CSE- 321
Software Engineering

Security

Software Security

Software Security

What does Software Security mean?

In the general sense, security is “the state of being free from danger or threat”. The security of software systems in particular is a vast topic.

Software security is the application of techniques that assess, mitigate, and protect software systems from vulnerabilities.

These techniques ensure that software continues to function and are safe from attacks. Developing secure software involves considering security at every stage of the life cycle.

Software security isn’t the same thing as security software.

Software Security

What does Software Security mean?

Security testing takes the following six measures to provide a secured environment

1. **Confidentiality** − It protects against disclosure of information to unintended recipients.
2. **Integrity** − It allows transferring accurate and correct desired information from senders to intended receivers.
3. **Availability** − It ensures readiness of the information on requirement.
4. **Non-repudiation** − It ensures there is no denial from the sender or the receiver for having sent or received the message.
5. **Authentication** − It verifies and confirms the identity of the user.
6. **Authorization** − It specifies access rights to the users and resources.

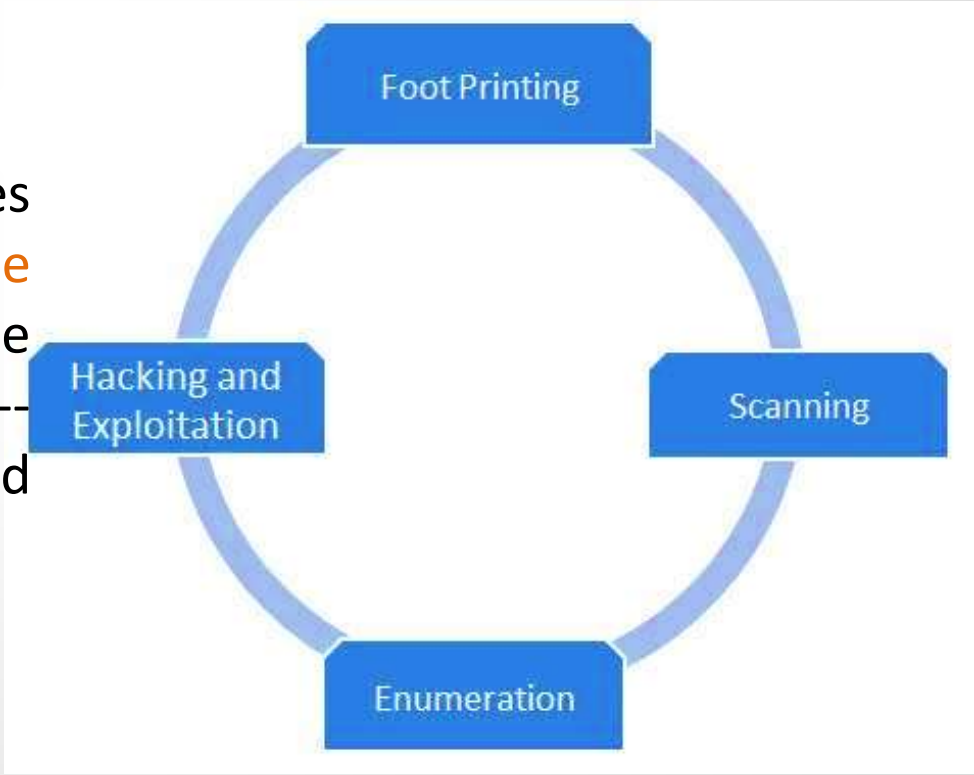
Software Security

Penetration testing, also called **pen testing** or **ethical hacking**, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.

The main objective of penetration testing is to identify security weaknesses.

Penetration testing can be automated with software applications or performed manually.

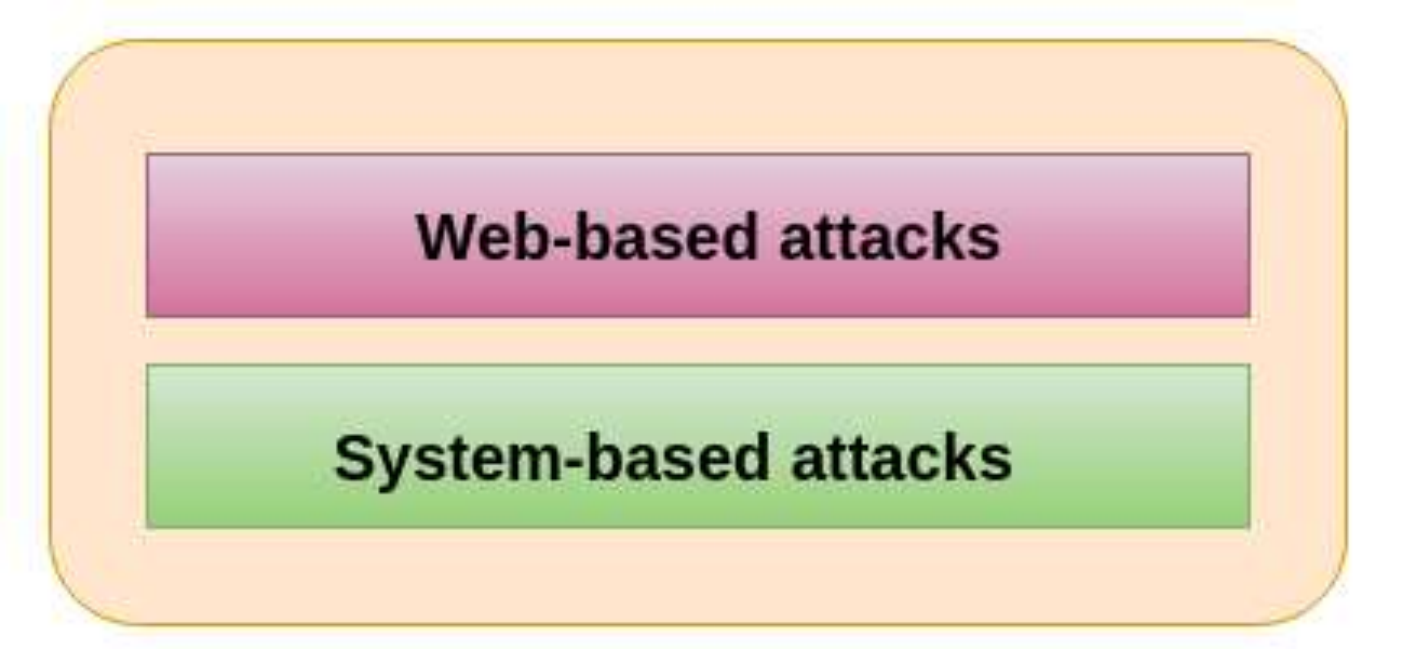
Either way, the process involves gathering information about the target before identifying possible entry points, attempting to break in -- either virtually or for real -- and reporting back the findings.



Malicious software (malware)

Malicious software (malware) is any software that gives partial to full control of the system to the attacker/malware creator**.**

Types of Attacks



Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

Web-based attacks

Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

Web-based attacks

Denial of Service (DOS)

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

Web-based attacks

Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

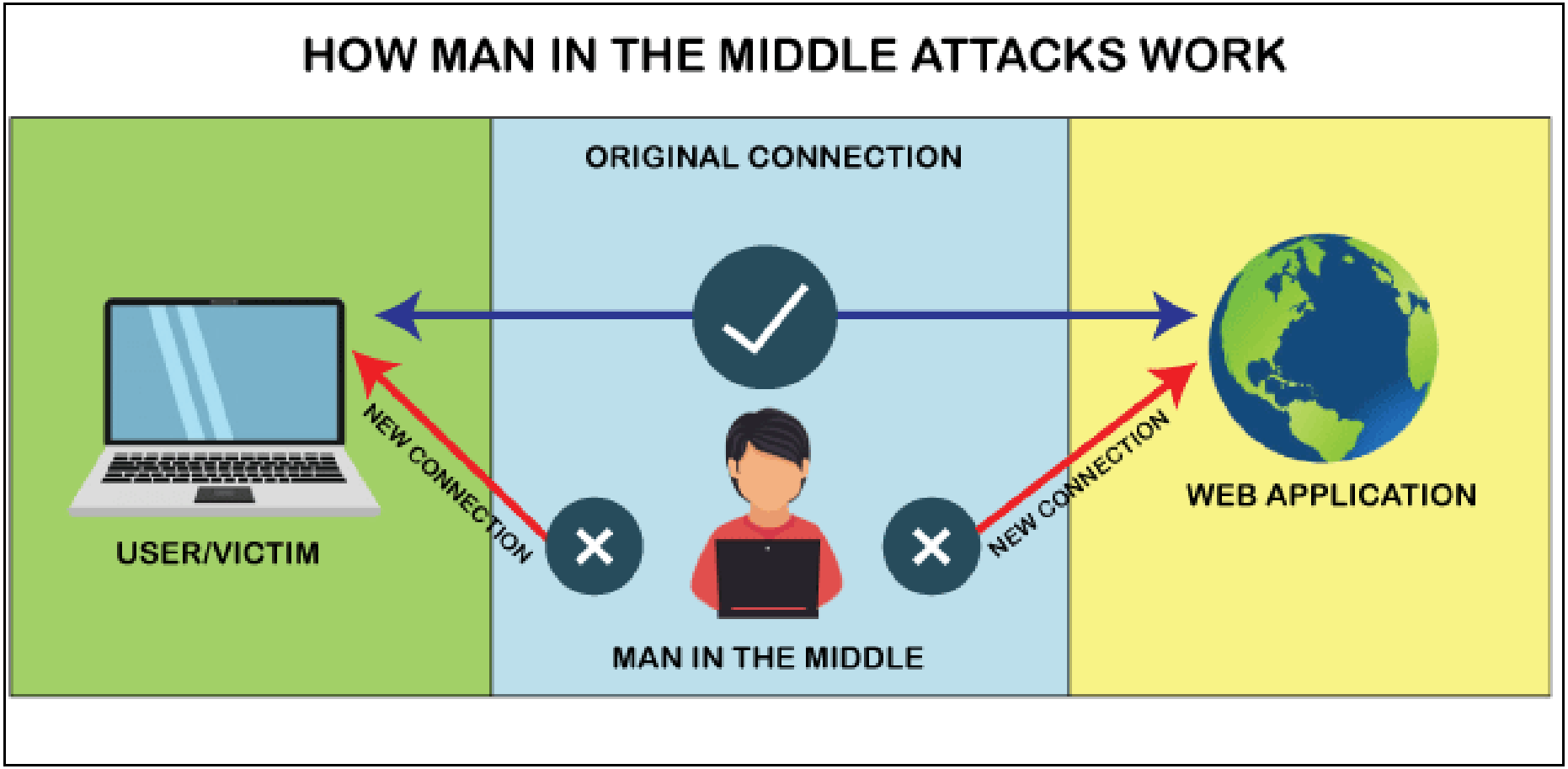
File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

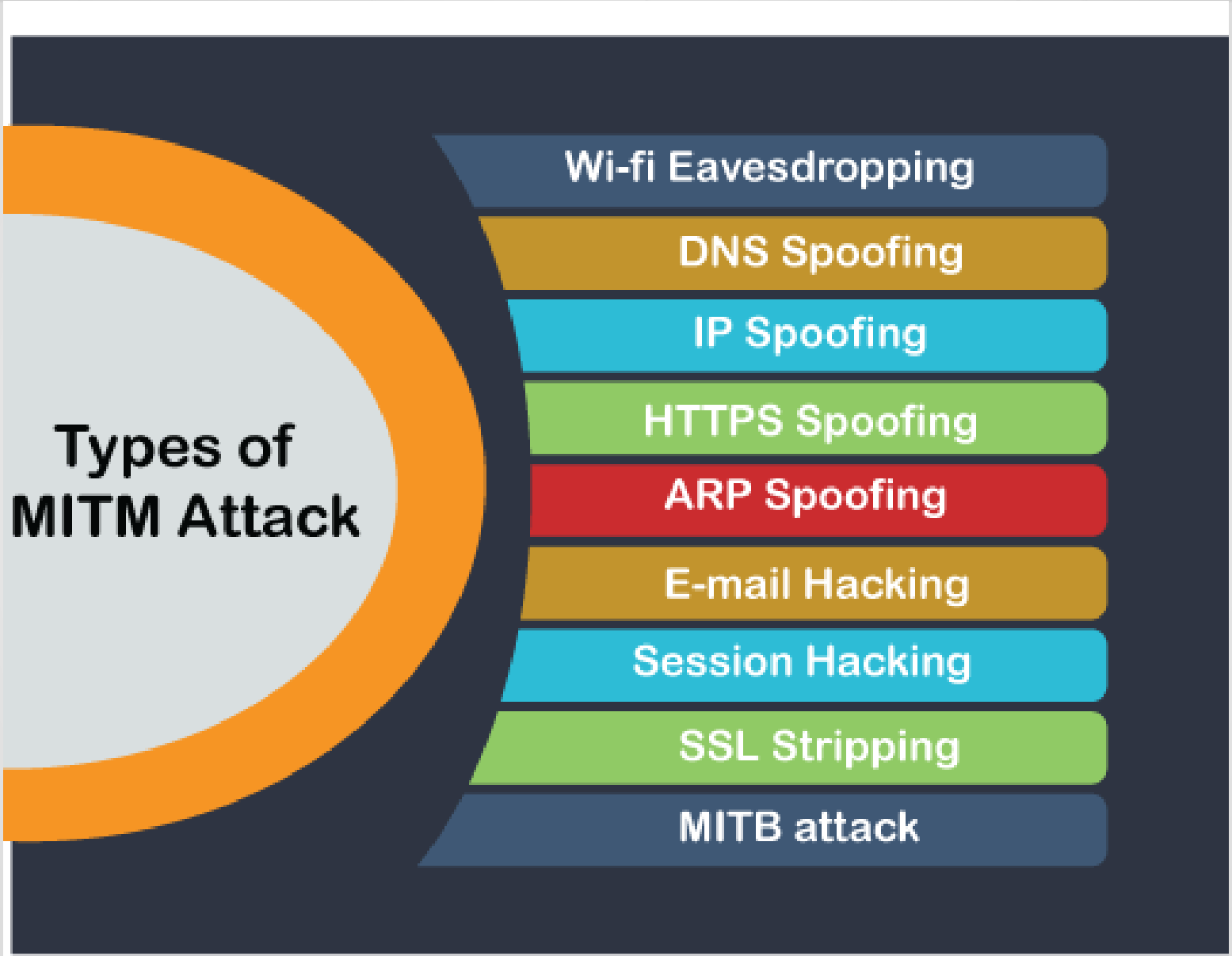
Man in the middle attacks(MITM)

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

MIMT


HOW MAN IN THE MIDDLE ATTACKS WORK
ORIGINAL CONNECTION
NEW CONNECTION
NEW CONNECTION
USER/VICTIM
MAN IN THE MIDDLE
WEB APPLICATION

MIMT



https://www.javatpoint.com/cyber-security-mitm-attacks

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

Web-based attacks

Adware − Adware, also known as freeware or pitchware, is a free computer software that contains commercial advertisements of games, desktop toolbars, and utilities. It is a web-based application and it collects web browser data to target advertisements, especially pop-ups.

Spyware − Spyware is infiltration software that anonymously monitors users which enables a hacker to obtain sensitive information from the user's computer. Spyware exploits users and application vulnerabilities that is quite often attached to free online software downloads or to links that are clicked by users.

Ransomware - is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them

Web-based attacks

Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

Backdoors

It is a method that **bypasses the normal authentication process**. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

Web-based attacks

Rootkit − A rootkit is a software used by a hacker to gain admin level access to a computer/network which is installed through a stolen password or by exploiting a system vulnerability without the victim's knowledge.

Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Web-based attacks

KeyLoggers:
Traditionally, Keyloggers are software that monitor user activity such as keys typed using keyboard.

Modern keyloggers can,

- Record keystrokes on keyboard
- Record mouse movement and clicks
- Record menus that are invoked
- Take screenshots of the desktop at predefined intervals

Security Technologies

1.Firewalls

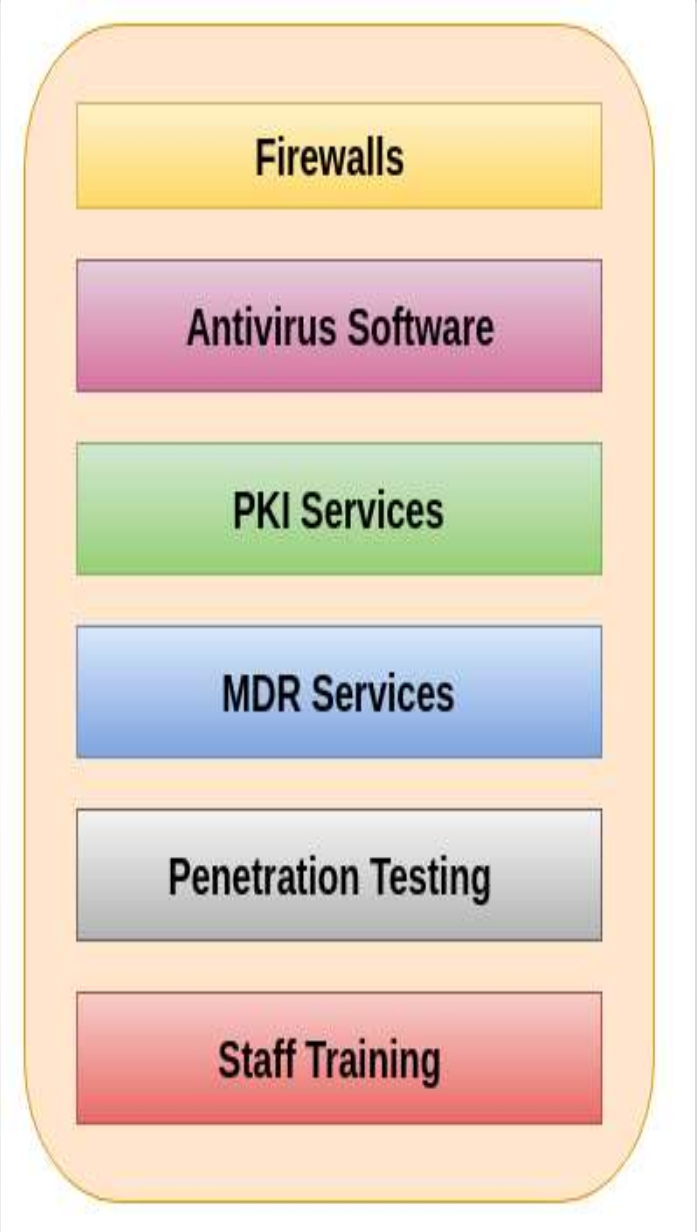
2. Antivirus Software

3. PKI Services (Public Key Infrastructure)

4. Managed Detection and Response Service (MDR)

5. Penetration Testing

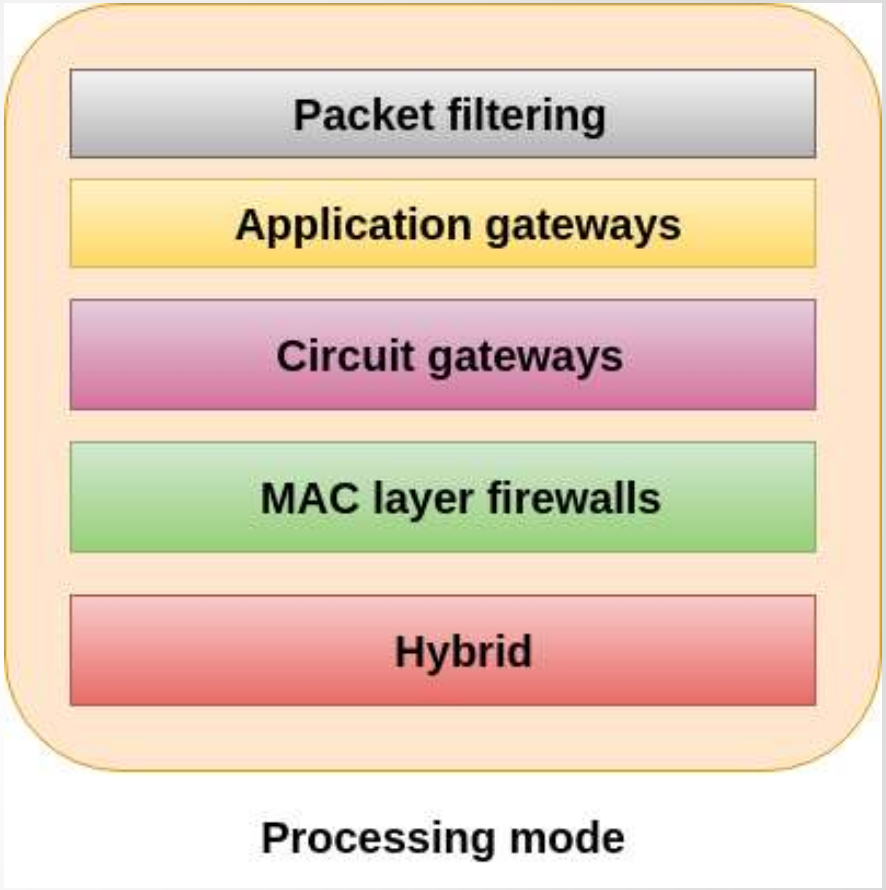
6. Staff Training



Security Technologies

Firewall

Firewall is a computer network security system designed to prevent unauthorized access to or from a private network. It can be implemented as hardware, software, or a combination of both. Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages are entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those that do not meet the specified security criteria.



Security Technologies

Intrusion Detection System (IDS)

An IDS is a security system which monitors the computer systems and network traffic.

It analyses that traffic for possible hostile attacks originating from the outsider and also for system misuse or attacks originating from the insider.

A firewall does a job of filtering the incoming traffic from the internet, the IDS in a similar way compliments the firewall security. Like, the firewall protects an organization sensitive data from malicious attacks over the Internet, the Intrusion detection system alerts the system administrator in the case when someone tries to break in the firewall security and tries to have access on any network in the trusted side.

Security Technologies

Access Control

Access control is a process of selecting restrictive access to a system. It is a concept in security to minimize the risk of unauthorized access to the business or organization.

In this, users are granted access permission and certain privileges to a system and resources. Here, users must provide the credential to be granted access to a system. These credentials come in many forms such as password, keycard, the biometric reading, etc. Access control ensures security technology and access control policies to protect confidential information like customer data.

The access control can be categories into two types-

- Physical access control
- Logical access control

Security Technologies

Encoding and Decoding

Encoding is the process of putting a sequence of characters such as letters, numbers and other special characters into a specialized format for efficient transmission.

Decoding is the process of converting an encoded format back into the original sequence of characters. It is completely different from Encryption which we usually misinterpret.

Encoding should NOT be used for transporting sensitive information.

Cryptography is useful tool for securing data, communications, and code globs, but it's no silver bullet.

Security Technologies

Security orchestration, automation and response (SOAR) software solutions combine the functionality of security tools and add intelligent automation functionality to improve a security operations team's ability to tackle threats in real time with minimal manual labour.

User and entity behaviour analytics (UEBA) software and zero trust networking solutions are designed to detect threats in real time. These tools all use behaviour-based analytics to identify strange behaviours and misuse within a network.

Digital Signature

A digital signature is a **mathematical technique** which validates the authenticity and integrity of a message, software or digital documents. It allows us to verify the author name, date and time of signatures, and authenticate the message contents. The digital signature offers far more inherent security and intended to solve the problem of tampering and impersonation (Intentionally copy another person's characteristics) in digital communications.

Algorithms in Digital Signature

A digital signature consists of three algorithms:

1. Key generation algorithm

The key generation algorithm selects private key randomly from a set of possible private keys. This algorithm provides the private key and its corresponding public key.

2. Signing algorithm

A signing algorithm produces a signature for the document.

3. Signature verifying algorithm

A signature verifying algorithm either accepts or rejects the document's authenticity.

Threat to E-Commerce

Threat to E-Commerce

In **e-cash**, we stored financial information on the electronic device or on the internet which is vulnerable to the hackers. Some of the major threats related to e-cash system are-

E-cash Threats

Threat to E-Commerce

Backdoors Attacks

It is a type of attacks which gives an attacker to unauthorized access to a system by bypasses the normal authentication mechanisms. It works in the background and hides itself from the user that makes it difficult to detect and remove.

Denial of service attacks

A denial-of-service attack (DoS attack) is a security attack in which the attacker takes action that prevents the legitimate (correct) users from accessing the electronic devices. It makes a network resource unavailable to its intended users by temporarily disrupting services of a host connected to the Internet.

Direct Access Attacks

Direct access attack is an attack in which an intruder gains physical access to the computer to perform an unauthorized activity and installing various types of software to compromise security. These types of software loaded with worms and download a huge amount of sensitive data from the target victims.

Threat to E-Commerce

Eavesdropping

This is an unauthorized way of listening to private communication over the network. It does not interfere with the normal operations of the targeting system so that the sender and the recipient of the messages are not aware that their conversation is tracking.

Credit/Debit card fraud

A credit card allows us to borrow money from a recipient bank to make purchases. The issuer of the credit card has the condition that the cardholder will pay back the borrowed money with an additional agreed-upon charge.

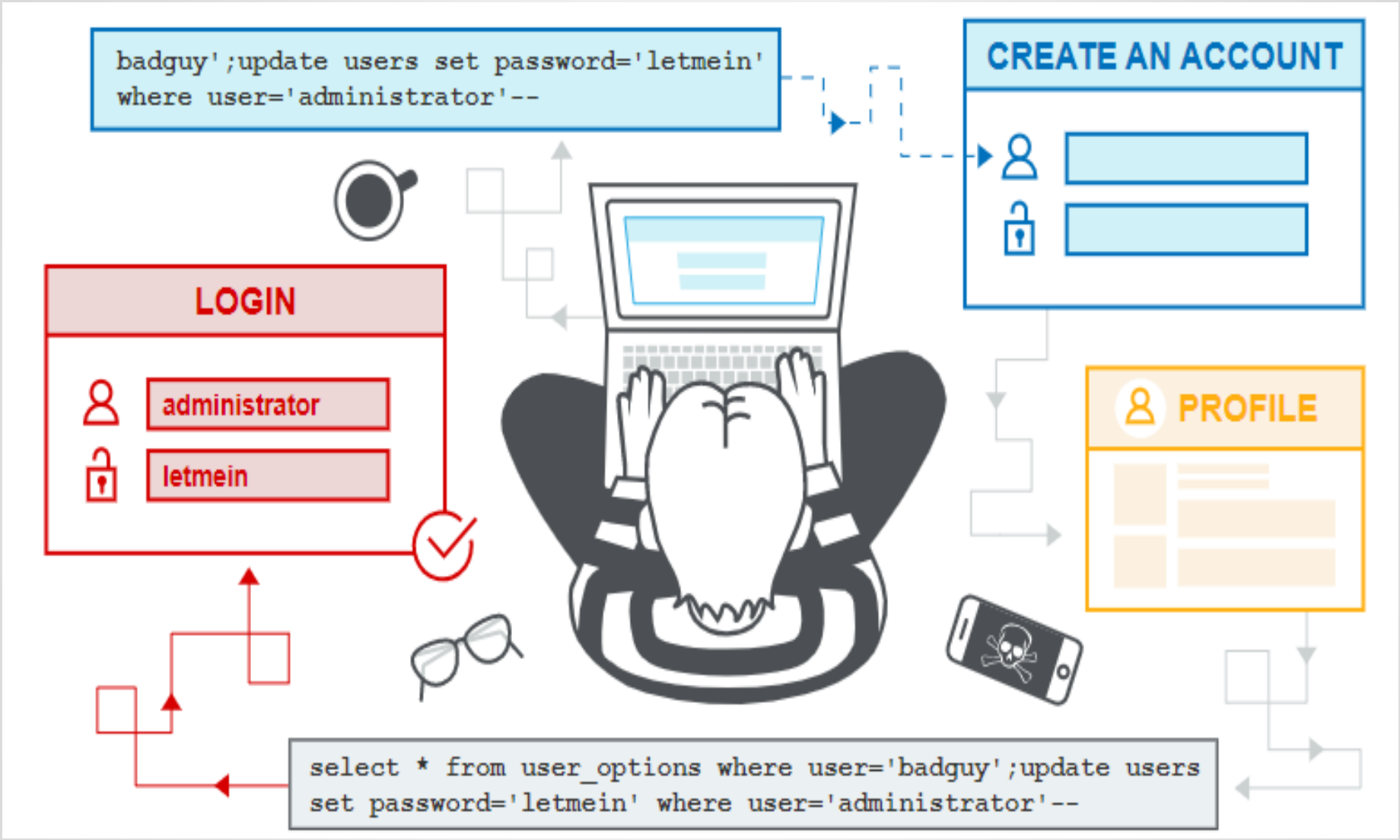
Web Application - Injection

Injection technique consists of **injecting a SQL query** or a command using the input fields of the application.

A successful SQL injection can read, modify sensitive data from the database, and can also delete data from a database. It also enables the hacker to perform administrative operations on the database such as shutdown the DBMS/dropping databases.

Blind SQL injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.

Web Application - Injection



Web Application - Injection

```
String query = "SELECT * FROM EMP WHERE EMPID = '" + request.getParameter("id") + "'";
```

Step 1 − Navigate to the SQL Injection area of the application.

Step 2 − Here, we use String SQL Injection to bypass authentication. Use SQL injection to log in as the boss ('Neville') without using the correct password. Verify that Neville's profile can be viewed and that all functions are available (including Search, Create, and Delete).

Step 3 − We will Inject a SQL such that we are able to bypass the password by sending the parameter as 'a' = 'a' or 1 = 1. The SQL above is valid and will return ALL rows from the “EMP" table, since OR 1=1 is always TRUE.

Step 4 − Post Exploitation, we are able to login as Neville who is the Admin

Web Application - Injection

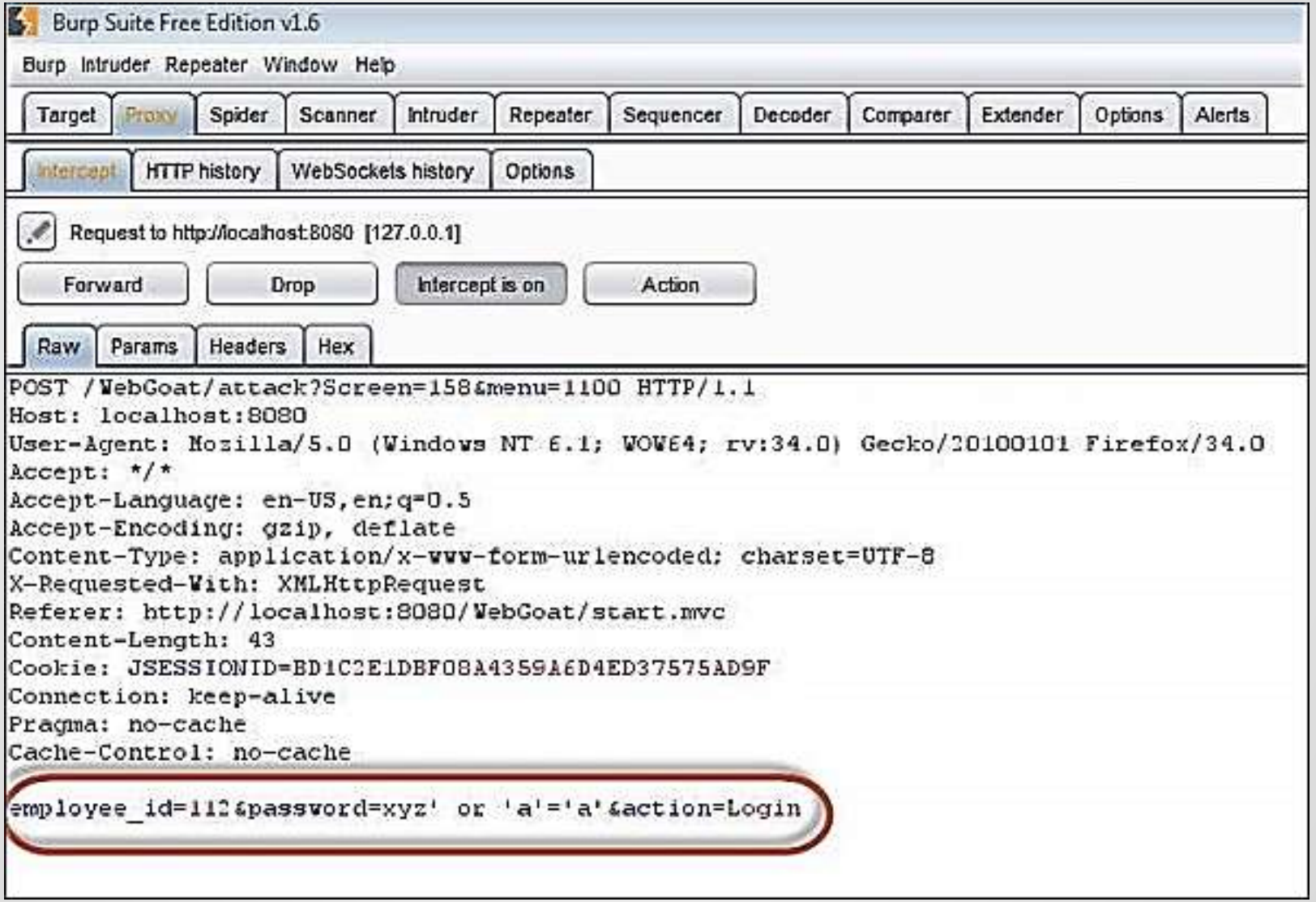
Preventing SQL Injection
There are plenty of ways to prevent SQL injection.

When developers write the code, they should ensure that they handle special characters accordingly. There are cheat sheets/prevention techniques available from OWASP(Open Web Application Security Project) which is definitely a guide for developers.

- Using Parameterized Queries
- Escaping all User Supplied Input
- Enable Least Privilege for the database for the end users

Web Application - Injection

String query = "SELECT * FROM EMP WHERE EMPID = '" + request.getParameter("id") + "'";



Web Application - Injection

String query = "SELECT * FROM EMP WHERE EMPID = '" + request.getParameter("id") + "'";

Source Code Analyzers

Free Source Code Analysers

- OWASP Orizon
- OWASP O2
- SearchDiggity
- FXCOP
- Splint
- Boon
- W3af
- FlawFinder

Commercial Source Code Analysers

- Parasoft C/C++ test
- HP Fortify
- Appscan
- Armorize CodeSecure
- GrammaTech

Are you a software Engineer ?

Thanks to All