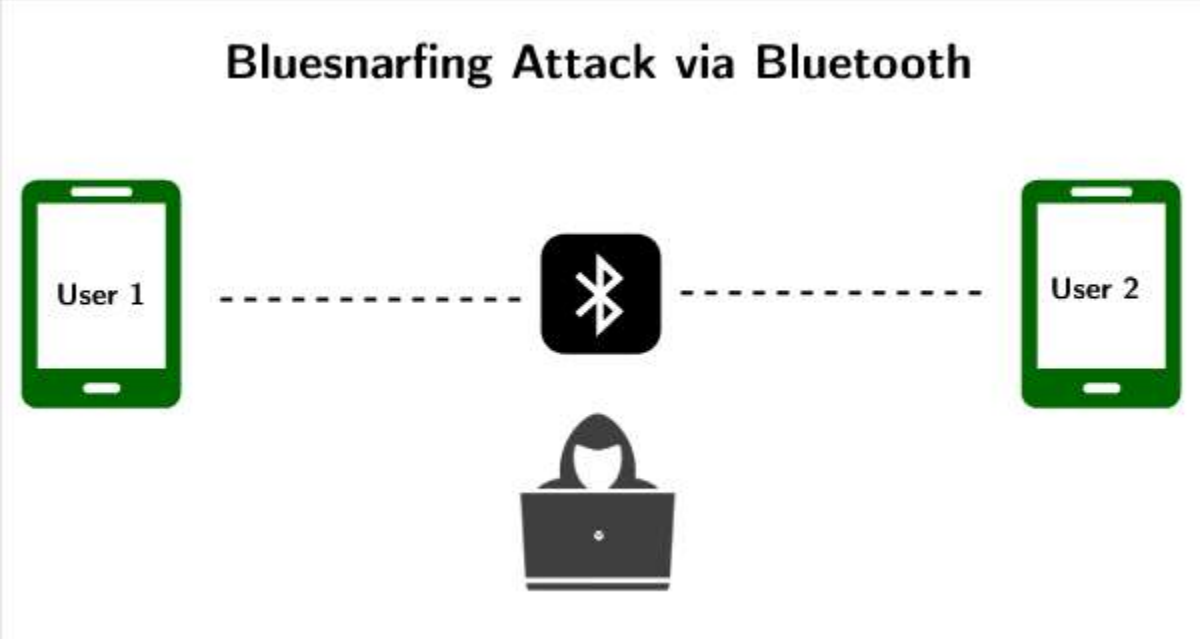
1. What do you mean by blue-snarfing.

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.

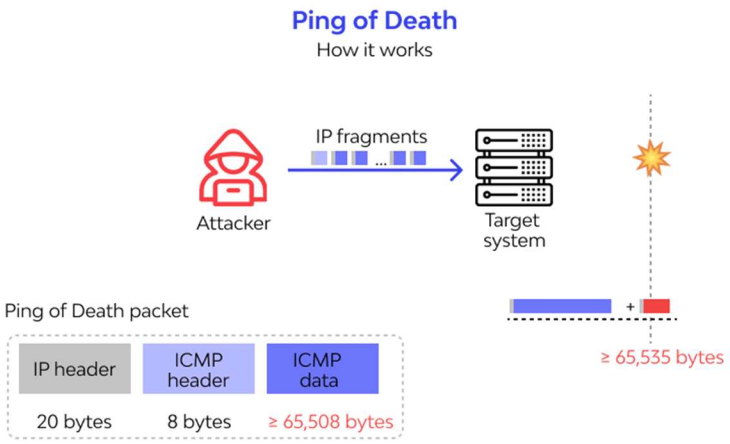
Attack description

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. Do not store secrets (for example, passwords) in plaintext. Do not pass credentials in plaintext over the wire. Protect authentication cookies with Secure Sockets Layer (SSL).
Tampering with data	Use data hashing and signing. Use digital signatures. Use strong authorization. Use tamper-resistant protocols across communication links. Secure communication links with protocols that provide message integrity.
Repudiation	Create secure audit trails. Use digital signatures.
Information disclosure	Use strong authorization. Use strong encryption.

	Secure communication links with protocols that provide message confidentiality. Do not store secrets (for example, passwords) in plaintext.
Denial of service	Use resource and bandwidth throttling techniques. 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

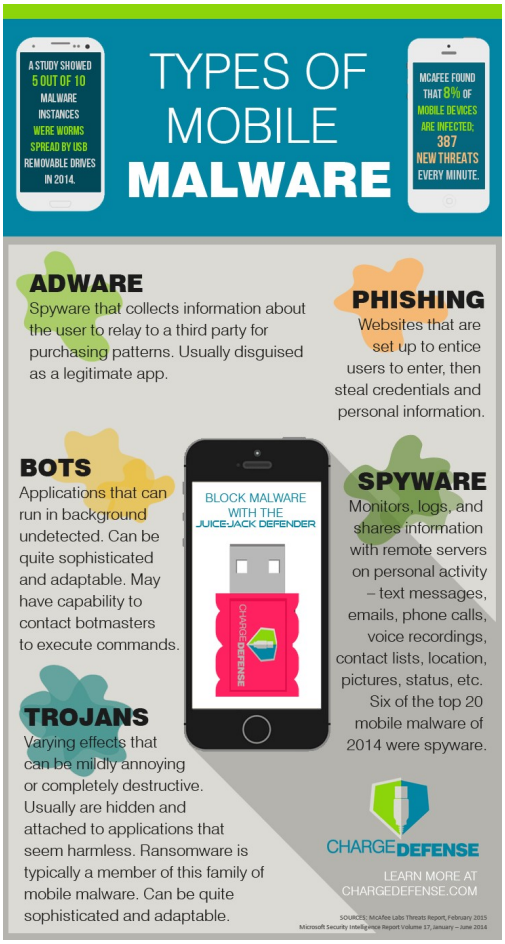
1. Enforce a strong password policy.
2. Apply operating system updates often.
3. Set up a Virtual Private Network (VPN) for remote staff.
4. Require Wi-Fi encryption.
5. Review your call logs.
6. Restrict your calling and block private calls.
7. Deactivate inactive accounts.
8. Encrypt voice traffic
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 mearsures.

- 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.

- Cryptomining 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).

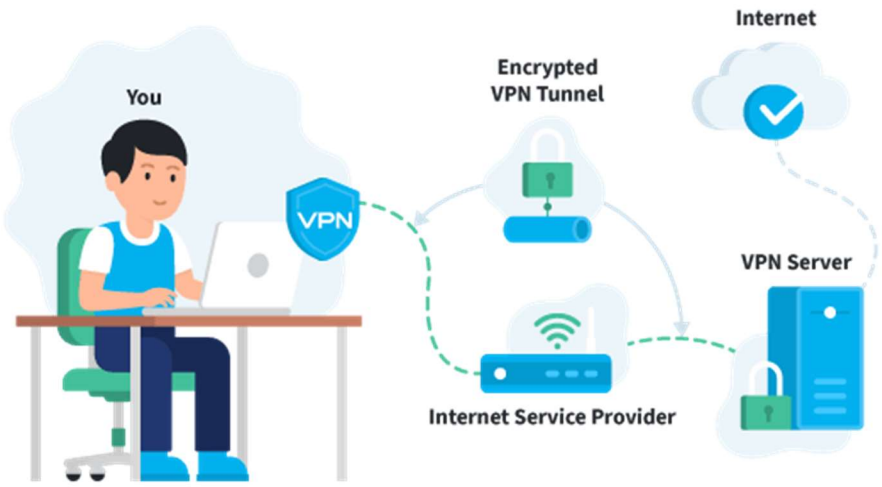
The effect of this encryption is that VPN connections remain private even if they stretch across public Internet infrastructure. Imagine Alice is working from home, and she connects to her company's VPN so that she can access a company database that is stored in a server 100 miles away. Suppose all of 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.