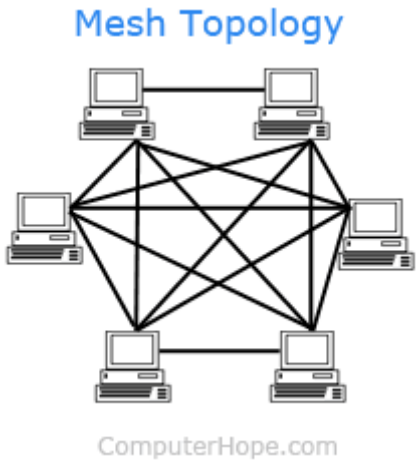
# SAMPLE PAPER 1

**1. Discuss Mesh Topology.**

A mesh topology is a network setup where each computer and network device is interconnected with one another. This topology setup allows for most transmissions to be distributed even if one of the connections goes down. It is a topology commonly used for wireless networks. Below is a visual example of a simple computer setup on a network using a **mesh topology**.




**2. What is DMZ?**

In computer networks, a DMZ, or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet. DMZs are also known as *perimeter networks* or *screened subnetwork*s.

Any service provided to users on the public internet should be placed in the DMZ network. External-facing servers, resources and services are usually located there. Some of the most common of these services include web, email, domain name system, File Transfer Protocol and proxy servers.

Servers and resources in the DMZ are accessible from the internet, but the rest of the internal LAN remains unreachable. This approach provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data from the internet.

**3. Explain XSRF attack.**

An attacker's aim for carrying out a CSRF attack is to force the user to submit a state-changing request. Examples include:

- Submitting or deleting a record.
- Submitting a transaction.
- Purchasing a product.
- Changing a password.
- Sending a message.

Social engineering platforms are often used by attackers to launch a CSRF attack. This tricks the victim into clicking a URL that contains a maliciously crafted, unauthorized request for a particular Web application. The user's browser then sends this maliciously crafted request to a targeted Web application. The request also includes any credentials related to the particular website (e.g., user session cookies). If the user is in an active session with a targeted Web application, the application treats this new request as an authorized request submitted by the user. Thus, the attacker succeeds in exploiting the Web application's CSRF vulnerability.

**4. List types of Bluetooth attacks**

**1. Bluebugging**

Through this Bluetooth attack, hackers can:

- Eavesdrop on phone calls by gaining access to a device.
- Connect themselves to the user's Internet.
- Receive and send text messages and emails.
- Make calls, when the owner of the device is unaware of it.

This kind of attack generally happens in **phones with older models**.

**2. Bluejacking**

Bluejacking is not as serious as the other Bluetooth attacks.

It is a common and harmless attack that was earlier used to prank people.

Through this, the hacker can only send text messages to the hacked device. It doesn't give them access to your smartphone or the data in it.

So, to tackle this problem, keep your Bluetooth **settings non-discoverable or invisible**, or just ignore the received messages.

**3. Bluesnarfing**

Out of the different types of Bluetooth attacks, this is one of the most **dangerous**.

When hackers are within 300 feet of a device, they can conduct a bluesnarfing attack (around 90 meters).

This happens because, even if your device is set to non-discoverable mode, hackers can still attack and access your personal information.

They can also copy the data on your device, including your photos and videos, phone number, contact list, emails, and passwords.

Thus, keep your Bluetooth in **invisible mode**. Since it makes it difficult for hackers to figure out the model and name of your device.

**5. Location Tracking**

This attack is one of the different types of Bluetooth attacks that occur on locating and tracking devices.

**Fitness lovers** are more vulnerable to this attack since their fitness devices are always linked to their Bluetooth.

**5. Describe GSM algorithms**

GSM uses three different security algorithms called **A3, A5, and A8**. In practice, A3 and A8 are generally implemented together (known as A3/A8). An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centers.

**6. What it scripting language? Explain its types.**

All scripting languages are programming languages. The scripting language is basically a language where instructions are written for a run time environment. They do not require the compilation step and are rather interpreted. It brings new functions to applications and glue complex system together. A scripting language is a programming language designed for integrating and communicating with other programming languages.

There are many scripting languages some of them are discussed below:

- **bash:** It is a scripting language to work in the Linux interface. It is a lot easier to use bash to create scripts than other programming languages.
- **Node js:** It is a framework to write network applications using **JavaScript**. Corporate users of Node.js include IBM, LinkedIn, Microsoft, Netflix, PayPal, Yahoo for real-time web applications.
- **Ruby:** Its flexibility has allowed to create innovative software.
- **Perl:** A scripting language with innovative features to make it different and popular. Found on all windows and Linux servers

## 7. What is CAPTCHA and how does it work?

CAPTCHA stands for the Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHAs are tools you can use to differentiate between real users and automated users, such as bots. CAPTCHAs provide challenges that are difficult for computers to perform but relatively easy for humans.

Classic CAPTCHAs, which are still in use on some web properties today, involve asking users to identify letters. The letters are distorted so that bots are not likely to be able to identify them. To pass the test, users have to interpret the distorted text, type the correct letters into a form field, and submit the form. If the letters don't match, users are prompted to try again. Such tests are common in login forms, account signup forms, online polls, and e-commerce checkout pages.

## 8. How input injection attack is performed? Explain all methods.

During an injection attack, an attacker can provide malicious input to a web application (inject it) and change the operation of the application by forcing it to execute certain commands.

An injection attack can expose or damage data and lead to a denial of service or a full webserver compromise. Such attacks are possible due to vulnerabilities in the code of an application that allows for unvalidated user input.

SQL Injection (SQLi): SQL is a query language to communicate with a database. It can be used to perform actions to retrieve, delete and save data in the database.

Cross-Site Scripting (XSS): Whenever an application allows user input within the output it generates, it allows an attacker to send malicious code to a different end-user without validating or encoding it. XSS takes these opportunities to inject malicious scripts into trusted websites.

Code Injection: In this scenario, an attacker is acquainted with the application code and programming language. By exploiting a vulnerability, they may attempt to inject code into the application to be executed as a command by its web server.

CCS Injection: A CCS injection exploits a vulnerability found in the Change Cipher Spec processing in some versions of OpenSSL.

SMTP/IMAP, Host Header Injection, LDAP Injection and CRLF Injection.

**9. Explain different session hijacking and fixation techniques. How session hijacking is done?**

Active Session Hijacking : An Active Session Hijacking occurs when the attacker takes control over the active session. The actual user of the network becomes in offline mode, and the attacker acts as the authorized user. They can also take control over the communication between the client and the server.

Passive Session Hijacking : In Passive Session Hijacking, instead of controlling the overall session of a network of targeted user, the attacker monitors the communication between a user and a server.

Hybrid Hijacking : The combination of Active Session Hijacking and Passive Session Hijacking is referred to as Hybrid Hijacking. In this the attackers monitors the communication channel (the network traffic), whenever they find the issue, they take over the control on the web session and fulfill their malicious tasks.

Session Hijacking. Those methods are:

1. Brute Forcing the Session ID
2. Cross-Site Scripting (XSS) or Misdirected Trust
3. Man in the browser
4. Malware infections
5. Session Fixation
6. Session side-jacking

**10. Discuss encryption process of mono-alphabetic cipher working.**

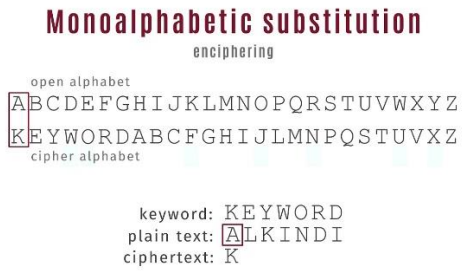
The substitution cipher is the oldest forms of encryption algorithms according to creates each character of a plaintext message and require a substitution process to restore it with a new character in the ciphertext.

This substitution method is deterministic and reversible, enabling the intended message recipients to reverse-substitute ciphertext characters to retrieve the plaintext.

The specific form of substitution cipher is the Monoalphabetic Substitution Cipher, is known as “Simple Substitution Cipher”. Monoalphabetic Substitution Ciphers based on an individual key mapping function K, which consistently replaces a specific character α with a character from the mapping K (α).

A mono-alphabetic substitution cipher is a type of substitution ciphers in which the equivalent letters of the plaintext are restored by the same letters of the ciphertext. Mono, which defines one, it signifies that each letter of the plaintext has a single substitute of the ciphertext.

Caesar cipher is a type of Monoalphabetic cipher. It uses the similar substitution method to receive the cipher text characters for each plain text character. In Caesar cipher, it can see that it is simply for a hacker to crack the key as Caesar cipher supports only 25 keys in all. This pit is covered by utilizing Monoalphabetic cipher.




**Differentiate between all topologies along with advantages.**

Bus topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.

Advantages of Bus topology:

Low-cost cable, Familiar technology, Moderate data speeds and Limited failure.

Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.

Advantages of Ring topology

Network Management, Product availability, Cost and Reliable.

Star Topology

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.

Advantages of Star Topology

Efficient troubleshooting, Network control, Limited Failure, Familiar Technology, Easily Expandable, Cost Effective and High Data Speeds.

Tree Topology

- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.

Advantages

Support for broadband transmission, Easily expandable, Easily manageable, Error detection Limited failure, Point-to-point wiring

Mesh Technology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.

Advantages

Reliable, Fast Communication and Easier Reconfiguration.

Hybrid Technology

- The combination of various different topologies is known as Hybrid topology.
- A Hybrid topology is a connection between different links and nodes to transfer the data.

Advantages

Reliable, Scalable, Flexible and Effective.

**11.Explain remote server security attacks? Explain all methods? Explain mitigations.**

An attacker could breach a system via remote access by:

- Scanning the Internet for vulnerable IP addresses.
- Running a password-cracking tool.

- Simulating a remote access session with cracked username and password information.

Once inside the system, the attacker may upload malware, copy all sensitive data, and use the compromised system to attack other computers or network within the same environment. The malware will continue to steal data even after the attacker logs out and may go undetected for a long period of time.

**DoS attacks**

DoS, or Denial of Service, is an attempt to make a computer or network unavailable for its intended users.

**DNS Poisoning**

Using DNS (Domain Name Server) poisoning, hackers can trick the DNS server of any computer into believing that fake data is legitimate and authentic.

**Port scanning**

Port scanning is used to determine which computer ports are open on a network host. A port scanner is software designed to find such ports.

**TCP desynchronization**

TCP desynchronization is a technique used in TCP Hijacking attacks. It is triggered by a process in which the sequential number in incoming packets differs from the expected sequential number.

**SMB Relay**

SMB Relay and SMBRelay2 are special programs that are capable of carrying out attacks against remote computers.

**ICMP attacks**

ICMP (Internet Control Message Protocol) is a popular and widely-used Internet protocol. It is used primarily by networked computers to send various error messages.

Mitigation, or Attack Mitigation, is the reduction in severity or seriousness of an event. In cybersecurity, mitigation is centered around strategies to limit the impact of a threat against data in custody.

Threats against data can come from outside attackers motivated by profit, activism, retribution, or mischief. Insider threats may have the same motives but could be tied to workplace issues resulting in people abusing their access privileges to inflict harm.

In either case, it is the responsibility of a data owner to protect data from misuse, disclosure, theft, unauthorized exposure, wrongful transmission, and so on while still making the data useful and available to conduct business. To that end, a mitigation strategy should be strict in accordance with risk appetites and realistic enough to allow for the licit use of the data by those authorized.

## A. 12. How CSS attack is performed? Explain methods and solutions.

To carry out a cross site scripting attack, an attacker injects a malicious script into user-provided input. Attackers can also carry out an attack by modifying a request. If the web app is vulnerable to XSS attacks, the user-supplied input executes as code. For example, in the request below, the script displays a message box with the text "xss."

*http://www.site.com/page.php?var=<script>alert('xss');</script>*

There are many ways to trigger an XSS attack. For example, the execution could be triggered automatically when the page loads or when a user hovers over specific elements of the page (e.g., hyperlinks).

Potential consequences of cross site scripting attacks include these:

- Capturing the keystrokes of a user.
- Redirecting a user to a malicious website.
- Running web browser-based exploits (e.g., crashing the browser).
- Obtaining the cookie information of a user who is logged into a website (thus compromising the victim's account).

**Stored XSS.** Takes place when the malicious payload is stored in a database. It renders to other users when data is requested—if there is no output encoding or sanitization.

**Reflected XSS.** Occurs when a web application sends attacker-provided strings to a victim's browser so that the browser executes part of the string as code. The payload echoes back in response since it doesn't have any server-side output encoding.

**DOM-based XSS.** Takes place when an attacker injects a script into a response. The attacker can read and manipulate the document object model (DOM) data to craft a malicious URL. The attacker uses this URL to trick a user into clicking it.

**Solutions**

- Never trust user input.
- Implement output encoding.
- Perform user input validation.
- Follow the defense in depth principle.
- Ensure that web application development aligns with OASP's XSS Prevention Cheat Sheet.
- After remediation, perform penetration testing to confirm it was successful.

## a) How XML attack is performed? Explain methods and solutions.

XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access.

In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure, by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.

- Exploiting XXE to retrieve files, where an external entity is defined containing the contents of a file, and returned in the application's response.
- Exploiting XXE to perform SSRF attacks, where an external entity is defined based on a URL to a back-end system.
- Exploiting blind XXE exfiltrate data out-of-band, where sensitive data is transmitted from the application server to a system that the attacker controls.
- Exploiting blind XXE to retrieve data via error messages, where the attacker can trigger a parsing error message containing sensitive data.

**Solutions**

**Leveraging Automation for Identification of XXE**

A majority of XXE vulnerabilities are identified reliably, swiftly, and accurately by an intelligent, automated, and hassle-free web application scanner backed with Global Threat Intelligence.

**Application Security Testing Performed by Security Experts**

Some kinds of XML External Entities are not identified by automated web scanning tools such as blind XXE, file retrievals, and XInclude attacks.

**Managed WAF with Custom-Defined Rules**

Traditional WAFs are bypassed rather easily by attackers exploiting the XXE vulnerabilities in the application.

**Disabling DTD Support**

External DTD is designed to be utilized by trusted parties. However, it is a legacy feature and often, leveraged by malicious actors to attack web applications.

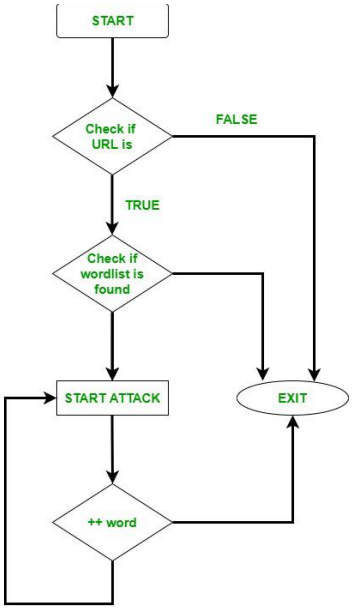
# SAMPLE PAPER 2

**1. Define directory traversal attack.**

Properly controlling access to web content is crucial for running a secure web server. Directory traversal or Path Traversal is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory.

Web servers provide two main levels of security mechanisms

- Access Control Lists (ACLs)
- Root directory




An Access Control List is used in the authorization process. It is a list which the web server's administrator uses to indicate which users or groups are able to access, modify or execute particular files on the server, as well as other access rights.

**Advantages**

1. DirBuster provides a GUI interface, which is obviously very easy to understand and use. DirBuster is often employed by anyone with no hustle.
2. As compared to other Directory Brute-forcing tools, GoBuster is extremely fast. GoBuster has been developed in the Go language & This language is known for speed.

**2. How buffer overflow is used to perform malicious activities?**

Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.

If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

**Types of Buffer Overflow Attacks**

**Stack-based buffer overflows** are more common, and leverage stack memory that only exists during the execution time of a function.

**Heap-based attacks** are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

In addition, modern operating systems have runtime protection. Three common protections are:

- **Address space randomization (ASLR)**—randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.
- **Data execution prevention**—flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.
- **Structured exception handler overwrite protection (SEHOP)**—helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions.

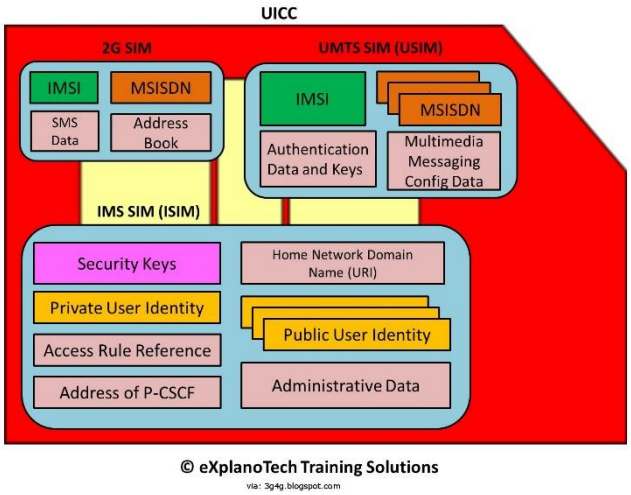
**3. Explain SIM/UICC Security**.

The Universal Integrated Circuit Card (UICC) is a type of SIM card, a smart card used for mobile terminals/phones utilizing GSM or UMTS networks. The UICC is used to ensure the security and integrity of all kinds of personal data as well as hold information that identifies the user to the wireless operator in order for the latter to know the plans and services associated with the card.

The UICC is a type of smart card technology that has its own processor, software and data storage; so, it is essentially a computer in and of itself. It is essentially an evolution of the subscriber identification module (SIM) card, and, as such, it contains many of the latter's features, such as storing contact details and maintaining a list of preferred networks.

Since the card slot is standardized, a subscriber can easily move their wireless account and phone number from one handset to another. This will also transfer their phone book and text messages. Similarly, usually a subscriber can change carriers by inserting a new carrier's UICC card into

their existing handset. However, it is not always possible because some carriers (e.g., in U.S.) SIM-lock the phones that they sell, preventing rival carriers' cards from being used.




## 4. What is browser exploit?

In cybersecurity, an exploit is a piece of code that utilizes vulnerabilities in computer software or hardware in order to perform malicious actions. These actions may include gaining control of a device, infiltrating a network, or launching some form of cyber attack. A browser exploit is a type of exploit that takes advantage of a web browser vulnerability in order to breach web browser security.

A browser exploit is a form of malicious code that takes advantage of a flaw or vulnerability in an operating system or piece of software with the intent to breach browser security to alter a user's browser settings without their knowledge. Malicious code may exploit ActiveX, HTML, images, Java, JavaScript, and other Web technologies and cause the browser to run arbitrary code.

Prevention

**Install firewall software and other security software**

**Keep all software up to date**

**Be careful when browsing the web, especially when downloading files**

**Don’t click on suspicious attachments or links in emails**

**Use a more secure browser, or remote browser isolation**

## 5. What are canonicalization attacks?

A canonicalization attack is a cyberattack method in which the attacker substitutes various inputs for the canonical name of a path or file.

Canonicalization is the process of mapping inputs to their canonical equivalent. It is often used for cryptographic algorithms and data that are intended to be secured from tampering, usually by hashing. In computer security, a Canonicalization attack aims to find or compute the mapping between two different inputs which produce the same output when processed by a given system.

This attack then seeks ways to manipulate input strings so they both result in an undesired output (such as "war" which can be manipulated into each other by changing just one character). With some algorithms such as MD5, even minor changes in input will result in enormous differences in hash values, making this type of attack relatively easy. A Canonicalization attack is a type of specific-pattern attack.

Key Points:

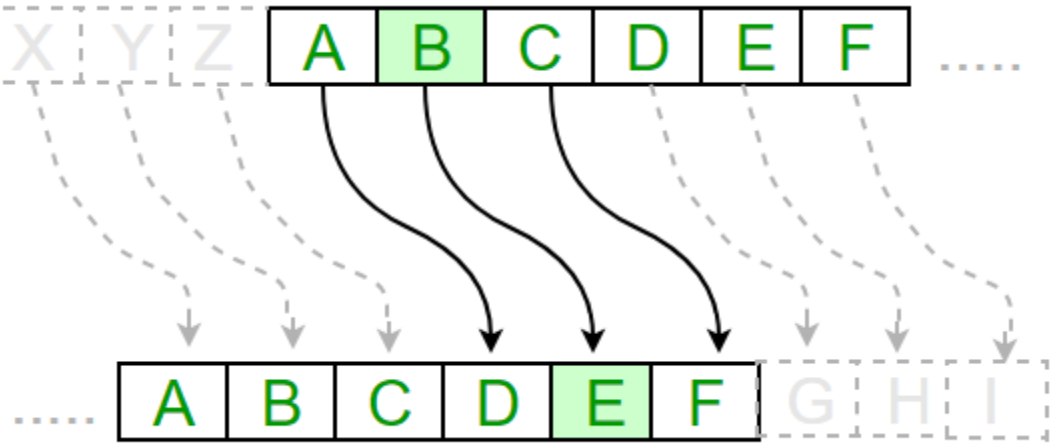
- This technique is used to steal a victim's data from the server.
- The attacker first creates a domain, usually at different TLDs, for example: .com, .co.uk or .info etc. Then registers a website with that domain name, and finally publishes links to the site from various social media or different blogs around the internet so that it will appear on search engines' results pages for certain keywords searched by users.
- The attacker then waits for users who arrive at their fake site and enter their username/password in order to complete an action (e.g., perform a payment).
- In the case of a payment operation, users would be redirected to the real website of cybercriminals, where they would complete the operation and then immediately be redirected back to the fake website through a cryptocurrency mining script.
- A user can visit any malicious site that is using this technique. Such sites may appear in search engines and social media results, but not on legitimate results pages. The only way to know if it's safe to enter information on such websites is to check for certificate errors: If it gives one, then it's fake.

## 6. Explain Creaser cipher with an example.

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.

For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.




**Text** : ABCDEFGHIJKLMNOPQRSTUVWXYZ
**Shift**: 23
**Cipher**: XYZABCDEFGHIJKLMNOPQRSTUVW

**Text** : ATTACKATONCE
**Shift**: 4
**Cipher**: EXXEGOEXSRGI

**Algorithm for Caesar Cipher:**
**Input:**

1. A String of lower case letters, called Text.
2. An Integer between 0-25 denoting the required shift.

**Procedure:**

- Traverse the given text one character at a time .
- For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
- Return the new string generated.

## 7. Explain encryption and decryption process of Monoalphabetic cipher with an example

### Monoalphabetic and Polyalphabetic Cipher

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.

All of the substitution ciphers we have discussed earlier in this chapter are monoalphabetic; these ciphers are highly susceptible to cryptanalysis.

Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process. The next two examples, **playfair and Vigenere Cipher are polyalphabetic ciphers**.

The substitution cipher is the oldest forms of encryption algorithms according to creates each character of a plaintext message and require a substitution process to restore it with a new character in the ciphertext.

This substitution method is deterministic and reversible, enabling the intended message recipients to reverse-substitute ciphertext characters to retrieve the plaintext.

The specific form of substitution cipher is the Monoalphabetic Substitution Cipher, is known as "Simple Substitution Cipher". Monoalphabetic Substitution Ciphers based on an individual key mapping function K, which consistently replaces a specific character α with a character from the mapping K (α).

A mono-alphabetic substitution cipher is a type of substitution ciphers in which the equivalent letters of the plaintext are restored by the same letters of the ciphertext. Mono, which defines one, it signifies that each letter of the plaintext has a single substitute of the ciphertext.

Caesar cipher is a type of Monoalphabetic cipher. It uses the similar substitution method to receive the cipher text characters for each plain text character. In Caesar cipher, it can see that it is simply for a hacker to crack the key as Caesar cipher supports only 25 keys in all. This pit is covered by utilizing Monoalphabetic cipher.

In Monoalphabetic cipher, the substitute characters symbols supports a random permutation of 26 letters of the alphabet. 26! Permutations of the alphabet go up to 4*10^26. This creates it complex for the hacker to need brute force attack to gain the key.

Mono-alphabetic cipher is a type of substitution where the relationship among a symbol in the plaintext and a symbol in the cipher text is continually one-to-one and it remains fixed throughout the encryption process.

These ciphers are considered largely susceptible to cryptanalysis. For instance, if 'T' is encrypted by 'J' for any number of appearance in the plain text message, then 'T' will continually be encrypted to 'J'.

If the plaintext is "TREE", thus the cipher text can be "ADOO" and this showcases that the cipher is possibly mono-alphabetic as both the "O"s in the plaintext are encrypted with "E"s in the cipher text.

Although the hacker will not be capable to need brute force attack, it is applicable for consider the key by using the All- Fearsome Statistical Attack. If the hacker understand the characteristics of plaintext of any substitution cipher, then regardless of the size of the key space, it can simply break the cipher using statistical attack. Statistical attack includes measuring the frequency distribution for characters, comparing those with same statistics for English.

**8. Discuss polyalphabetic algorithm with example.**

A poly-alphabetic cipher is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters are enciphered differently based upon their installation in the text. Rather than being a one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes.

For example, ‘a’ can be enciphered as ‘d’ in the starting of the text, but as ‘n’ at the middle. The polyalphabetic ciphers have the benefit of hiding the letter frequency of the basic language. Therefore attacker cannot use individual letter frequency static to divide the ciphertext.

The first Polyalphabetic cipher was the Alberti Cipher which was introduced by Leon Battista Alberti in the year 1467. It used a random alphabet to encrypt the plaintext, but at different points and it can change to a different mixed alphabet, denoting the change with an uppercase letter in the cipher text.

It can utilize this cipher, Alberti used a cipher disc to display how plaintext letters are associated to cipher text letters. In this cipher, each ciphertext character based on both the corresponding plaintext character and the position of the plaintext character in the message.

As the name polyalphabetic recommend this is achieved by using multiple keys rather than only one key. This implies that the key should be a stream of subkeys, in which each subkey depends somehow on the position of the plaintext character that needs subkey for encipherment.

In other words, it is required to have s key stream k = ($K_1$, $K_2$, $K_3$ ...) in which $K_i$ is used to encipher the ith character in the plaintext to make the $i^{th}$ character in the ciphertext. The best known and simplest of such algorithm is defined as Vigenere cipher.

Vigenere cipher is one of the simplest and popular algorithms in polyalphabetic cipher. In this approach, the alphabetic text is encrypted using a sequence of multiple Caesar ciphers based on the letters of a keyword.

The Caesar cipher restoring each letter in the plaintext with the letters standing constant position to the right in the alphabet. This shift is implemented modulo 26. For instance, in a Caesar cipher of shift 3, A can become D, B can become E and so on.

The Vigenère cipher includes several simple substitution ciphers in sequence with several shift values. In this cipher, the keyword is repeated just before it connects with the duration of the plaintext.

Encryption is implemented by going to the row in the table correlating to the key, and discover the column heading the corresponding letter of the plaintext character; the letter at the intersection of corresponding row and column of the Vigenere Square create the ciphertext character. The rest of the plaintext is encrypted in the similar method.

**9. What types of attacks are performed on Apache server? Explain each with their countermeasures.**

**How Security Disasters Develop**

The scenarios you'll face are the following:

- Intruders gaining simple access
- Denial of service
- Defacement or total system seizure

Let's run through the factors that invite these situations.

**Intruders Gaining Simple Access**

Simple unauthorized access can happen in several ways:

- Insiders who once had authorized access (former employees or developers, for example) return to haunt you.
- Your users make bad password choices on other networks that fall to hackers. This leads to cross-network unauthorized access.
- Your underlying operating system has holes, and diligent hackers exploit it to gain limited access.
- The tools you use in conjunction with Apache are flawed.

Denial-of-Service (DoS) / Distributed Denial-of-service (DDoS)

- Reduce Attack Surface Area
- Plan for Scale
- Know what is normal and abnormal traffic
- Deploy Firewalls for Sophisticated Application attacks

Web Defacement Attack

- **Avoid common web vulnerabilities**
- **Secure your database**
- **Secure your source code**

SSH Brute Force Attack.

- Don't allow root to login
- Don't allow ssh passwords (use private key authentication)
- Don't listen on every interface

Cross-site scripting (XSS)

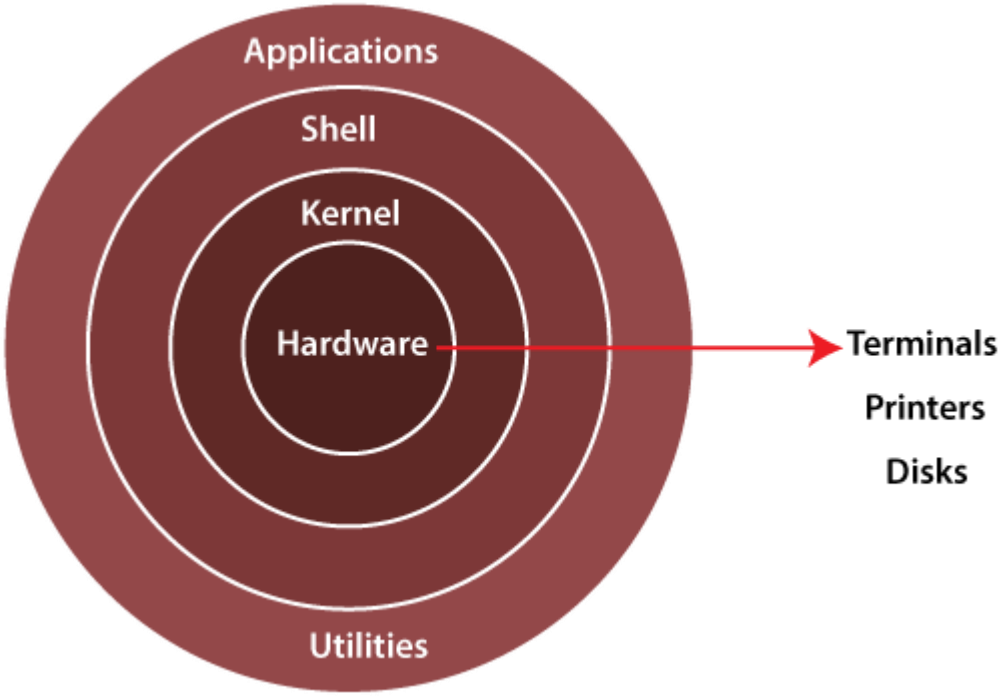
1. Blacklist filtering.
2. Whitelist filtering.
3. Contextual Encoding.
4. Input Validation.
5. Content Security Policy.

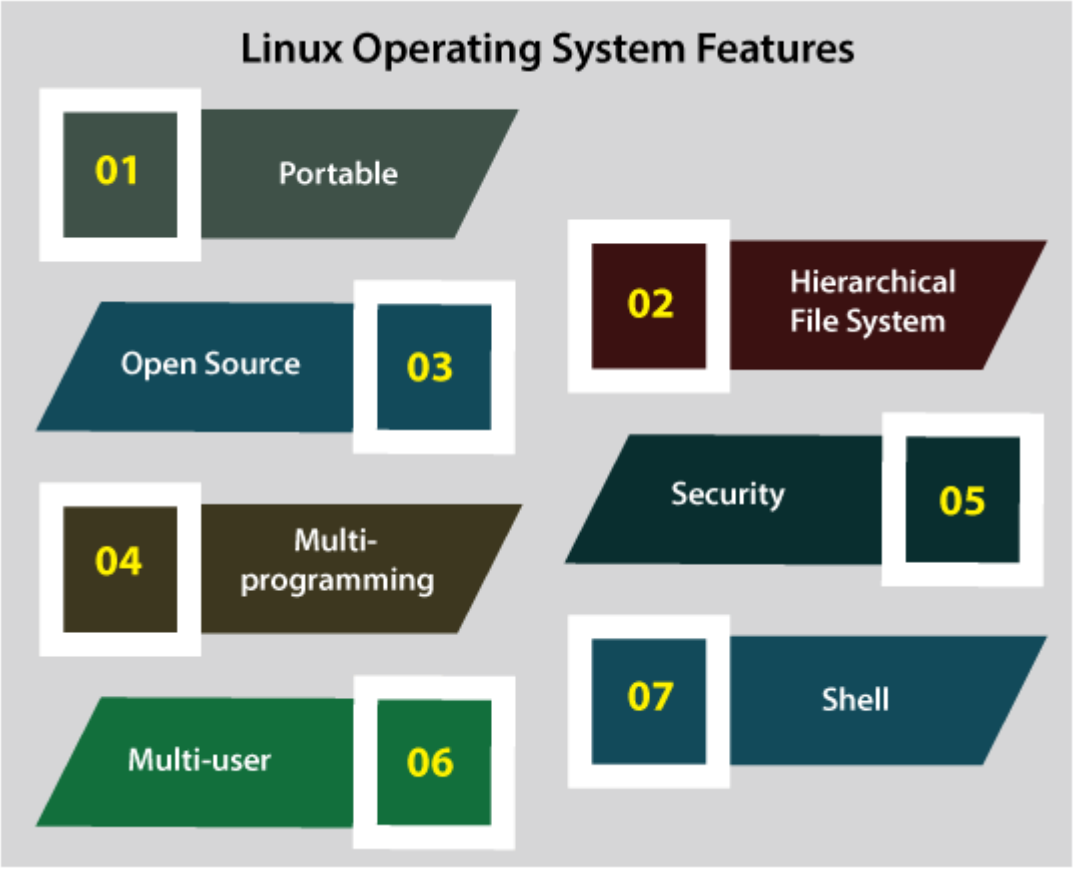
**10. Explain features of Window and Linux along with layer architecture. How these platforms are made secure? Explain in detail.**

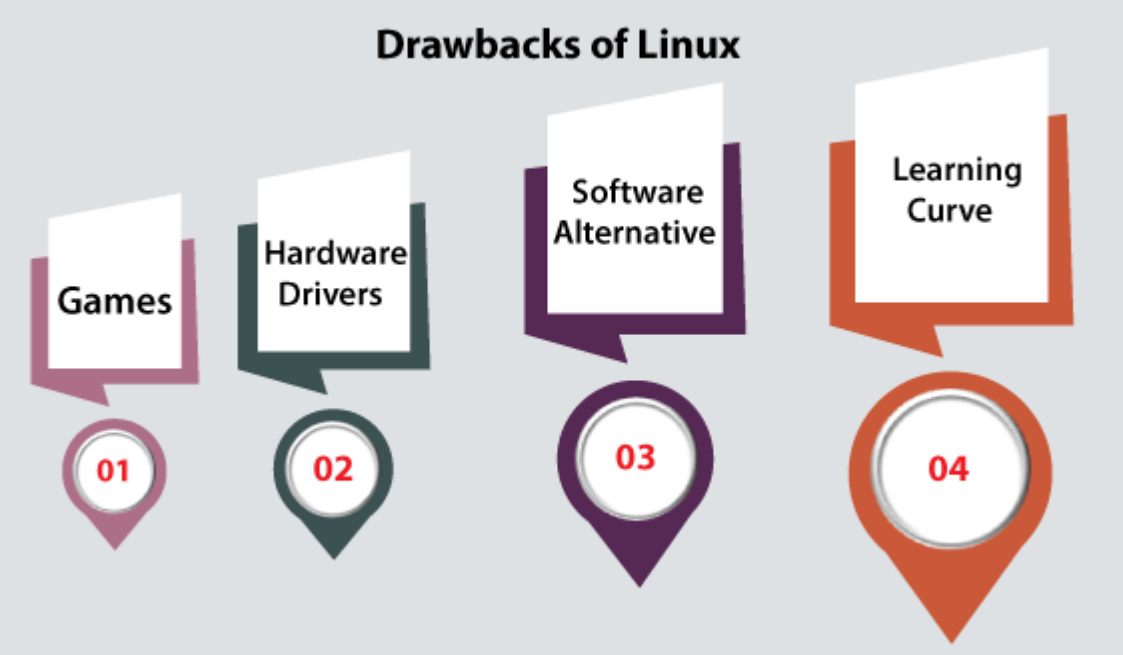
An operating system can be described as an interface among the computer hardware and the user of any computer. It is a group of software that handles the resources of the computer hardware and facilitates basic services for computer programs.

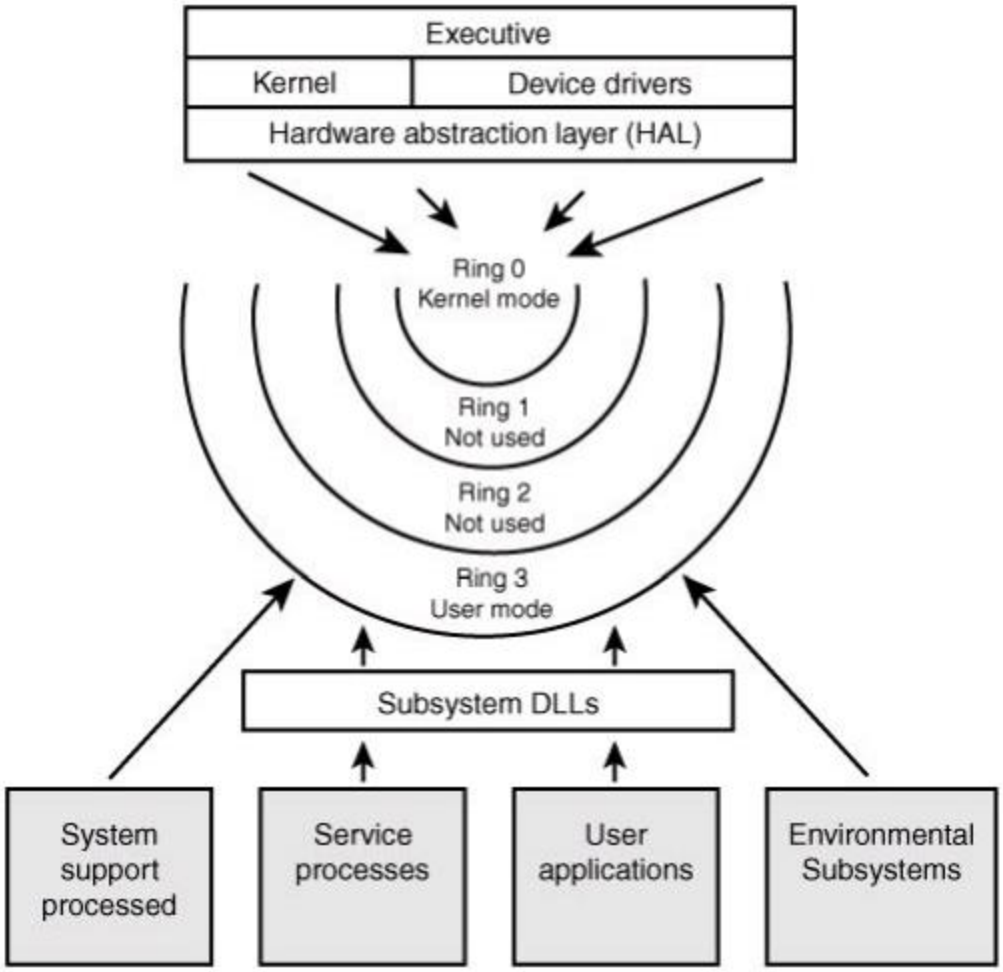
An operating system is an essential component of system software within a computer system. The primary aim of an operating system is to provide a platform where a user can run any program conveniently or efficiently.

On the other hand, Linux OS is one of the famous versions of the UNIX OS. It is developed to provide a low-cost or free OS for several personal computer system users. Remarkably, it is a complete OS Including an **X Window System, Emacs editor, IP/TCP, GUI** (graphical user interface), etc.

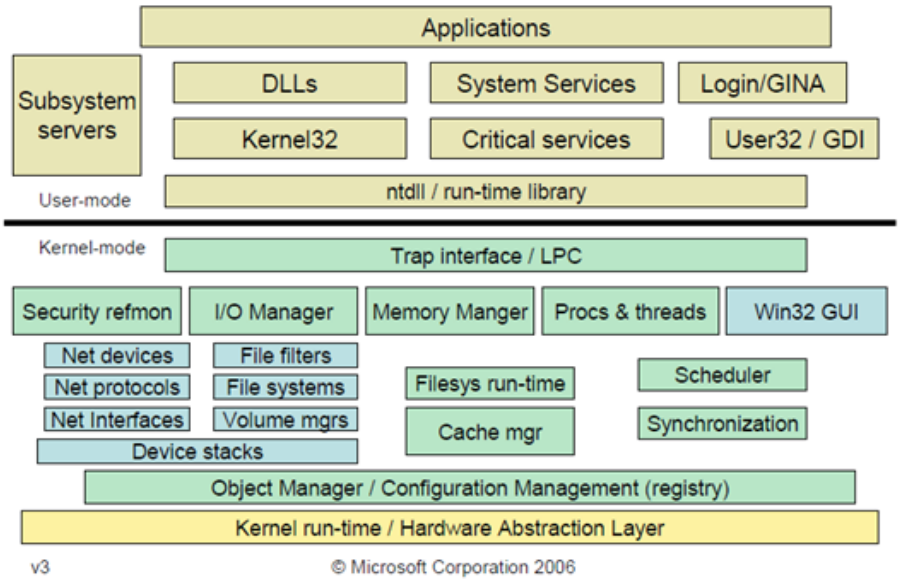



Linux Operating System Features
01
Portable
02
Hierarchical File System
Open Source
03
04
Multi-programming
Security
05
07
Shell
Multi-user
06


Drawbacks of Linux
Games
Hardware Drivers
Software Alternative
Learning Curve
01
02
03
04




# Windows Architecture




v3

## 11. Explain security attacks and measures of WI-FI attacks.

What are the risks to your wireless network?

Whether it's a home or business network, the risks to an unsecured wireless network are the same. Some of the risks include:

### Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can use your connection. The typical indoor broadcast range of an access point is 150–300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could open your internet connection to many unintended users. These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files.

### Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections available outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks. This practice is known as "wardriving."

### Evil Twin Attacks

In an evil twin attack, an adversary gathers information about a public network access point, then sets up their system to impersonate it. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information. Always confirm the name and password of a public Wi-Fi hotspot prior to use. This will ensure you are connecting to a trusted access point.

### Wireless Sniffing

Many public access points are not secured and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted "in the clear," malicious actors could use sniffing tools to obtain sensitive information such as passwords or credit card numbers. Ensure that all the access points you connect to use at least WPA2 encryption.

Unauthorized Computer Access

An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing. Ensure that when you connect your devices to public networks, you deny sharing files and folders. Only allow sharing on recognized home networks and only while it is necessary to share items. When not needed, ensure that file sharing is disabled. This will help prevent an unknown attacker from accessing your device's files.

Shoulder Surfing

In public areas malicious actors can simply glance over your shoulder as you type. By simply watching you, they can steal sensitive or personal information. Screen protectors that prevent shoulder-surfers from seeing your device screen can be purchased for little money. For smaller devices, such as phones, be cognizant of your surroundings while viewing sensitive information or entering passwords.

Theft of Mobile Devices

Not all attackers rely on gaining access to your data via wireless means. By physically stealing your device, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts. Taking measures to protect your devices from loss or theft is important, but should the worst happen, a little preparation may protect the data inside. Most mobile devices, including laptop computers, now have the ability to fully encrypt their stored data—making devices useless to attackers who cannot provide the proper password or personal identification number (PIN). In addition to encrypting device content, it is also advisable to configure your device's applications to request login information before allowing access to any cloud-based information. Last, individually encrypt or password-protect files that contain personal or sensitive information. This will afford yet another layer of protection in the event an attacker is able to gain access to your device.

**What can you do to minimize the risks to your wireless network?**

Change default passwords. Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default passwords makes it harder for attackers to access a device. Use and periodic changing of

complex passwords is your first line of defense in protecting your device. (See Choosing and Protecting Passwords.)

Restrict access. Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the "guest" account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.

Encrypt the data on your network. Encrypting your wireless data prevents anyone who might be able to access your network from viewing it. There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices. WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.

Protect your Service Set Identifier (SSID). To prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device's SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer's default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.

Install a firewall. Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer (see Understanding Firewalls for Home and Small Office Use).

Maintain antivirus software. Install antivirus software and keep your virus definitions up to date. Many antivirus programs also have additional features that detect or protect against spyware and adware (see Protecting Against Malicious Code and What is Cybersecurity?).

Use file sharing with caution. File sharing between devices should be disabled when not needed. You should always choose to only allow file sharing over home or work networks, never on public networks. You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories. In addition, you should password protect anything you share. Never open an entire hard drive for file sharing (see Choosing and Protecting Passwords).

Keep your access point software patched and up to date. The manufacturer of your wireless access point will periodically release updates to and patches for a device's software and firmware. Be sure to check the manufacturer's website regularly for any updates or patches for your device.

Check your internet provider's or router manufacturer's wireless security options. Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions.

Connect using a Virtual Private Network (VPN). Many companies and organizations have a VPN. VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

## 12. How SQL injection is performed? Explain methods, types and solutions

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities.

- Attackers can use SQL Injections to find the credentials of other users in the database. They can then impersonate these users. The impersonated user may be a database administrator with all database privileges.
- SQL lets you select and output data from the database. An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.
- SQL also lets you alter data in a database and add new data. For example, in a financial application, an attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.
- You can use SQL to delete records from a database, even drop tables. Even if the administrator makes database backups, deletion of data could affect application availability until the database is restored. Also, backups may not cover the most recent data.
- In some database servers, you can access the operating system using the database server. This may be intentional or accidental. In such case, an attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

SQL injections typically fall under three categories: In-band SQLi (Classic), Inferential SQLi (Blind) and Out-of-band SQLi. You can classify SQL injections types based on the methods they use to access backend data and their damage potential.

## Types of SQL Injections

SQL injections typically fall under three categories: In-band SQLi (Classic), Inferential SQLi (Blind) and Out-of-band SQLi. You can classify SQL injections types based on the methods they use to access backend data and their damage potential.

In-band SQLi

The attacker uses the same channel of communication to launch their attacks and to gather their results. In-band SQLi's simplicity and efficiency make it one of the most common types of SQLi attack. There are two sub-variations of this method:

- **Error-based SQLi**—the attacker performs actions that cause the database to produce error messages. The attacker can potentially use the data provided by these error messages to gather information about the structure of the database.
- **Union-based SQLi**—this technique takes advantage of the UNION SQL operator, which fuses multiple select statements generated by the database to get a single HTTP response. This response may contain data that can be leveraged by the attacker.

Inferential (Blind) SQLi

The attacker sends data payloads to the server and observes the response and behavior of the server to learn more about its structure. This method is called blind SQLi because the data is not transferred from the website database to the attacker, thus the attacker cannot see information about the attack in-band.

Blind SQL injections rely on the response and behavioral patterns of the server so they are typically slower to execute but may be just as harmful. Blind SQL injections can be classified as follows:

- **Boolean**—that attacker sends a SQL query to the database prompting the application to return a result. The result will vary depending on whether the query is true or false. Based on the result, the information within the HTTP response will modify or stay unchanged. The attacker can then work out if the message generated a true or false result.
- **Time-based**—attacker sends a SQL query to the database, which makes the database wait (for a period in seconds) before it can react. The attacker can see from the time the database takes to respond, whether a query is true or false. Based on the result, an HTTP response will be generated instantly or after a waiting period. The attacker can thus work out if the message they used returned true or false, without relying on data from the database.

Out-of-band SQLi

The attacker can only carry out this form of attack when certain features are enabled on the database server used by the web application. This form of attack is primarily used as an alternative to the in-band and inferential SQLi techniques.

Out-of-band SQLi is performed when the attacker can't use the same channel to launch the attack and gather information, or when a server is too slow or unstable for these actions to be performed. These techniques count on the capacity of the server to create DNS or HTTP requests to transfer data to an attacker.

**Primary Defenses:**

- **Option 1: Use of Prepared Statements (with Parameterized Queries)**
- **Option 2: Use of Properly Constructed Stored Procedures**
- **Option 3: Allow-list Input Validation**
- **Option 4: Escaping All User Supplied Input**

**Additional Defenses:**

- **Also: Enforcing Least Privilege**
- **Also: Performing Allow-list Input Validation as a Secondary Defense**

**1)** Continuous Scanning and Penetration Testing

**2)** Restrict Privileges

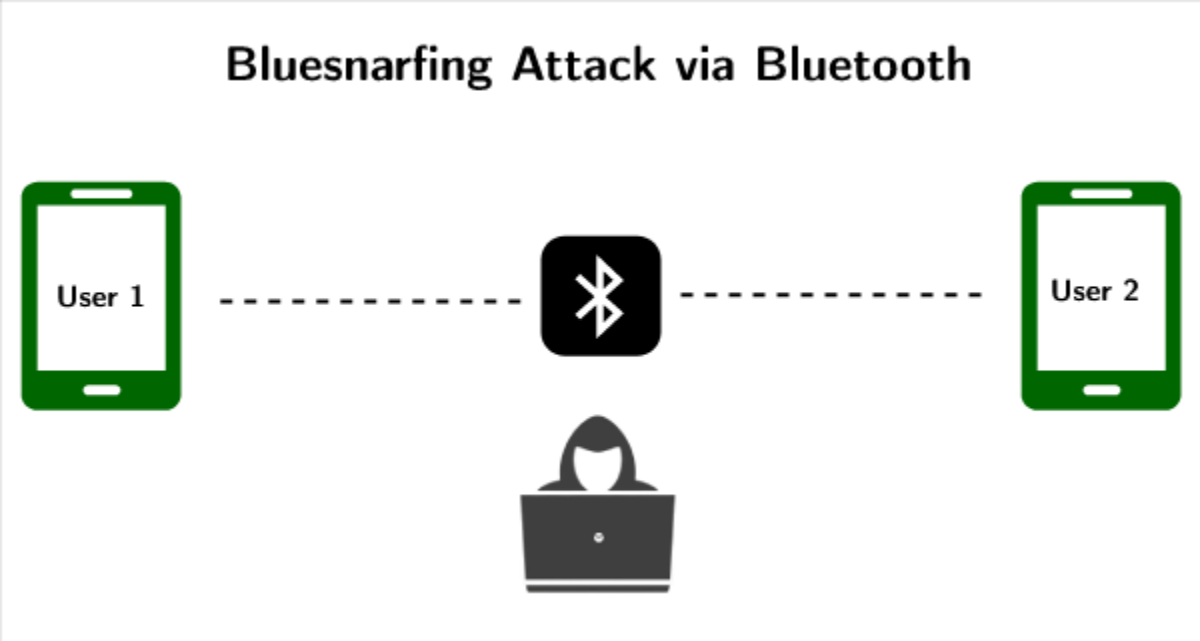
**3) Use Query Parameters**

**4) Instant Protection.**

# SAMPLE PAPER 3

**1. What do you mean by blue-snarfing.**

Blue snarfing is a hacking technique that is used to retrieve data from a victim's device. Blue snarfing attacks happen when your Bluetooth is on and set on "discoverable to others" mode. To launch a Blue snarfing attack, the attacker needs to exploit the object exchange protocol (OBEX protocol) to exchange information between the wireless devices. OBEX is a vendor-independent protocol implemented on different operating systems. Many tools are used to exploit the inherent vulnerabilities and loopholes of the OBEX Protocol. Hackers can pair themselves with the victim's device. Then the attackers can retrieve the data from the victim's device if their firmware protection is not that strong.




Often, hackers create their own software for hacking otherwise, many options are present on the dark web. One of them is Bluediving, which is used for the penetration testing of Blue tooth devices. It has different tools to exploit the OBEX protocol, like BlueBug, BlueSnarf, BlueSnarf++, BlueSmack, etc.

**2. How blue-jacking is done?**

Bluejacking is used for sending unauthorized messages to another Bluetooth device. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers and other devices.

Bluetooth has a very small range so only when a person is within 10 (highly location dependent) meters distance of a bluejacker and his Bluetooth enabled in his device, does bluejacking happen.

Bluejacking involves sending unsolicited business cards, messages, or pictures. The bluejacker discovers the recipient's phone via doing a scan of Bluetooth devices. He would then select any device, craft a message as is allowed within the body of the phone's contact interface. He stays near the receiver to monitor his reactions.

**Steps To Bluejack A Device**

1. Blue jacker opens his contacts and creates a new contact.
2. He does not save a name and number rather he saves the message in place of the contact and does not need to save a number (It is optional if he wants to send a business card, he can save the number).
3. He would scan for nearby Bluetooth devices.
4. He would then share the contact with the Bluetooth device connected.
5. The message will reach the recipient and he will have no clue as to who had sent the message.

## 3. What are different types of captcha?

1. **Fundamental math :**
   It is one of most widely recognized types of captcha being utilized in better places like sites, forms, and so forth.
2. **Word issue :**
   This standard kind of captcha changes in different structures anyway they all go with two direct parts : book box and course of action of letters or numbers
3. **Social media sign in :**
   Exactly when you seek after site, alternative of entering your private information is using your social record.
4. **Time-based :**
   Recording proportion of time that customers spend to complete structure is another effective kind of captcha.
5. **Honeypot :**
   Honeypot propels gathering lot of covered fields on page to beguile bots. Bots are redone to balance all fields they find, even invisible ones.
6. **Picture conspicuous confirmation :**
   Picture conspicuous verification captcha offers different kinds of picture tests, from naming pictures, perceiving pictures from lot of pictures to recognizing odd picture out of set.
7. **No captcha Recaptcha :**
   Google has as of late pushed this sort of captcha since 2014 anyway it has gotten continuously notable on the web. Customers are given checkbox assigning "I am not robot" and they simply snap it.
8. **Invisible Recaptcha :**
   Invisible Recaptcha is revived variation of No captcha Recaptcha. Like its name,

this captcha is absolutely invisible to customers, hoping to make more satisfying customer experiences than as of late referenced procedures.

9. **Confident Recaptcha:**
   Confident captcha is picture based procedure. It outfits selection of pictures with bearings
10. **Sweet captcha:**
    Such captcha is extremely similar to previous one. Customers are drawn nearer to move or match things to one another, which can cause difficulties for bots.
11. **Biometrics:**
    As there are creating number of wise devices getting ready to finger impression sensors, this part comes in accommodating to assert uncommon character.

## 4. What is dictionary attack?

A Dictionary Attack is an attack vector used by the attacker to break in a system, which is password protected, by putting technically every word in a dictionary as a form of password for that system. This attack vector is a form of Brute Force Attack.

The dictionary can contain words from an English dictionary and also some leaked list of commonly used passwords and when combined with common character replacing with numbers, can sometimes be very effective and fast.

Basically, it is trying every single word that is already prepared. It is done using automated tools that try all the possible words in the dictionary.

## 5. How ping of death attack is performed?

Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

While PoD attacks exploit legacy weaknesses which may have been patched in target systems. However, in an unpatched systems, the attack is still relevant and dangerous. Recently, a new type of PoD attack has become popular. This attack, commonly known as a Ping flood, the targeted system is hit with ICMP packets sent rapidly via ping without waiting for replies.

Attack description

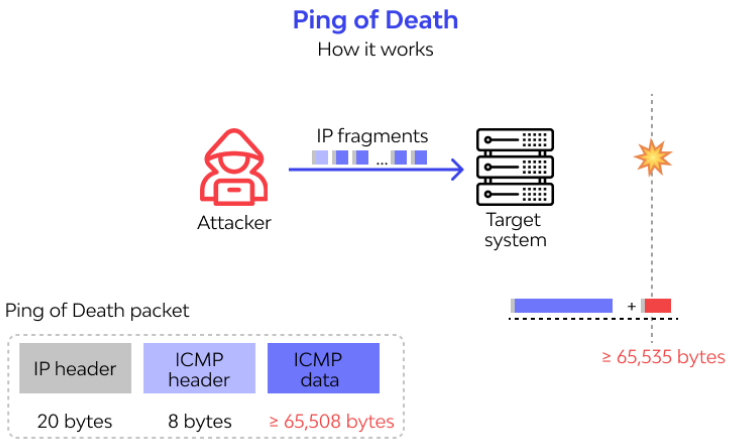
The size of a correctly-formed IPv4 packet including the IP header is 65,535 bytes, including a total payload size of 84 bytes. Many historical computer systems simply could not handle larger packets, and would crash if they received one. This bug was easily exploited in early TCP/IP implementations in a wide range of operating systems including Windows, Mac, Unix, Linux, as well as network devices like printers and routers.

Since sending a ping packet larger than 65,535 bytes violates the Internet Protocol, attackers would generally send malformed packets in fragments. When the target system attempts to

reassemble the fragments and ends up with an oversized packet, memory overflow could occur and lead to various system problems including crash.

Ping of Death attacks were particularly effective because the attacker's identity could be easily spoofed. Moreover, a Ping of Death attacker would need no detailed knowledge of the machine he/she was attacking, except for its IP address.

It is worthy of note that this vulnerability, though best recognized for its exploitation by PoD attacks, can actually be exploited by anything that sends an IP datagram – ICMP echo, TCP, UDP and IPX.




**6. Explain different types of mobile malwares and security practices.**

1. Remote Access Tools (RATs) offer extensive access to data from infected victim devices and are often used for intelligence collection. RATs can typically access information such as installed applications, call history, address books, web browsing history, and sms data. RATs may also be used to send SMS messages, enable device cameras, and log GPS data.

2. Bank trojans are often disguised as legitimate applications and seek to compromise users who conduct their banking business — including money transfers and bill payments — from their mobile devices. This type of trojan aims to steal financial login and password details.

3. Ransomware is a type of malware used to lock out a user from their device and demand a "ransom" payment — usually in untraceable Bitcoin. Once the victim pays the ransom, access codes are provided to allow them to unlock their mobile device.

4. Crypto mining Malware enables attackers to covertly execute calculations on a victim's device – allowing them to generate cryptocurrency. Crypto mining is often conducted through Trojan code that is hidden in legitimate-looking apps.

5. Advertising Click Fraud is a type of malware that allows an attacker to hijack a device to generate income through fake ad clicks.

Security Steps

1. Keep a Close Eye on the Apps
2. Install a Good Mobile Antivirus
3. Double Check Your Settings
4. Be Careful While Browsing
5. Be Aware of the Latest Mobile Threats

**7. What types of attacks are performed through Bluetooth connection? Explain.**

1. Bluesnarf Attack

Bluesnarf attacks are one of the most prevalent types of Bluetooth attack. The OBject EXchange (OBEX) protocol is used for importing business cards and other items.

2. Bluesnarf++ Attack

This attack is similar to the Bluesnarf attack. The main difference is the method the attacker uses to gain access to the file system

3. BluePrinting Attack

Through a BluePrinting attack, it is possible to capture information such as the brand and model of the device by using the data provided by Bluetooth technology.

4. HelloMoto Attack

This attack exploits the vulnerability in some of Motorola's devices with improper management of "trusted devices".

5. BlueBump Social Engineering Attack

This attack **requires some social engineering**. The main idea is to provide a secure connection with the victim. This is possible with a virtual job card or a file transfer.

6. BlueDump Attack

Here, the attacker has to know the addresses with which the Bluetooth device is paired, i.e. the Bluetooth Device Address (BD_ADDR), a unique identifier assigned to each device by manufacturers.

7. BlueChop Attack

This attack uses the main device's ability to connect to multiple devices to create an expanded network (Scatternet).

8. Authentication Abuse

Authentication applies to all devices that use a service on Bluetooth devices; but anything that connects to the main device to use a service can also use all other services that provide unauthorized access.

9. BlueSmack DoS Attack

BlueSmack is a Denial-of-Service (DoS) attack, possible to create using the Linux BlueZ Bluetooth layer. Essentially, a cybercriminal sends over a data packet that overwhelms the target device.

10. BlueBorne

Using the vulnerabilities in the Bluetooth stack, Blueborne can connect to devices without owners' knowledge and run commands with maximum authority inside the device.

11. Car Whisperer Attack

In this attack, attackers use PIN codes that come by default on Bluetooth radios in cars. Devices connect to vehicles by emulating a phone.

**8. Explain Attacks and countermeasures for common web authentication.**

- **Spoofing**. *Spoofing* is attempting to gain access to a system by using a false identity. This can be accomplished using stolen user credentials or a false IP address. After the attacker successfully gains access as a legitimate user or host, elevation of privileges or abuse using authorization can begin.

- **Tampering**. *Tampering* is the unauthorized modification of data, for example as it flows over a network between two computers.
- **Repudiation**. *Repudiation* is the ability of users (legitimate or otherwise) to deny that they performed specific actions or transactions. Without adequate auditing, repudiation attacks are difficult to prove.
- **Information disclosure**. *Information disclosure* is the unwanted exposure of private data. For example, a user views the contents of a table or file he or she is not authorized to open, or monitors data passed in plaintext over a network. Some examples of information disclosure vulnerabilities include the use of hidden form fields, comments embedded in Web pages that contain database connection strings and connection details, and weak exception handling that can lead to internal system level details being revealed to the client. Any of this information can be very useful to the attacker.
- **Denial of service**. *Denial of service* is the process of making a system or application unavailable. For example, a denial of service attack might be accomplished by bombarding a server with requests to consume all available system resources or by passing it malformed input data that can crash an application process.
- **Elevation of privilege**. *Elevation of privilege* occurs when a user with limited privileges assumes the identity of a privileged user to gain privileged access to an application. For example, an attacker with limited privileges might elevate his or her privilege level to compromise and take control of a highly privileged and trusted process or account.

| Threat | Countermeasures |
|---|---|
| Spoofing user identity | Use strong authentication.<br>Do not store secrets (for example, passwords) in plaintext.<br>Do not pass credentials in plaintext over the wire.<br>Protect authentication cookies with Secure Sockets Layer (SSL). |
| Tampering with data | Use data hashing and signing.<br>Use digital signatures.<br>Use strong authorization.<br>Use tamper-resistant protocols across communication links.<br>Secure communication links with protocols that provide message integrity. |
| Repudiation | Create secure audit trails.<br>Use digital signatures. |
| Information disclosure | Use strong authorization.<br>Use strong encryption.<br>Secure communication links with protocols that provide message confidentiality.<br>Do not store secrets (for example, passwords) in plaintext. |
| Denial of service | Use resource and bandwidth throttling techniques.<br>Validate and filter input. |
| Elevation of privilege | Follow the principle of least privilege and use least privileged service accounts to run processes and access resources. |

- **Information gathering**
- **Sniffing**
- **Spoofing**
- **Session hijacking**
- **Denial of service**

**Information Gathering**

Network devices can be discovered and profiled in much the same way as other types of systems. Attackers usually start with port scanning. After they identify open ports, they use banner grabbing and enumeration to detect device types and to determine operating system and application versions. Armed with this information, an attacker can attack known vulnerabilities that may not be updated with security patches.

Countermeasures to prevent information gathering include:

- Configure routers to restrict their responses to footprinting requests.
- Configure operating systems that host network software (for example, software firewalls) to prevent footprinting by disabling unused protocols and unnecessary ports.

**Sniffing**

*Sniffing* or *eavesdropping* is the act of monitoring traffic on the network for data such as plaintext passwords or configuration information. With a simple packet sniffer, an attacker can easily read all plaintext traffic. Also, attackers can crack packets encrypted by lightweight hashing algorithms and can decipher the payload that you considered to be safe. The sniffing of packets requires a packet sniffer in the path of the server/client communication.

Countermeasures to help prevent sniffing include:

- Use strong physical security and proper segmenting of the network. This is the first step in preventing traffic from being collected locally.
- Encrypt communication fully, including authentication credentials. This prevents sniffed packets from being usable to an attacker. SSL and IPSec (Internet Protocol Security) are examples of encryption solutions.

**Spoofing**

Spoofing is a means to hide one's true identity on the network. To create a spoofed identity, an attacker uses a fake source address that does not represent the actual address of the packet. Spoofing may be used to hide the original source of an attack or to work around network access control lists (ACLs) that are in place to limit host access based on source address rules.

Although carefully crafted spoofed packets may never be tracked to the original sender, a combination of filtering rules prevents spoofed packets from originating from your network, allowing you to block obviously spoofed packets.

Countermeasures to prevent spoofing include:

- Filter incoming packets that appear to come from an internal IP address at your perimeter.
- Filter outgoing packets that appear to originate from an invalid local IP address.

**Session Hijacking**

Also known as man in the middle attacks, session hijacking deceives a server or a client into accepting the upstream host as the actual legitimate host. Instead the upstream host is an attacker's host that is manipulating the network so the attacker's host appears to be the desired destination.

Countermeasures to help prevent session hijacking include:

- Use encrypted session negotiation.
- Use encrypted communication channels.
- Stay informed of platform patches to fix TCP/IP vulnerabilities, such as predictable packet sequences.

**Denial of Service**

Denial of service denies legitimate users access to a server or services. The SYN flood attack is a common example of a network level denial of service attack. It is easy to launch and difficult to track. The aim of the attack is to send more requests to a server than it can handle. The attack exploits a potential vulnerability in the TCP/IP connection establishment mechanism and floods the server's pending connection queue.

Countermeasures to prevent denial of service include:

- Apply the latest service packs.
- Harden the TCP/IP stack by applying the appropriate registry settings to increase the size of the TCP connection queue, decrease the connection establishment period, and employ dynamic backlog mechanisms to ensure that the connection queue is never exhausted.
- Use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks.

- **Viruses, Trojan horses, and worms**
- **Footprinting**
- **Profiling**
- **Password cracking**
- **Denial of service**

- **Arbitrary code execution**
- **Unauthorized access**

### Viruses, Trojan Horses, and Worms

A virus is a program that is designed to perform malicious acts and cause disruption to your operating system or applications. A Trojan horse resembles a virus except that the malicious code is contained inside what appears to be a harmless data file or executable program. A worm is similar to a Trojan horse except that it self-replicates from one server to another. Worms are difficult to detect because they do not regularly create files that can be seen. They are often noticed only when they begin to consume system resources because the system slows down or the execution of other programs halt. The Code Red Worm is one of the most notorious to afflict IIS; it relied upon a buffer overflow vulnerability in a particular ISAPI filter.

Although these three threats are actually attacks, together they pose a significant threat to Web applications, the hosts these applications live on, and the network used to deliver these applications. The success of these attacks on any system is possible through many vulnerabilities such as weak defaults, software bugs, user error, and inherent vulnerabilities in Internet protocols.

Countermeasures that you can use against viruses, Trojan horses, and worms include:

- Stay current with the latest operating system service packs and software patches.
- Block all unnecessary ports at the firewall and host.
- Disable unused functionality including protocols and services.
- Harden weak, default configuration settings.

### Footprinting

Examples of footprinting are port scans, ping sweeps, and NetBIOS enumeration that can be used by attackers to glean valuable system–level information to help prepare for more significant attacks. The type of information potentially revealed by footprinting includes account details, operating system and other software versions, server names, and database schema details.

Countermeasures to help prevent footprinting include:

- Disable unnecessary protocols.
- Lock down ports with the appropriate firewall configuration.
- Use TCP/IP and IPSec filters for defense in depth.
- Configure IIS to prevent information disclosure through banner grabbing.
- Use an IDS that can be configured to pick up footprinting patterns and reject suspicious traffic.

### Password Cracking

If the attacker cannot establish an anonymous connection with the server, he or she will try to establish an authenticated connection. For this, the attacker must know a valid username and password combination. If you use default account names, you are giving the attacker a head start. Then the attacker only has to crack the account's password. The use of blank or weak passwords makes the attacker's job even easier.

Countermeasures to help prevent password cracking include:

- Use strong passwords for all account types.
- Apply lockout policies to end-user accounts to limit the number of retry attempts that can be used to guess the password.
- Do not use default account names, and rename standard accounts such as the administrator's account and the anonymous Internet user account used by many Web applications.
- Audit failed logins for patterns of password hacking attempts.

**Denial of Service**

Denial of service can be attained by many methods aimed at several targets within your infrastructure. At the host, an attacker can disrupt service by brute force against your application, or an attacker may know of a vulnerability that exists in the service your application is hosted in or in the operating system that runs your server.

Countermeasures to help prevent denial of service include:

- Configure your applications, services, and operating system with denial of service in mind.
- Stay current with patches and security updates.
- Harden the TCP/IP stack against denial of service.
- Make sure your account lockout policies cannot be exploited to lock out well known service accounts.
- Make sure your application is capable of handling high volumes of traffic and that thresholds are in place to handle abnormally high loads.
- Review your application's failover functionality.
- Use an IDS that can detect potential denial of service attacks.

**Arbitrary Code Execution**

If an attacker can execute malicious code on your server, the attacker can either compromise server resources or mount further attacks against downstream systems. The risks posed by arbitrary code execution increase if the server process under which the attacker's code runs is over-privileged. Common vulnerabilities include weak IID configuration and unpatched servers that allow path traversal and buffer overflow attacks, both of which can lead to arbitrary code execution.

Countermeasures to help prevent arbitrary code execution include:

- Configure IIS to reject URLs with "../" to prevent path traversal.
- Lock down system commands and utilities with restricted ACLs.
- Stay current with patches and updates to ensure that newly discovered buffer overflows are speedily patched.

**Unauthorized Access**

Inadequate access controls could allow an unauthorized user to access restricted information or perform restricted operations. Common vulnerabilities include weak IIS Web access controls, including Web permissions and weak NTFS permissions.

Countermeasures to help prevent unauthorized access include:

- Configure secure Web permissions.
- Lock down files and folders with restricted NTFS permissions.
- Use .NET Framework access control mechanisms within your ASP.NET applications, including URL authorization and principal permission demands.

## 9. What attacks are performed on VoIP? How is it made secure? Explain

Packet Sniffing and Black Hole Attacks

One of the most common VoIP attacks is called packet sniffing, which allows hackers to steal and log unencrypted information contained in voice data packets while they are in transit.

Packet loss, when voice data packets don't reach their destination, is caused by packet sniffers looking to steal information and slow service via a packet drop attack (sometimes called a black hole attack.) These packet sniffers intentionally drop packets into data streams by taking control of your router, resulting in a much slower network service or a complete loss of network connection.

**DDoS (Distributed Denial of Service) attacks**

As the name suggests, make it impossible for businesses to use their own VoIP services by intentionally overwhelming servers.

Usually, these DDoS are caused by a network of botnets, which are remotely-controlled computers/bots that hackers have manipulated. These "Zombie Computers" flood networks, websites, and servers with much more data or connection requests than they're able to handle, rendering VoIP services inoperable.

**VISHING**

Vishing is VoIP-based phishing, meaning that a hacker pretends to call you from a trusted phone number or source with the intent of getting you to reveal sensitive information to them, such as passwords, credit card numbers, and more.

Caller ID spoofing – the process where these vishing hackers make the names and numbers that appear on your caller ID seem legitimate — intentionally confuses potential victims. These hackers may appear to be calling from your bank's phone number, claiming that your account has been compromised, and requesting your password so they can secure it immediately.

**Malware and viruses**

impact internet-based applications like VoIP, creating a multitude of network security issues. These damaging programs specifically consume network bandwidth and add to signal congestion, which causes signal breakdown for your VoIP calls. These also corrupt data being transmitted across your network, which means that you'll experience packet loss.

Phreaking Attack

A phreaking attack is a type of fraud where hackers break into your VoIP system in order to make long-distance calls, change calling plans, add more account credits, and make any additional phone calls they want — all on your dime.

**SPIT**

SPIT, or Spam over IP Telephony, is similar to phishing attempts and other spam in emails. SPIT contains prerecorded messages that are sent on VoIP phone systems. These calls are mostly a nuisance that ties up your virtual phone numbers, but the spam carries other risks with it, such as viruses, malware, and other malicious attacks.

Man-in-the-Middle Attacks

As the name suggests, man-in-the-middle attacks occur when a hacker inserts themselves in between your VoIP network and the call's intended destination.

**Toll Fraud**

Toll Fraud is somewhat similar to a phreaking attack, but here, hackers intentionally make an excessive number of international calls from your business phone system so they can get a portion of the revenue the calls generate for themselves.

Call Tampering

Call tampering may not be as severe of a cyber attack as some of the others on this list, but it still seriously limits the way you can do business.

**Vomit**

Voice over Misconfigured Internet Telephones, or VOMIT, (gross, we know) is a VoIP hacking tool that actually converts conversations into files that can be played anywhere, making it easy to siphon information from your business phone system.

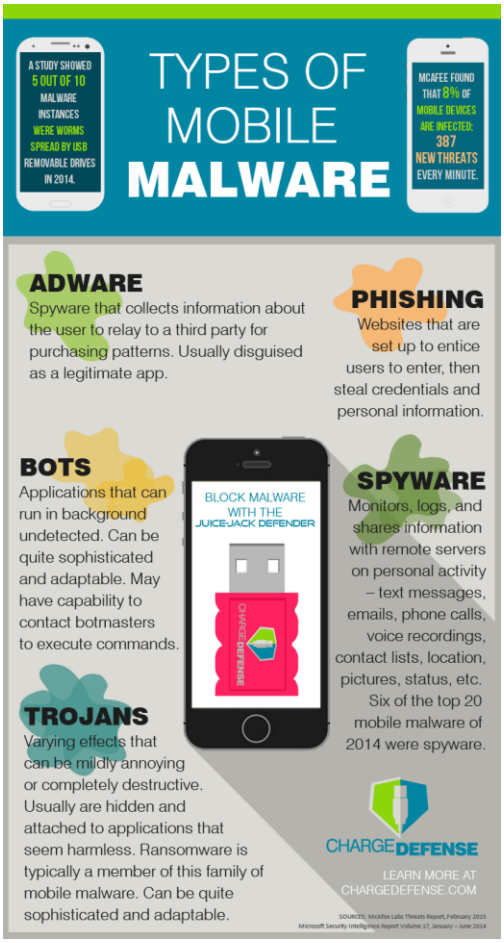
**Security Measures**

1. Enforce a strong password policy.

2. Apply operating system updates often.
3. Set up a Virtual Private Network (VPN) for remote staff.
4. Require Wi-Fi encryption.
5. Review your call logs.
6. Restrict your calling and block private calls.
7. Deactivate inactive accounts.
8. **Encrypt voice traffic**
9. **Encrypt WiFi**
10. **Use a VPN**
11. **Strong passwords**
12. **Run regular security checks**
13. **Enable Network Address Translation (NAT)**
14. **Close Port 80 With a Firewall**
15. **Keep systems and software up-to-date**
16. **Avoid international calling, unless needed**
17. **Consider remote device management**
18. **Educate users about VoIP security**

**10. Explain mobile malwares in detail. What security practices are applied to keep your Mobile phone safe? Discuss all counter measures.**

- Remote Access Tools (RATs) offer extensive access to data from infected victim devices and are often used for intelligence collection. RATs can typically access information such as installed applications, call history, address books, web browsing history, and sms data. RATs may also be used to send SMS messages, enable device cameras, and log GPS data.
- Bank trojans are often disguised as legitimate applications and seek to compromise users who conduct their banking business — including money transfers and bill payments — from their mobile devices. This type of trojan aims to steal financial login and password details.
- Ransomware is a type of malware used to lock out a user from their device and demand a "ransom" payment — usually in untraceable Bitcoin. Once the victim pays the ransom, access codes are provided to allow them to unlock their mobile device.
- Crypto mining Malware enables attackers to covertly execute calculations on a victim's device – allowing them to generate cryptocurrency. Cryptomining is often conducted through Trojan code that is hidden in legitimate-looking apps.
- Advertising Click Fraud is a type of malware that allows an attacker to hijack a device to generate income through fake ad clicks.




- Enable user authentication.
- Always run updates.
- Avoid public wifi.
- Use a password manager.
- Enable remote lock.
- Cloud backups.
- Use MDM/MAM.
- *Keep Your Phone* Locked
- Set *Secure* Passwords
- *Keep Your Device's* OS Up-To-Date
- Beware *of* Downloads
- If it's not already the default on your phone, consider encrypting your data

11.

**a) Why IOS is more secure than android? Explain**

Android makes it easier for hackers to develop exploits, increasing the threat level. Apple's closed development operating system makes it more challenging for hackers to gain access to develop exploits. Android is the complete opposite. Anyone (including hackers) can view its source code to develop exploits.

iOS is a closed system. Apple doesn't release its source code to app developers, and the owners of iPhones and iPads can't easily modify the code on their phones themselves. This makes it more difficult for hackers to find vulnerabilities on iOS-powered devices.

Apple's iOS mobile operating system is tightly controlled by Apple itself, which also tightly controls the apps available in the Apple App Store. This control allows Apple devices to offer good security "out of the box," at the price of some user restrictions.

For example, iOS only allows one copy of an app on each device. So, if a user has a company-provided security-restricted copy of an app, the user cannot also have an unrestricted version of the same app for personal use. Customizability is more restricted with iOS as well, with everything from the phone's appearance to app functionality having to fall into Apple's design rules.

iOS users will find themselves limited to Apple-approved devices and apps, which is a positive for streamlining security. With limited touchpoints across the whole ecosystem, Apple can provide support to each of their devices for a longer lifespan than platforms with hardware-OS fragmentation. Apple's smaller platform means even older phones may still be able to run the recent OS and apps, reaping all the benefits of new security fixes in the process. iPhone security, as a result, has gained a "safer" reputation among users.

Additionally, the closed ecosystem only permits apps that don't access the phone's root coding, which reduces both the need for iOS antivirus and makes an iOS antivirus impossible to create for App Store approval.

However, iOS is not invulnerable to malware attacks. If Apple misses any vulnerabilities or chooses certain undesirable approaches to security, you will have little to no control over this.

**b) Elaborate the countermeasures or mitigations for SQL INJECTION attack.**

The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

If you discover an SQL Injection vulnerability, for example using an Acunetix scan, you may be unable to fix it immediately. For example, the vulnerability may be in open source code. In such cases, you can use a web application firewall to sanitize your input temporarily.

Developers can prevent SQL Injection vulnerabilities in web applications by utilizing **parameterized database queries with bound, typed parameters and careful use of parameterized stored procedures in the database**.

This can be accomplished in a variety of programming languages including Java, .NET, PHP, and more.

1. Keep all web application software components including libraries, plug-ins, frameworks, web server software, and database server software up to date with the latest security patches available from vendors.
2. Utilize the principle of least privilege when provisioning accounts used to connect to the SQL database
3. Do not use shared database accounts between different web sites or applications.
4. Validate user-supplied input for expected data types, including input fields like drop-down menus or radio buttons, not just fields that allow users to type in input.
5. Configure proper error reporting and handling on the web server and in the code so that database error messages are never sent to the client web browser.

## 12. How VPN is used to provide security in public network? Explain.

Encryption is a way of scrambling data so that only authorized parties can understand the information. It takes readable data and alters it so that it appears random to attackers or anyone else who intercepts it. In this way, encryption is like a "secret code."

A VPN works by establishing encrypted connections between devices. (VPNs often use the IPsec or SSL/TLS encryption protocols.) All devices that connect to the VPN set up encryption keys, and these keys are used to encode and decode all information sent between them. This process may add a small amount of latency to network connections, which will slow network traffic (learn more about VPN performance).

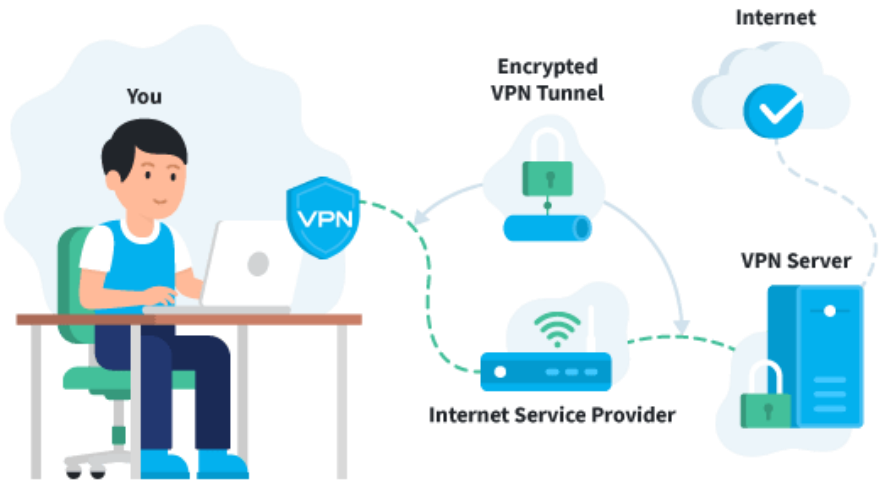
The effect of this encryption is that VPN connections remain private even if they stretch across public Internet infrastructure. Imagine Alice is working from home, and she connects to her company's VPN so that she can access a company database that is stored in a server 100 miles away. Suppose all of her requests to the database, as well as the database's responses, travel through an intermediate Internet exchange point (IXP).

Now suppose that a criminal has secretly infiltrated this IXP and is monitoring all data passing through (sort of like tapping a telephone line). Alice's data is still secure because of the VPN. All the criminal can see is the encrypted version of the data.

Connecting to a VPN is generally quite simple. After subscribing to a VPN provider, you **download and install the VPN** software. You then select a server you want to connect to, and the VPN will do the rest.

Want to know the ins and outs? Once the connection has been established, here's **how your data is transmitted through an encrypted tunnel**.

1. The VPN client software on your computer encrypts your data traffic and sends it to the VPN server through a secure connection. The data goes through your ISP, but it's been so scrambled because of the encryption, they can no longer decipher it.
2. The encrypted data from your computer is decrypted by the VPN server.
3. Your data is then sent to the internet and receives a reply that's meant for you, the user.
4. The traffic is then encrypted again by the VPN server and is sent back to you.
5. The VPN client on your device will decrypt the data so you can actually understand and use it.




Advantage 1: Anonymity online

Advantage 2: Protection against hackers and governments

Advantage 3: Secure browsing on public networks

Advantage 4: Fight online censorship

Advantage 5: Bypass geographical restrictions

Advantage 6: Anonymous downloading

Advantage 7: Prevent a digital file

Advantage 8: Secure access to your company’s network

VPN safety is an important factor to consider. Your internet traffic is redirected and runs through the servers of your chosen VPN provider. So, the VPN provider company could see everything you do if it wanted to. Therefore, it’s crucial to **choose a trusted VPN that does not keep logs of user data** that can be shared with third parties

A VPN **masks your IP address by acting as an intermediary and rerouting your traffic**. It also adds encryption, or a tunnel around your identity, as you connect. The combination of the VPN server and the encryption tunnel blocks your ISP, governments, hackers, and anyone else from spying on you as you navigate the web.