5. NGSSQLCrack
6. Microsoft SQL Server Fingerprint (MSSQLFP) Tool

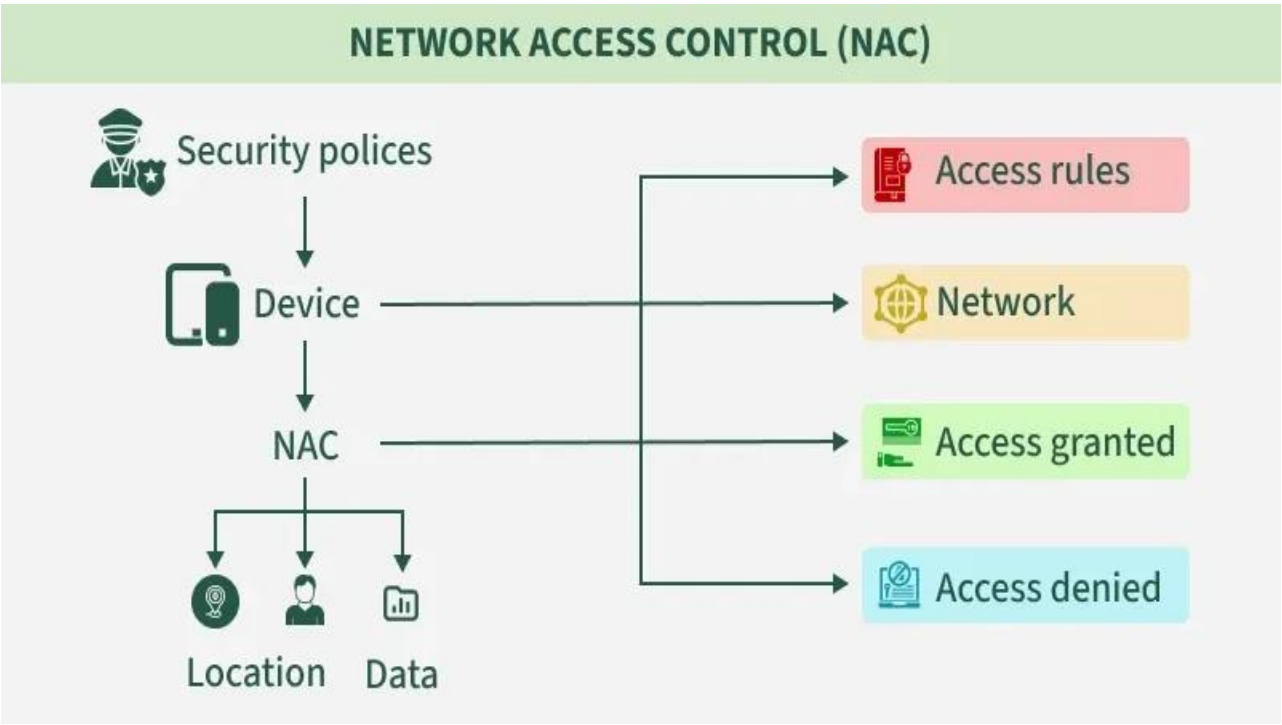
4. How to Prevent SQL Injection Attacks

SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection.

1. Input validation
2. Modify error reports
3. Other preventions

Network Access Control

Network Access Control (NAC) is a security solution that uses a set of protocols to prevent unauthorized users and devices from accessing a private network or to grant restricted access to devices that comply with network security policies. It is also known as Network Admission Control.



NAC is responsible for network management and security by enforcing security policies, ensuring compliance, and managing access control.
It operates across both wired and wireless networks by identifying and evaluating the devices that attempt to connect.
To set up a NAC solution, administrators define protocols that determine how devices and users are authenticated and authorized for different levels of access.
Access rules are typically based on factors such as the device being used, the location of access, the user's access rights, and the specific data or resources being requested.

Types of Network Access Control

Different types of network access control are:

Pre-admission

Post-admission

Pre-admission

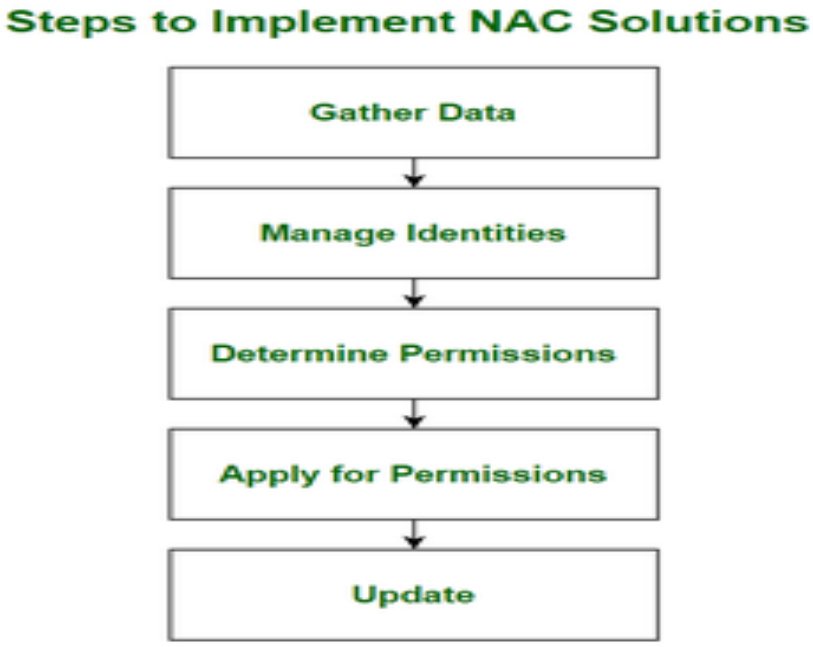
It happens before access to the network is granted, during the initialization of a request by a user or device to access the network. It evaluates the access attempt and only allows access if the user or device is compliant with the organization's security policies and authorized to access the network.

Post-admission

It happens within the network when the user or device attempts to access the different parts of the network. It restricts the lateral movement of the device within the network by asking for re-authentication for each request to access a different part of the network.

Steps to Implement NAC Solutions

Following are the steps to implement NAC solutions:



Gather Data: Perform an exhaustive survey and collect information about every device, user, and server that has to interface with the network resources.

Manage Identities: Verify user identities within the organization by authentication and authorization.

Determine Permissions: Create permission policies stating different access levels for identified user groups.

Apply for Permissions: Apply permission policies on identified user groups and register each user in the NAC system to trace their access level and activity within the network.

Update: Monitor security operations and make adjustments to permission policies based on the changing requirements of the organization over time.

Importance of Network Access Control

Given below the importance of Network Access Control:

There has been exponential growth in the number of mobile devices accessing private organizational networks in recent years.

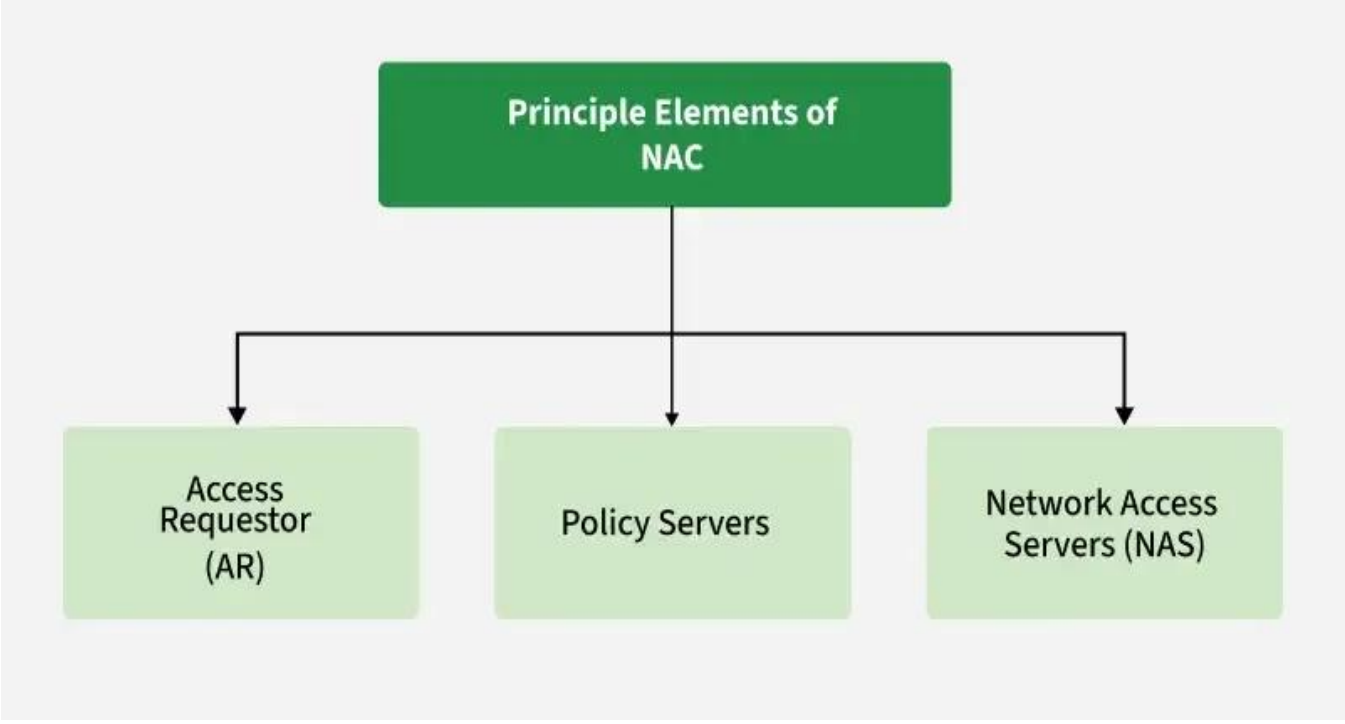
This surge has increased security risks to organizational resources.

To address these risks, tools are needed that offer visibility, access control, and compliance enforcement to strengthen network security.

Network Access Control (NAC) systems can:

- Deny access to non-compliant or unauthorized devices.
- Grant restricted access to devices that partially meet security policies.
- Prevent insecure devices from infecting or compromising the network.

NAC solutions are capable of managing large enterprise networks with a wide variety of device types.



Access Requestor(AR)

An Access Requestor (AR) is any device, user, or process that attempts to gain access to network resources. These could include servers, IP cameras, printers, or other IP-enabled devices managed by the NAC system.

ARs are sometimes referred to as supplicants or clients. To ensure security, ARs must comply with the organization's specific policies or guidelines. This process ensures that unauthorized entities are denied access to protected resources.

Policy Server

The policy server determines what level of access should be granted to an Access Requestor (AR) based on:

The AR's identity.

Its permission level.

The nature of the access request.

The organization's predefined access policies.

It often relies on backend services like:

Antivirus software

Patch management systems

User directories (e.g., Active Directory)

The policy server evaluates the state of the host and uses the organization's rules to either:

Authorize access if the AR complies with policies

Deny or restrict access if the AR does not comply

Network Access Server(NAS)

Users connecting to an organization's internal network from distant locations utilize the NAS as an access control point. NAS devices often serve as VPNs and provide users with access to the company's internal network. These days, NAS functionality is frequently included in policy server systems.

Remote employees can connect to the company's internal network via NAS, which serves as an access point for them. This allows the company and its employees to create a secure connection and grant authorized access to the network.

Key Responsibilities of Network Access Control

Here are the key responsibilities of Network Access Control systems, organized clearly for understanding:

- It allows only compliant, authenticated devices to access network resources and infrastructure.
- It controls and monitors the activity of connected devices on the network.
- It restricts the availability of network resources of private organizations to devices that follow their security policy.
- It regulates the access of network resources to the users.
- It mitigates network threats by enforcing security policies that block, isolate, and repair non-compliant machines without administrator attention.

Real-Life NAC Examples

Here are some real-life Network Access Control (NAC) examples to help you understand how it's used in enterprise environments:

Corporate Office : NAC ensures only company-issued, secure laptops can access internal systems. Unapproved or non-compliant devices are blocked or sent to a restricted network.

Hospital / Healthcare : NAC verifies that medical devices and staff computers meet security standards before accessing patient data. Non-compliant devices are denied or limited in access.

Retail Store : It restricts access so only authorized point-of-sale systems connect to the network. Customer and staff devices are placed on a separate guest Wi-Fi.

Smart Home : It checks smart devices before letting them connect. Guests get internet access only, keeping home automation systems secure.

Limitations of Network Access Control (NAC)

Here are the Limitations of NAC systems that are important to understand, especially in real-world deployments:

Limited Visibility for IoT Devices: NAC has low visibility and control over IoT devices or endpoints without specific user identities.

No Internal Threat Protection: NAC does not protect against threats that originate within the network, such as insider attacks or compromised internal devices.

Compatibility Issues: NAC solutions may not function effectively if they are incompatible with existing security tools or infrastructure within the organization.

CLOUD SECURITY

Cloud computing delivers services such as storage, computing power, and applications over the Internet.

While it provides flexibility and cost savings, it also introduces unique security challenges because data and applications are hosted on shared, virtualized infrastructure managed by third-party providers.

Major Cloud Security Issues

a) Data Breaches

Definition: Unauthorized access to sensitive information stored in the cloud.

Example: Hackers exploiting vulnerabilities in cloud storage to steal customer records.

Causes: Weak authentication, misconfigured cloud storage, insecure APIs.

Countermeasures:

Strong encryption for data at rest and in transit

Multi-factor authentication (MFA)

Proper access control and regular auditing

b) Data Loss

Definition: Permanent loss or corruption of customer data due to system failure or malicious attacks.

Example: Accidental deletion of storage buckets or ransomware attacks.

Countermeasures:

Regular data backups and replication

Disaster recovery planning

Version control and integrity verification

c) Insecure APIs

Definition: Cloud services communicate through APIs, and insecure design may expose sensitive data.

Example: Poorly coded APIs allowing attackers to manipulate requests.

Countermeasures:

- Use of secure API gateways
- Implement authentication tokens and input validation
- Apply rate limiting and API monitoring

d) Account Hijacking

Definition: Attackers gain unauthorized access to user or admin accounts.

Example: Phishing attacks capturing cloud login credentials.

Countermeasures:

- Use of strong passwords and MFA
- User behavior analytics
- Session timeouts and monitoring of login anomalies

e) Insider Threats

Definition: Malicious or careless actions by employees or administrators that compromise data.

Example: Cloud administrator leaking data for personal gain.

Countermeasures:

- Role-based access control (RBAC)
- Least privilege policy
- Employee monitoring and awareness training

f) **Denial of Service (DoS) Attacks**

Definition: Attackers flood the cloud service with traffic, making it unavailable.

Countermeasures:

Auto-scaling and load balancing

Intrusion detection systems (IDS)

Use of Content Delivery Networks (CDNs) and DDoS mitigation tools

G)Data Privacy and Compliance

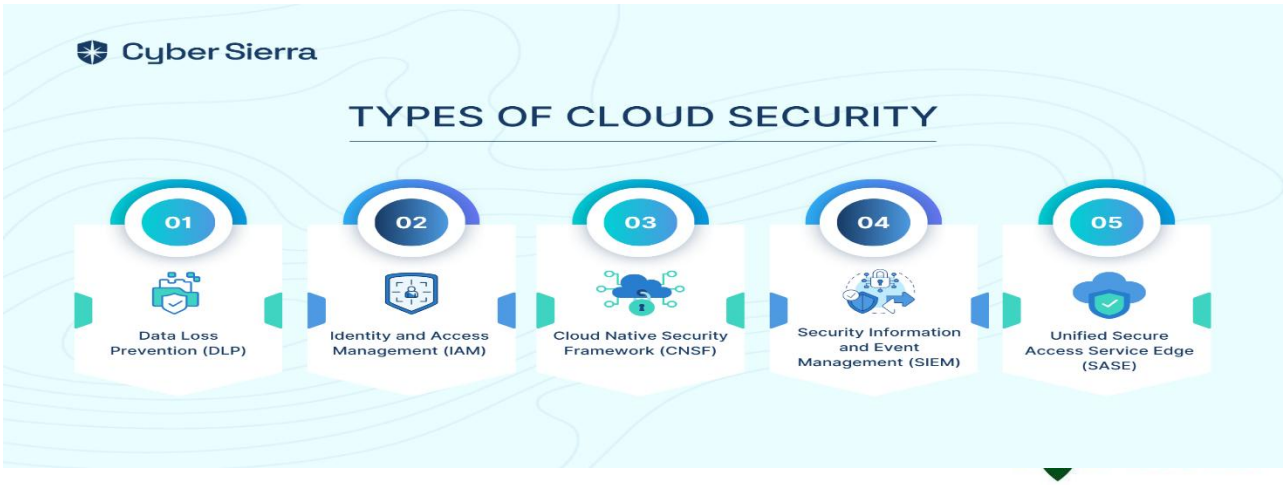
Definition: Failure to comply with laws like GDPR, HIPAA, etc., when storing or processing data in the cloud.

Countermeasures:

Data classification and location control

Compliance with international privacy standards

Periodic security audits



Types of Cloud Security

1. Data Loss Prevention (DLP)

Definition: DLP tools prevent unauthorized access, transmission, or leakage of sensitive data from the cloud.

Functions:

- Monitors data in motion, at rest, and in use.
- Detects and blocks unauthorized sharing or downloads.

Techniques:

- Content inspection
- Encryption
- Access control policies

Example: Google Workspace and Microsoft 365 use DLP to prevent data leakage via emails or file sharing.

2. Identity and Access Management (IAM)

Definition: IAM controls who can access what resources in the cloud.

Functions:

- User authentication and authorization
- Role-Based Access Control (RBAC)
- Multi-Factor Authentication (MFA)

Purpose: Prevents unauthorized access to sensitive systems and ensures accountability.

Example: AWS IAM, Azure Active Directory.

3. Cloud-Native Security Framework (CNSF)

Definition: CNSF focuses on security measures built directly into cloud platforms and applications.

Functions:

Secures containers, microservices, and serverless architectures.

Integrates security into DevOps pipelines (DevSecOps).

Benefits:

Scalability

Automation

Continuous security monitoring

Example: Kubernetes security policies, AWS Security Hub.

4.Security Information and Event Management (SIEM)

Definition: SIEM tools collect, analyze, and correlate security logs and alerts from multiple sources.

Functions:

Detects suspicious activities and anomalies.

Provides real-time incident alerts.

Supports compliance reporting.

Example: Splunk, IBM QRadar, Azure Sentinel**.**

Benefit: Enhances threat detection and incident response in cloud environments.

5.Unified Secure Access Service Edge (SASE)

Definition: SASE is a modern security model that merges network security and wide area networking (WAN) into a unified cloud-based service.

Components:

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB)

Firewall as a Service (FWaaS)

Zero Trust Network Access (ZTNA)

Benefits:

Secure remote access

Simplified management

Consistent security across users and locations

WEB SECURITY

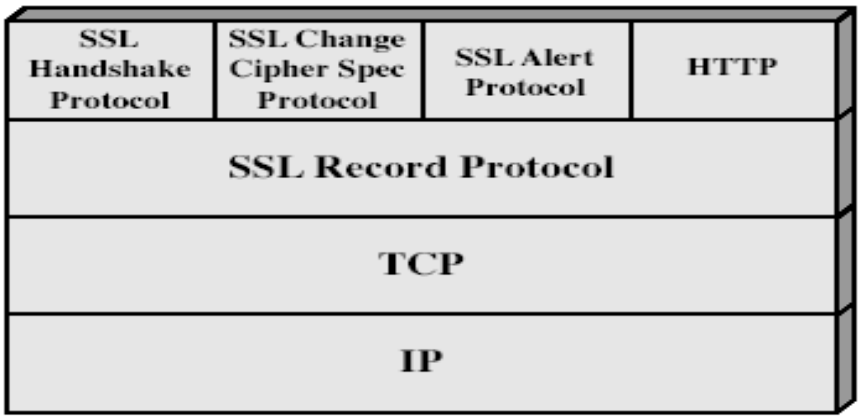
Web now widely used by business, government, individuals but Internet & Web are vulnerable

- It has variety of threats
  - integrity
  - confidentiality
  - denial of service
  - authentication
- need added security mechanisms

SSL (Secure Socket Layer)

- transport layer security service
- originally developed by Netscape
- version 3 designed with public input
- subsequently became Internet standard known as TLS (Transport Layer Security)
- uses TCP to provide a reliable end-to-end service
- SSL has two layers of protocols

SSL Architecture



- **SSL session**
  - an association between client & server
  - created by the Handshake Protocol
  - define a set of cryptographic parameters
  - may be shared by multiple SSL connections
- **SSL connection**
  - a transient, peer-to-peer, communications link
  - associated with 1 SSL session

A session state is defined by the following parameters.

- **Session identifier:** An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
- **Peer certificate:** An X509.v3 certificate of the peer. This element of the state may be null.
- •**Compression method:** The algorithm used to compress data prior to encryption.
- **Cipher spec:** Specifies the bulk data encryption algorithm (such as null, AES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash_size.
- **Master secret:** 48-byte secret shared between the client and server.
- **Is resumable:** A flag indicating whether the session can be used to initiate new connections.

A connection state is defined by the following parameters.

- **Server and client random:** Byte sequences that are chosen by the server and client for each connection.
- • **Server write MAC secret:** The secret key used in MAC operations on **data** sent by the server.

- **Client write MAC secret:** The secret key used in MAC operations on data sent by the client.
- **Server write key:** The secret encryption key for data encrypted by the server and decrypted by the client.
- **Client write key:** The symmetric encryption key for data encrypted by the client and decrypted by the server.
- **Initialization vectors:** When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key.This field is first initialized by the SSL Handshake Protocol. Thereafter, the final ciphertext block from each
- record is preserved for use as the IV with the following record.
- **Sequence numbers:** Each party maintains separate sequence numbers for transmitted and received messages for each connection.When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero. Sequence numbers may not exceed $2^{64} - 1$

SSL Record Protocol

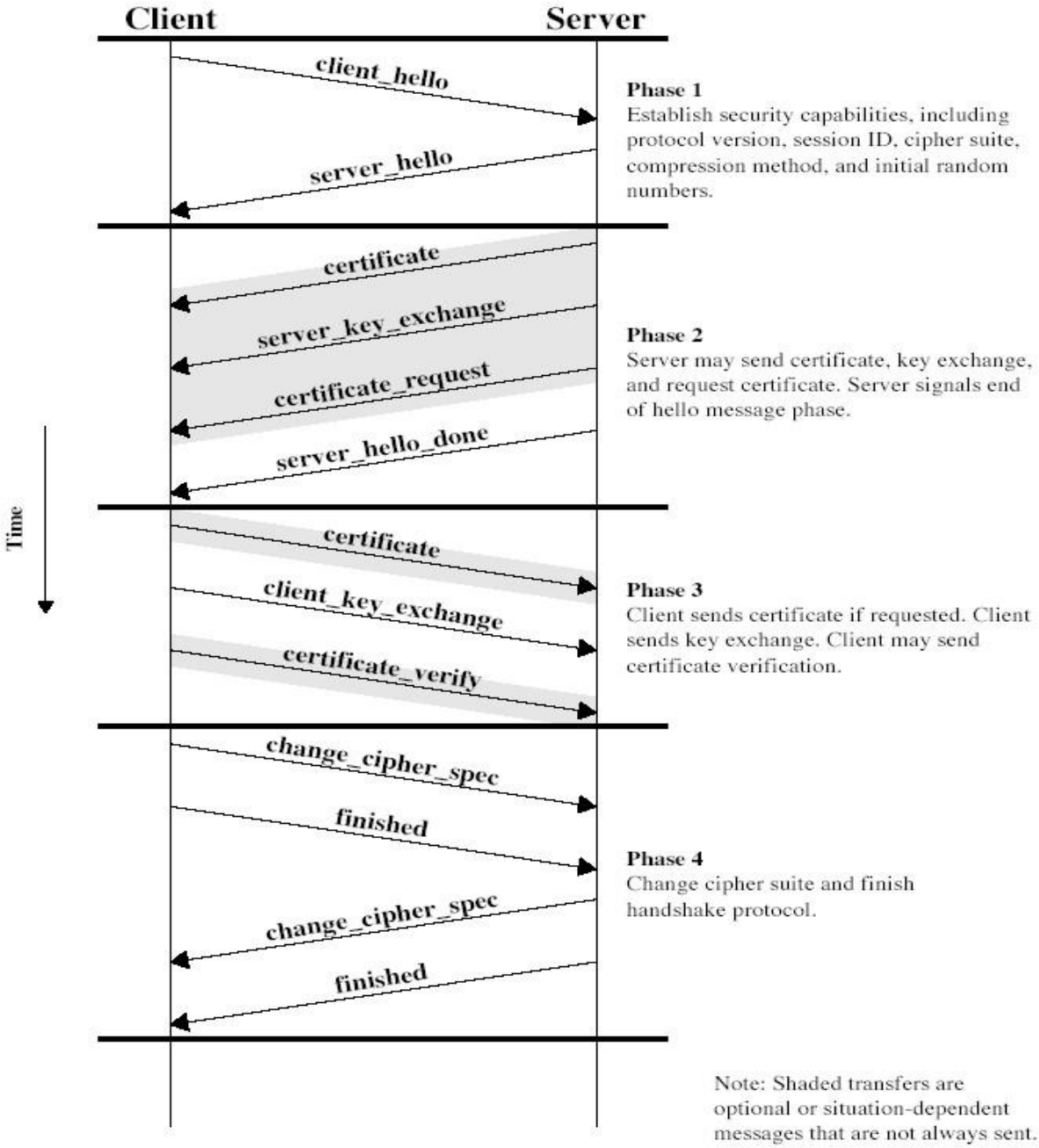
- The SSL Record Protocol provides two services for SSL connections:
- **Confidentiality:** The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads.
- **Message Integrity:** The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

- **SSL Alert Protocol**
- conveys SSL-related alerts to peer entity
- severity
    - warning or fatal
- specific alert
    - unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
    - close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
- compressed & encrypted like all SSL data

SSL Handshake Protocol

- allows server & client to:
    - authenticate each other
    - to negotiate encryption & MAC algorithms
    - to negotiate cryptographic keys to be used
- comprises a series of messages in phases
    - Establish Security Capabilities
    - Server Authentication and Key Exchange
    - Client Authentication and Key Exchange
    - Finish

SSL Handshake Protocol



WIRELESS SECURITY

What is Wireless Security?

Wireless security involves protecting wireless networks and devices (like Wi-Fi routers, smartphones, and laptops) from unauthorized access, data breaches, and other cyber threats.

Common Wireless Security Threats

- **Eavesdropping:** Unauthorized interception of wireless communications.
- **Man-in-the-Middle (MitM) Attacks:** Attackers intercept and possibly alter communication between two parties.
- **Rogue Access Points:** Unauthorized wireless access points that mimic legitimate ones.
- **Denial-of-Service (DoS) Attacks:** Overwhelming the network to disrupt normal operations.
- **Replay Attacks:** Capturing and retransmitting valid data to gain unauthorized access.

Wireless Security Protocols

- **WEP (Wired Equivalent Privacy):** An outdated and insecure protocol.
- **WPA (Wi-Fi Protected Access):** Improved security over WEP but still vulnerable.
- **WPA2:** Utilizes AES encryption for better security.
- **WPA3:** The latest standard with enhanced encryption and protection against brute-force attacks.

Proliferation of mobile and wireless devices:

- People hunched over their smartphones or tablets in cafes, airports, supermarkets and even at bus stops, seemingly oblivious to anything or anyone around them.
- They play games, download email, go shopping or check their bank balances on the go.
- They might even access corporate networks and pull up a document or two on their mobile gadgets.

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Figure below helps us understand how these terms are related. Let us understand the concept of mobile computing and the various types of devices.

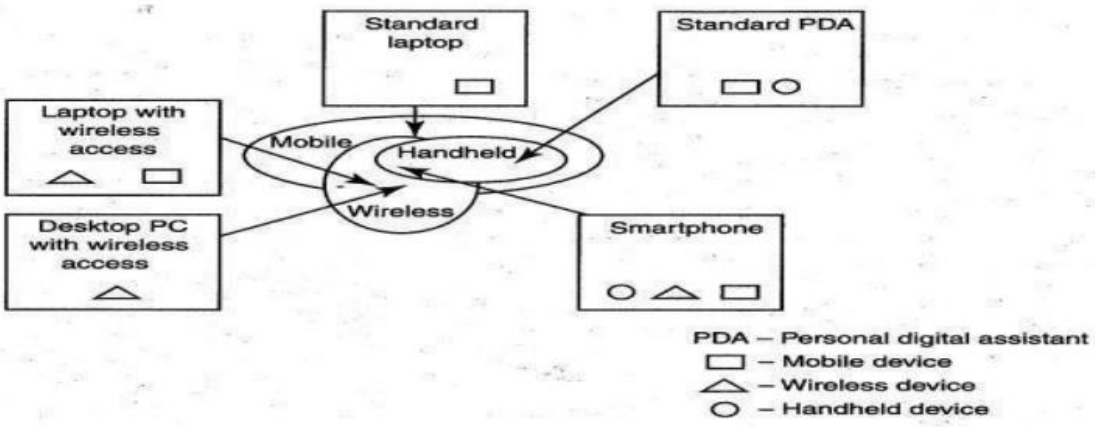


Figure : Mobile, Wireless and hand-held Devices

Mobile computing is "taking a computer and all necessary files and software out into the field." Many types of mobile computers have been introduced since 1990s. They are as follows:

1. **Portable computer:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.

2. **Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touchscreen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasksthat an ordinary laptop would be able to perform.

3. Internet tablet: It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.

4. Personal digital assistant (PDA): It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.

5. Ultramobile (PC): It is a full-featured, PDA-sized computer running a general-purpose operating system(OS).

6. Smartphone: It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.

7. Carputer: It is a computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.

8. Fly Fusion Pentop computer: It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Trends in Mobility:

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity

It is worth noting the trends in mobile computing; this will help readers to readers to realize the seriousness of cybersecurity issues in the mobile computing domain. Figure below shows the different types of mobility and their implications and the attackers (hackers and crackers) are among its biggest fans.

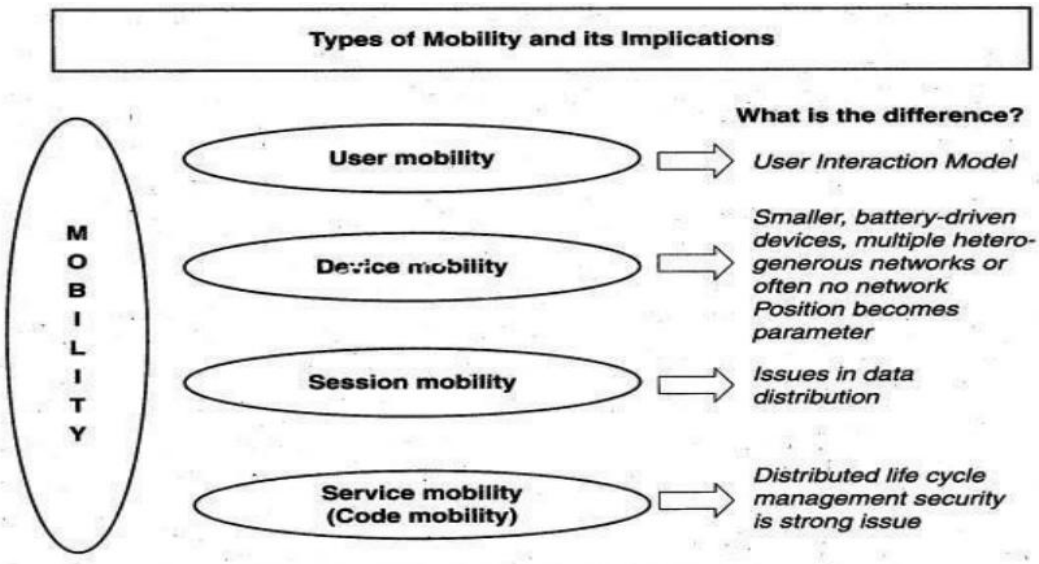


Figure: Mobility types and implications

The new technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators. There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network - that is, public Internet, private networks and other operator's networks - and the other is within the mobile networks that is, devices

such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network. Popular types of attacks against 3G mobile networks are as follows:

1. **Malwares, viruses and worms: Although** many users are still in the transient process of switching from 2G,2.5G2G,2.5G to 3G,3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:

- **Skull Trojan:** I targets Series 60 phones equipped with the Symbian mobile OS.

- **Cabir Worm:** It is the first dedicated mobile-phone worm infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.

- **Mosquito Trojan:** It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.

- **Brador Trojan:** It affects the Windows CE OS by creating a svchost. exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments.

- **Lasco Worm:** It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.

1. **Denial-of-service (DoS):**

The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable. Presently, one of the most common cyber security threats to wired Internet service providers (iSPs) is a distributed denial-of-service (DDos) attack .DDoS attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped.

3.Overbilling attack: Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct or authorize to conduct.

4. Spoofed policy development process (PDP): These of attacks exploit the vulnerabilities in the GTP [GeneralPacket Radio Service (GPRS) Tunneling Protocol].

5. Signaling-level attacks: The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VolP systems.

Credit Card Frauds in Mobile and Wireless Computing Era:

These are new trends in cybercrime that are coming up with mobile computing - mobile commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. Today belongs to "mobile compüting," that is, anywhere anytime computing. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment.

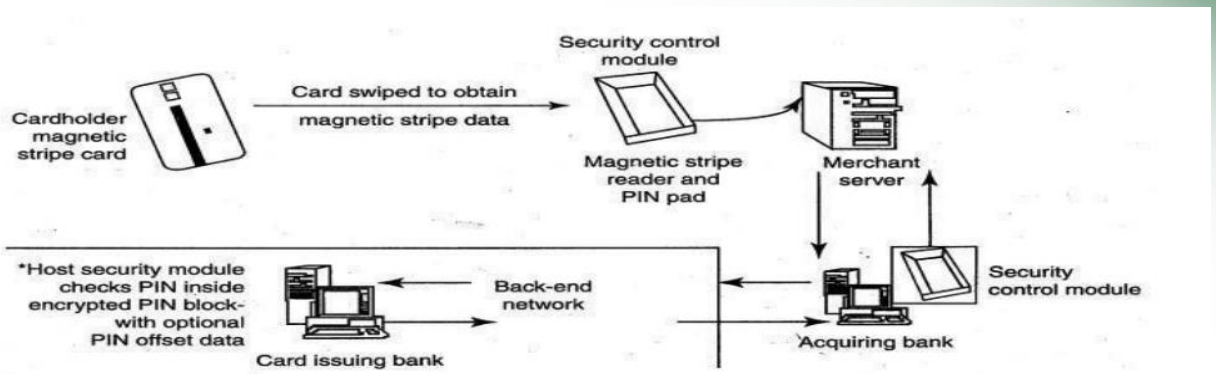


Figure : Online environment for credit card transactions

There is a system available from an Australian company "Alacrity" called closed-loop environment for wireless (CLEW). Figure above shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.

As shown in Figure, the basic flow is as follows:

1. Merchant sends a transaction to bank
2. The bank transmits the request to the authorized cardholder
3. The cardholder approves or rejects (password protected)
4. The bank/merchant is notified
5. The credit card transaction is completed.

Security Challenges Posed by Mobile Devices:

Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. When people are asked about important in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in below figure. As the number of mobile device users increases, two challenges are presented: one at the device level called "micro challenges" and another at the organizational level called "macrochallenges."

Some well-known technical challenges in mobile security are: managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API), security etc.

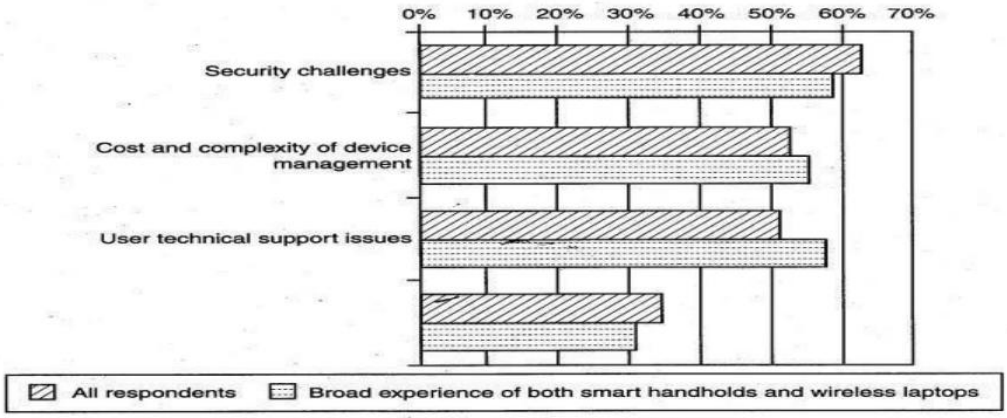


Figure: Important issues for managing mobile devices

Registry Settings for Mobile Devices:

Let us understand the issue of registry settings on mobile devices through an example: Microsoft Activesync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the "gateway between Windows powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device. In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context, registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Authentication Service Security:

There are two components of security in mobile computing: security of devices and security in networks. A secure network access involves authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices. Some eminent kinds of attacks to which mobile devices are subjected to are: push attacks, pull attacks and crash attacks.

Authentication services security is important given the typical attacks on mobile devices through wireless networks: Dos attacks, traffic analysis, eavesdropping, man-in-the-middle attacks and session hijacking. Security measures in this scenario come from Wireless Application Protocols (WAPs), use of VPNs, media access control (MAC) address filtering and development in 802.xx standards.

Attacks on Mobile-Cell Phones:

- **Mobile Phone Theft:** Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals. The following factors contribute for outbreaks on mobile devices:

1. Enough target terminals: The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.

2. Enough functionality: Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.

3. Enough connectivity: Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

- Mobile viruses
- Concept of Mishing
- Concept of vishing
- Concept of smishing
- Hacking-Bluetooth

Mobile Devices:

Managing diversity and proliferation of hand-held devices We have talked about the micro issues of purely technical nature in mobile device security. Given the threats to information systems through usage of mobile devices, the organizations need to establish security practices at a level appropriate to their security objectives, subject to legal and other external constraints.

Unconventional/stealth storage devices :

We would like to emphasize upon widening the spectrum of mobile devices and focus on secondary storage devices, such as compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memory sticks) used by employees.

As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes – unconventional/stealth storage devices available nowadays are difficult to detect and have become a prime challenge for organizational security.

The features of the software allows system administrator to:

Monitor which users or groups can access USB Ports, Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices. Control the access to devices depending on the time of the day and day of the week. Create the white list of USB devices which allows you to authorize only specific devices that will not be locked regardless of any other settings. Set devices in read-only mode. Protect disks from accidental or intentional formatting. Threats through lost and stolen devices This is a new emerging issue for cyber security. Often mobile hand-held devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations.

Organizational Measures for Handling Mobile

A report based on a survey of London's 24,000 licensed cab drivers quotes that 2,900 laptops, 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001 over the last 6-month period.

Protecting data on lost devices

Readers can appreciate the importance of data protection especially when it resides ona mobile hand-held device. At an individual level, employees need to worry about this. **Organizational security Policies and Measures in Mobile Computing Era:**

Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People have grown so used to their hand-helds they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know;

They listen to music using their-hand-held devices. One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices. Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information.

Operating Guidelines for Implementing Mobile Device Security Policies

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical. Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

1.. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatory environment.

2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks. Biometrics techniques can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.

3. Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.

4. Develop a specific framework for using mobile computing devices, including guidelines for data syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.

5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.,

6. Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing or patch management with the centralized

7. Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

Organizational Policies for the Use of Mobile Hand-Held Devices

There are many ways to handle the matter of creating policy for mobile devices. One way is creating distinct mobile computing policy. Another way is including such devices existing policy. There are also approaches in between where mobile devices fall under both existing policies and a new one. In the hybrid approach, a new policy is created to address the specific needs of the mobile devices but more general usage issues fall under general IT policies. As a part of this approach, the "acceptable use" policy for other technologies is extended to the mobile devices. Companies new to mobile devices may adopt an umbrella mobile policy but they find over time the they will need to modify their policies to match the challenges posed by different kinds of mobile hand-held devices.

For example, wireless devices pose different challenges than non-wireless Also, employees who use mobile devices more than 20%% of the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs .

. **Concept of Laptops:** As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable Wireless capability in these devices has also raised cyber security concerns owing to the information being transmitted over other, which makes it hard to detect.

The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop. thieves. are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive.

Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees laptops and to reduce the likelihood that employees will lose laptops.

1. Cables and hardwired locks: The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cable. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40%% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms.

2. Laptop safes: Safes made of polycarbonate - the same material that is used in bulletproof windows, police riot shields and bank security screens-can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.

3. Motion sensors and alarms: Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to their loud nature, they help in deterring thieves. Modern systems for security countermeasures are becoming very vital to protect the information on the employees laptops and to reduce the likelihood that employees will lose laptops laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop.

4. Warning labels and stamps: Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which, in turn makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives and/or keyemployees of the organizations.

5. Other measures for protecting laptops are as follows:

• Engraving the laptop with personal details

• Keeping the laptop close to oneself wherever possible

• Carrying the laptop in a different and unobvious bag making it unobvious to potential thieves • Creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop

• Making a copy of the purchase receipt, laptop serial number and the description of the laptop

• Installing encryption software to protect information stored on the laptop

• Using personal firewall software to block unwanted access and intrusion

• Updating the antivirus software regularly

• Tight office security using security guards and securing the laptop by locking it down in lockers when not in use

• Never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an antitheft device;

• Disabling IR ports and wireless cards and removing PCMCIA cards when not in use. Information systems security also contains logical access controls.

This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical or access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering.

2. Avoiding weak passwords/ access.

3. Monitoring application security and scanning for vulnerabilities.

4. Ensuring that unencrypted data/unprotected file systems do not pose threats.

5. Proper handing of removable drives/storage mediums /unnecessary ports.

6. Password protection through appropriate passwords rules and use of strong passwords.

7. Locking down unwanted ports/devices.

8. Regularly installing security patches and updates.

9. Installing antivirus software/firewalls / intrusion detection system(IDSs).

10. Encrypting critical file systems.

ASSIGNMENT UNIT V QUESTIONS

S.No	Questions	CO	K
SET 1			
1.	Analyze different categories of cybercrimes and discuss their impact on individuals, organizations, and society.	CO5	K4
2.	Evaluate the consequences of SQL Injection attacks on database systems and propose secure coding practices to prevent them.	CO5	K5
SET 2			
3.	Evaluate the security differences between WEP, WPA, WPA2, and WPA3 wireless protocols, highlighting their strengths and weaknesses.	CO5	K5
4.	Analyze major web security vulnerabilities such as XSS, CSRF, and clickjacking, and assess their impact on web applications.	CO5	K4

PART – A QUESTIONS AND ANSWERS

1.What is Cyber Crime?

Cyber Crime refers to illegal activities carried out using computers or the internet, such as hacking, identity theft, and online fraud.

2.Name two classifications of Cyber Crimes.

Computer as a Target (e.g., virus attacks, hacking)

Computer as a Tool (e.g., cyberstalking, phishing)

3.What is Password Cracking?

Password Cracking is the process of recovering passwords from data stored or transmitted by a computer system using methods like brute force, dictionary attacks, or rainbow tables.

4.What is a Keylogger?

A Keylogger is a surveillance tool (software or hardware) that records every keystroke made on a computer, often used to steal sensitive data like passwords.

5.Define Spyware.

Spyware is malicious software that secretly gathers user information without consent and sends it to third parties.

6. What is SQL Injection?

SQL Injection is a code injection technique where malicious SQL code is inserted into input fields to manipulate a database and gain unauthorized access.

7.What is Network Access Control (NAC)?

NAC is a security approach that restricts unauthorized users and devices from accessing a network, ensuring only compliant devices can connect.

8.What is Cloud Security?

Cloud Security refers to policies, technologies, and controls deployed to protect data, applications, and infrastructure in cloud computing environments.

9.What is Web Security?

Web Security involves protecting websites and online services against cyber threats such as malware, phishing, and cross-site scripting (XSS).

10.What is Wireless Security?

Wireless Security is the prevention of unauthorized access or damage to wireless networks using protocols like WPA2/WPA3 and encryption techniques.

11.What is Phishing?

Phishing is a cyber attack that tricks individuals into providing sensitive information like usernames, passwords, or credit card details by pretending to be a trustworthy entity.

12.What is Malware?

Malware is malicious software designed to damage, disrupt, or gain unauthorized access to a computer system.

13.Define Ransomware.

Ransomware is a type of malware that locks or encrypts a user's data and demands payment to restore access.

14.What are the main objectives of Information Security?

The main objectives are Confidentiality, Integrity, and Availability, often referred to as the CIA Triad.

15.What is the difference between a Hacker and a Cracker?

A Hacker explores systems for knowledge and improvement, while a Cracker breaks into systems with malicious intent.

16.What is Social Engineering in cyber crime?

Social Engineering is manipulating people into giving up confidential information, often by impersonating a legitimate entity.

17.Mention two common tools used for password cracking.

1. John the Ripper
2. Hashcat

18.What is Brute Force Attack?

A Brute Force Attack tries all possible combinations of passwords until the correct one is found.

19.Define Firewall.

A Firewall is a network security system that monitors and controls incoming and outgoing traffic based on predetermined security rules.

20.What is Two-Factor Authentication (2FA)?

2FA is a security process where users verify their identity using two different factors, such as a password and a one-time code sent to a mobile device

21.What is the purpose of Intrusion Detection System (IDS)?

An IDS monitors network or system activities for malicious actions or policy violations and alerts administrators.

22.Define Encryption.

Encryption is the process of converting data into a coded format to prevent unauthorized access.

23.What is a Botnet?

A Botnet is a network of infected computers controlled by a hacker to perform coordinated cyber attacks.

24.What is Denial of Service (DoS) attack?

A DoS attack floods a system or network with traffic to make it unavailable to legitimate users.

25.Name two common Web Security threats.

1. Cross-Site Scripting (XSS)
2. Cross-Site Request Forgery (CSRF)

26.What is WPA2 in wireless security?

WPA2 (Wi-Fi Protected Access 2) is a security protocol used to secure wireless networks by encrypting data.

27.What is Data Breach?

A Data Breach is the unauthorized access and retrieval of sensitive information from a system or network.

28.What is Digital Forensics?

Digital Forensics is the process of collecting, analyzing, and preserving digital evidence from electronic devices to investigate cyber crimes.

29.What is Identity Theft?

Identity Theft is a cyber crime where someone illegally obtains and uses another person's personal data, often for financial gain.

30.Mention two cloud service models.

1. Infrastructure as a Service (IaaS)
2. Software as a Service (SaaS)

31.What is Cyber Espionage?

Cyber Espionage is the act of stealing sensitive or classified information from governments or organizations through cyber means, often for political or economic gain.

32.Define Ethical Hacking.

Ethical Hacking involves authorized testing of systems and networks to identify and fix security vulnerabilities before malicious hackers exploit them.

33.What is Shoulder Surfing?

Shoulder Surfing is a technique used to obtain personal information such as PINs or passwords by observing the user's screen or keyboard over their shoulder.

34.What is Cyber Terrorism?

Cyber Terrorism is the use of internet-based attacks to cause large-scale disruption or fear, typically for political or ideological motives.

35.Name two types of Keyloggers.

1. Software-based Keylogger
2. Hardware-based Keylogger

35.What is a Backdoor in computing?
A Backdoor is a hidden method of bypassing normal authentication to gain remote access to a computer system.

37.What is the main purpose of SQL Injection?
To manipulate a database by injecting malicious SQL code, usually to retrieve unauthorized data or bypass login authentication.

38.Name two tools used in SQL Injection attacks.

Answer:

1. SQLmap
2. Havij

39. What is Cloud Computing?
Cloud Computing is the delivery of computing services like storage, servers, and software over the internet ("the cloud").

40.What is Data Integrity?
Data Integrity refers to the accuracy, consistency, and reliability of data throughout its lifecycle.

41.What is a Zero-Day Vulnerability?
A Zero-Day Vulnerability is a security flaw unknown to the software vendor, exploited before a fix is released.

42.What is Network Sniffing?

Network Sniffing is monitoring and capturing data packets passing through a network, often used for both legitimate analysis and malicious spying.

43.Define Digital Signature.
A Digital Signature is a cryptographic technique used to verify the authenticity and integrity of a message, software, or digital document.

44.What is Man-in-the-Middle (MitM) attack?
In a MitM attack, an attacker secretly intercepts and possibly alters communication between two parties who believe they are directly communicating with each other.

45.What is a VPN (Virtual Private Network)?
A VPN encrypts internet connections and masks the user's IP address, providing privacy and secure access over public networks.

46.What is a Rootkit?
A Rootkit is a type of malware designed to hide the existence of certain processes or programs, allowing continued privileged access to a system.

47.What is Session Hijacking?
Session Hijacking is an attack where an attacker takes control of a user session by stealing or predicting a valid session token.

48.What is Multi-Factor Authentication (MFA)?
MFA is a security system that requires more than one method of authentication from independent categories to verify a user's identity.

49.What is the role of Antivirus software?
Antivirus software detects, prevents, and removes malicious software from a computer system.

50.What is Cyber Law?
Cyber Law refers to legal regulations governing the use of the internet, computers, and digital communication to prevent cyber crimes.

PART-B QUESTIONS

1. Apply any two password cracking techniques to explain how attackers retrieve passwords.
2. Illustrate how SQL Injection works with an example. Explain how to prevent it.
3. Demonstrate how a keylogger operates and how it can be detected.
4. Apply the concept of Network Access Control (NAC) to a university campus network. How does it enhance security?
5. Use examples to explain common wireless security protocols and their use in preventing cyber threats.
6. Analyze the different types of cyber crimes and their impact on individuals and organizations.
7. Compare and analyze Spyware, Ransomware, and Keyloggers in terms of behavior, detection, and prevention.
8. Analyze a real-world case study of a data breach. Identify how the breach occurred and what security failures were involved.
9. Explain and analyze the role of encryption in cloud security.
10. Examine how firewalls and intrusion detection systems (IDS) work together to secure a network.
11. Evaluate the effectiveness of current web security techniques against modern cyber threats.
12. Critically evaluate the role of digital forensics in solving cyber crimes.
13. Evaluate various cloud security challenges and how organizations can address them.
14. Assess the importance of ethical hacking in today's cyber security landscape.
15. Justify the implementation of multi-factor authentication over traditional password systems.
16. Design a secure wireless network for a small business organization. Include necessary security protocols and access controls.
17. Develop a security policy framework for a cloud-based enterprise application
18. Create an awareness campaign outline to educate employees about phishing and social engineering.
19. Propose a model for detecting and preventing insider threats in an organization.
20. Design a cyber incident response plan for a medium-sized company.
21. Explain the tools and methods used by cyber criminals to launch attacks. Illustrate with suitable examples.
22. Explain the working of keyloggers and spywares. How can users protect themselves from such attacks?
23. Explain the major security issues in cloud computing and describe countermeasures for each.
24. Illustrate the shared responsibility model in cloud security with examples from major service providers
25. Discuss how SSL/TLS, HTTPS, and digital certificates provide secure web communication.

GATE QUESTIONS

Password Cracking

Q1. Which type of password attack would be most successful against the password "T63k#s23A"?

Options:

a) Dictionary

b) Hybrid

c) Password guessing

d) Brute force

Answer: d) Brute force

Explanation: Brute-force attacks systematically try every possible combination, making them effective against complex passwords without recognizable patterns.

Q2. What is a wrapper in the context of cybersecurity?

Options:

a) A tool to encrypt data

b) A program that combines a Trojan and legitimate software

c) A type of firewall

d) A password manager

Answer: b) A program that combines a Trojan and legitimate software

Explanation: A wrapper is used to bind a Trojan with legitimate software, allowing the Trojan to be installed alongside the legitimate application.

Keyloggers & Spyware

Q3. Keyloggers are a form of:

Options:

a) Spyware

b) Shoulder surfing

c) Trojan

d) Social engineering

Answer: a) Spyware

Explanation: Keyloggers are software or hardware tools that record keystrokes to gather sensitive information, classifying them as spyware.

Q4. Which of the following best describes spyware?
Options:
a) Software that displays unwanted ads
b) Software that encrypts user data for ransom
c) Software that secretly gathers user information
d) Software that improves system performance
Answer: c) Software that secretly gathers user information
Explanation: Spyware covertly collects data from a user's system without their knowledge, often for malicious purposes.
Q5. What are effective countermeasures against spyware and keyloggers?
Options:
a) Installing more applications
b) Using reputable firewalls and keystroke encryption tools
c) Sharing passwords only with trusted individuals
d) Regularly updating social media profiles
Answer: b) Using reputable firewalls and keystroke encryption tools
Explanation: Firewalls monitor network activity to block malicious software, and keystroke encryption tools like KeyScrambler can prevent keyloggers from capturing sensitive information.

SQL Injection
Q6. Which of the following best describes a SQL Injection attack?
Options:
a) Injecting malicious scripts into a web page
b) Injecting SQL commands into input fields to manipulate the database
c) Overloading a server with requests to cause a crash
d) Intercepting data packets over a network
Answer: b) Injecting SQL commands into input fields to manipulate the database
Explanation: SQL Injection involves inserting malicious SQL statements into input fields, exploiting vulnerabilities in an application's software to manipulate or access the database.

Network Access Control

Q7. What is the primary purpose of Network Access Control (NAC)?

Options:

a) To monitor network traffic for suspicious activity
b) To prevent unauthorized devices from accessing the network
c) To encrypt data transmitted over the network
d) To provide high-speed internet access

Answer: b) To prevent unauthorized devices from accessing the network

Explanation: NAC solutions enforce security policies by allowing only compliant and trusted devices to access network resources, thereby enhancing network security.

Cloud Security

Q8. In cloud computing, which model provides the highest level of control to the customer?

Options:

a) Software as a Service (SaaS)
b) Platform as a Service (PaaS)
c) Infrastructure as a Service (IaaS)
d) Function as a Service (FaaS)

Answer: c) Infrastructure as a Service (IaaS)

Explanation: IaaS offers virtualized computing resources over the internet, giving customers control over operating systems, storage, and deployed applications.

Web Security

Q9. Which HTTP header is used to prevent cross-site scripting (XSS) attacks?

Options:

a) Content-Type
b) X-Content-Type-Options
c) X-XSS-Protection
d) X-Frame-Options

Answer: c) X-XSS-Protection

Explanation: The X-XSS-Protection header enables the cross-site scripting filter built into most modern web browsers, providing protection against XSS attacks.

Wireless Security

Q10. Which wireless security protocol is considered the most secure?

Options:

a) WEP

b) WPA

c) WPA2

d) WPA3

Answer: d) WPA3

Explanation: WPA3 is the latest Wi-Fi security protocol, offering enhanced security features over its predecessors, including stronger encryption and protection against brute-force attacks.

Supportive Online Certification Courses

1. Introduction to Cyber Security – **Coursera platform**
2. Certified Ethical Hacker (CEH) - **EC-Council / Simplilearn**
3. CompTIA Security+ Certification - **Udemy / Coursera**
4. Foundations of Cloud Security - **Coursera (Google Cloud / AWS)**
5. Advanced SQL Injection & Database Security - **Udemy / EC-Council**
6. Incident Response & Digital Forensics - Coursera (IBM / Google)

Real time Applications in day today life and to Industry

"Data Breach at Yahoo – A Global Cybercrime Incident"

Overview

One of the largest cyber security breaches in history.
Occurred between 2013–2014, exposed 3 billion user accounts.
Revealed weaknesses in data protection and network security.

Classification of Cyber Crime

Type: Data breach, identity theft, unauthorized access.
Category: Cybercrime against organizations and individuals.

Tools and Methods Used

- Phishing attacks and malicious emails.
- Password cracking of weakly hashed credentials (MD5).
- SQL Injection exploited vulnerabilities in web applications.

Key Cyber Security Issues

- Weak password encryption and outdated hashing.
- No multi-factor authentication (MFA).
- Poor network access control (NAC) and internal security.
- Unsecured cloud data storage and lack of encryption.

Impact

- Exposure of personal data (emails, passwords, recovery info).
- Major reputation loss and $117 million in settlements.
- Triggered global awareness of corporate cyber hygiene.

Preventive Measures Adopted

- Implementation of AES & SHA-256 encryption.
- Zero Trust Network Access (ZTNA) and MFA.
- Regular vulnerability testing & employee awareness training.

Relevance to Daily Life & Industry

- Highlights importance of strong passwords and secure logins for individuals.
- Encourages industries to adopt proactive security frameworks and cloud protection.
- Serves as a benchmark case for data privacy

CONTENT BEYOND THE SYLLABUS

- Digital Forensics (tools like Autopsy, FTK)
- Penetration Testing Frameworks (Metasploit, Burp Suite).
- Anti-Spyware Techniques (Sandboxing, Process Isolation).
- NoSQL Injection (MongoDB, Firebase).
- Zero Trust Architecture (ZTA).
- Shared Responsibility Model (AWS, Azure).
- DevSecOps and Secure SDLC.
- WPA3 and SAE handshake.

Mini Projects Suggestions

1. Cyber Crime & Threat Simulation Projects

Cyber Crime Case Study Analyzer

Description: Build a searchable database of real-world cyber crime incidents (classified by type: phishing, identity theft, etc.) with visual analytics.

Tools: Python (Flask/Django), SQLite/MySQL

Concepts: Classification of cyber crimes, threat intelligence

2. Phishing Email Detector

Description: Train a machine learning model to detect phishing emails based on features like suspicious URLs, sender info, etc.

Tools: Python (Scikit-learn, Pandas, NLP)

Concepts: Email security, ML in cybercrime detection

Security Tools Demonstration Projects

3. Password Cracking Simulator

Description: Create a demo tool to simulate dictionary and brute-force attacks (with constraints to avoid ethical issues).

Tools: Python (Tkinter/CLI)

Concepts: Password strength, brute-force vs dictionary attack

4. Keylogger & Detection Mechanism

Description: Build a simple keylogger (for educational purposes) and pair it with detection software that scans for suspicious activity.

Tools: Python (Pynput module)

Concepts: Malware behavior, endpoint security

5. SQL Injection Lab
Description: Develop a vulnerable login system and demonstrate SQL injection attacks and their prevention.
Tools: PHP/MySQL or Flask
Concepts: Web app security, SQL injection, input validation

Network & Web Security Projects
6. Network Access Control Simulation
Description: Simulate a NAC system using MAC address filtering, user authentication, and device validation.
Tools: Python, Wireshark, Linux tools
Concepts: NAC policies, network segmentation

7. Secure Web App using OWASP Top 10
Description: Create a mini web app and apply mitigations for OWASP Top 10 vulnerabilities like XSS, CSRF, SQLi.
Tools: Node.js or Flask, MongoDB
Concepts: Web security, best coding practices

8. Firewall Rule Engine
Description: Design a simple rule-based firewall that allows/blocks packets based on IP, ports, and protocols.
Tools: Python with socket programming
Concepts: Packet filtering, intrusion prevention

Cloud & Wireless Security Projects

9. Cloud Storage Encryption Tool

Description: Encrypt files before uploading to cloud storage providers like Google Drive or Dropbox using AES/RSA.
Tools: Python (PyCrypto, API integration)
Concepts: Cloud security, data encryption

10. Wireless Network Sniffer & Analyzer

Description: Build a tool to monitor Wi-Fi packets and detect unauthorized access or weak encryption usage.
Tools: Python (Scapy), Wireshark
Concepts: Wireless network security, Wi-Fi vulnerabilities

ASSESSMENT SCHEDULE

S.NO	Name of the Assessment	Portion	Proposed Date
1	First Internal Assessment	Unit-1 &Unit 2	14.08.2025
2	Second Internal Assessment	Unit-3 &Unit 4	22.09.2025
3	Model Examination	Unit 1-Unit 5	28.10.2025

Thank you

R.M.K GROUP OF INSTITUTIONS