Module 3- CyberSecurity Attack

Module Overview

This module aims to introduce CyberSecurity basics. After understanding the basic concepts, we will move towards understanding the different CyberSecurity threats in detail.

Module Objective

At the end of the module, you will be able,

- To understand the meaning and CyberSecurity
- Learn types of CyberSecurity threats

Basics of CyberSecurity

CyberSecurity is the protection of internet-connected systems, including hardware, software and data, from cyber attacks.

In a computing context, security comprises CyberSecurity and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of CyberSecurity.

Elements of CyberSecurity

Ensuring CyberSecurity requires the coordination of efforts throughout an information system, which includes:

- **Application security:** Application security is the use of software, hardware, and procedural methods to protect applications from external threats.

- **Information security:** Information security (infosec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Infosec responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.\

- **Network security:** Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

- **Disaster recovery/business continuity planning:** A business continuity plan (BCP) is a document that consists of the critical information an organization needs to continue operating during an unplanned event.

- **Operational security:** OPSEC (operational security) is an analytical process that classifies information assets and determines the controls required to protect these assets.

- **End-user education:** Not educating your end-users in cybersecurity initiatives is like trying to keep a flood at bay using a screen door. Your end-users are the first line of defense against cybersecurity attacks (like phishing scams).

Types of CyberSecurity threats

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. However, it's necessary in order to protect information and other assets from cyberthreats, which take many forms.

- **Ransomware** is a type of malware that involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.

- **Malware** is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.

- **Social engineering** is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.

- **Phishing** is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.

What CyberSecurity can prevent?

The use of CyberSecurity can help prevent cyber attacks, data breaches and identity theft and can aid in risk management.

When an organization has a strong sense of network security and an effective incident response plan, it is better able to prevent and mitigate these attacks. For example, end user protection defends information and guards against loss or theft while also scanning computers for malicious code.

Challenges in CyberSecurity

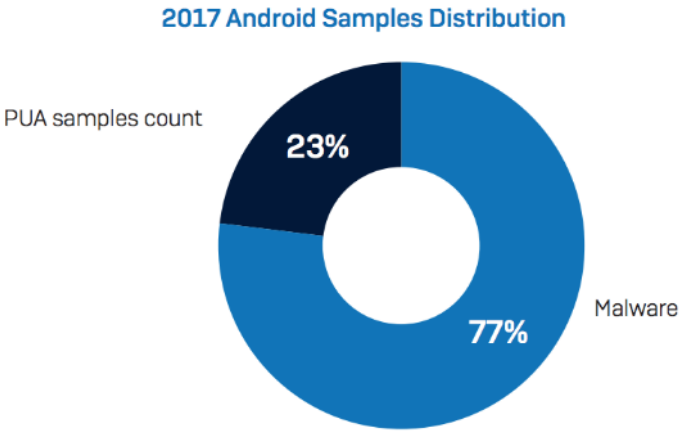
Here are the few challenges in Cybersecurity and trends:

1. **Ransomware Evolution**

   Ransomware is the bane of cybersecurity, IT, data professionals, and executives.

   Perhaps nothing is worse than a spreading virus that latches onto customer and business information that can only be removed if you meet the cybercriminal's egregious demands. And usually, those demands land in the hundreds of thousands (if not millions) of dollars.

   Ransomware attacks are one of the areas of cybercrime growing the fastest, too. The number of attacks has risen 36 percent this year (and doubled in cost).



2. **AI Expansion**

   Robots might be able to help defend against incoming cyber-attacks.

   Between 2016 and 2025, businesses will spend almost $2.5 billion on artificial intelligence to prevent cyberattacks.

3. IoT Threats

Most people are always plugged in.

The vast majority of humans in first-world countries have an iPhone in their pockets, a computer at work, a television at home, and a tablet in their cars.

The Internet of Things is making sure that every single device you own is connected. Your refrigerator can tell you when the milk runs out. Alexa can order you a pizza.

Of course, all of that connection carries with it massive benefits, which is what makes it so appealing in the first place. You no longer have to log in on multiple devices. You can easily control your TV with your phone. And you might even be able to control your at-home thermostat from other digital devices.

The problem is that all of that interconnectedness makes consumers highly susceptible to cyberattacks. In fact, one study revealed that 70 percent of IoT devices have serious security vulnerabilities.

Specifically, insecure web interfaces and data transfers, insufficient authentication methods, and a lack of consumer security knowledge leave users open to attacks.

And that truth is compounded by the fact that so many consumer devices are now interconnected. In other words, if you access one device, you've accessed them all. Evidently, with more convenience comes more risk.

That's a risk that security professionals need to be prepared to face by integrating password requirements, user verification, time-out sessions, two-factor authentication, and other sophisticated security protocols.

4. Blockchain Revolution

2017 ended with a spectacular rise in the valuation and popularity of crypto currencies like Bitcoin and Ethereum. These crypto currencies are built upon blockchains, the technical innovation at the core of the revolution, a decentralized and secure record of transactions.

What does blockchain technology have to do with cybersecurity?

It's a question that security professionals have only just started asking. As 2018 progresses, you'll likely see more people with answers.

While it's difficult to predict what other developments blockchain systems will offer in regards to cybersecurity, professionals can make some educated guesses. Companies are targeting a range of use cases which the blockchain helps enable from medical records management, to decentralized access control, to identity management. As the application and utility of blockchain in a cybersecurity context emerges, there will be a healthy tension but also complementary integrations with traditional, proven, cybersecurity approaches. You will undoubtedly see variations in approaches between public & private blockchains.

One thing's for sure, though. With blockchain technology, cybersecurity will likely look much different than it has in the past.

5. Serverless Apps Vulnerability

Serverless apps can invite cyber-attacks.

Customer information is particularly at risk when users access your application off-server — or locally — on their device.

Why?

Well, on-server — when the data is stored in the cloud rather than the user's device — you have control over that information and the security that surrounds it.

In other words, you're able to control what security precautions you take to ensure the user's data remains private from identity thieves and other cybercriminals.

With serverless applications, however, security precautions are, by and large, the responsibility of the user.

Of course, you can integrate software into the application that gives the user the best chance of defeating cybercriminals. But when all's said and done, you, the professional, can't directly defend the customer.

Serverless apps are most common as web service and data processing tools.

Cyberattack

A cyber attack is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems.

Let us go through ten most common cyber attack types:

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and Spear Phishing attack
- Drive-by attack
- Password attack
- SQL injection attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

Denial of Service and Distributed Denial of Service

A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

Unlike attacks that are designed to enable the attacker to gain or increase access, denial-of-service doesn't provide direct benefits for attackers. For some of them, it's enough to have the satisfaction of service denial. However, if the attacked resource belongs to a business competitor, then the benefit to the attacker may be real enough.

Another purpose of a DoS attack can be to take a system offline so that a different kind of attack can be launched. One common example is session hijacking

There are different types of DoS and DDoS attacks; the most common are **TCP SYN flood attack**, **teardrop attack, smurf attack, ping-of-death attack and botnets.**

TCP SYN flood attack

In this attack, an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker's device floods the target system's small in-process queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to time out while waiting for the response from the attacker's device, which makes the system crash or become unusable when the connection queue fills up.

- There are a few countermeasures to a TCP SYN flood attack:
- Place servers behind a firewall configured to stop inbound SYN packets.
- Increase the size of the connection queue and decrease the timeout on open connections.

Teardrop attack

This attack causes the length and fragmentation offset fields in sequential Internet Protocol (IP) packets to overlap one another on the attacked host; the attacked system attempts to reconstruct packets during the process but fails. The target system then becomes confused and crashes.

If users don't have patches to protect against this DoS attack, disable SMBv2 and block ports 139 and 445.

Smurf attack

This attack involves using IP spoofing and the ICMP to saturate a target network with traffic. This attack method uses ICMP echo requests targeted at broadcast IP addresses. These ICMP requests originate from a spoofed "victim" address.

For instance, if the intended victim address is 10.0.0.10, the attacker would spoof an ICMP echo request from 10.0.0.10 to the broadcast address 10.255.255.255. This request would go to all IPs in the range, with all the responses going back to 10.0.0.10, overwhelming the network. This process is repeatable, and can be automated to generate huge amounts of network congestion.

To protect your devices from this attack, you need to disable IP-directed broadcasts at the routers. This will prevent the ICMP echo broadcast request at the network devices. Another option would be to configure the end systems to keep them from responding to ICMP packets from broadcast addresses.

Ping of death attack

This type of attack uses IP packets to 'ping a target system with an IP size over the maximum of 65,535 bytes. IP packets of this size are not allowed, so attacker fragments the IP packet. Once the target system reassembles the packet, it can experience buffer overflows and other crashes.

Ping of death attacks can be blocked by using a firewall that will check fragmented IP packets for maximum size.

Botnets

Botnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks. These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities. These DDoS attacks are difficult to trace because botnets are located in differing geographic locations.

Botnets can be mitigated by:

- RFC3704 filtering, which will deny traffic from spoofed addresses and help ensure that traffic is traceable to its correct source network. For example, RFC3704 filtering will drop packets from bogon list addresses.

- Black hole filtering, which drops undesirable traffic before it enters a protected network. When a DDoS attack is detected, the BGP (Border Gateway Protocol) host should send routing updates to ISP routers so that they route all traffic heading to victim servers to a null0 interface at the next hop.

Man-in-the-middle (MitM) Attack

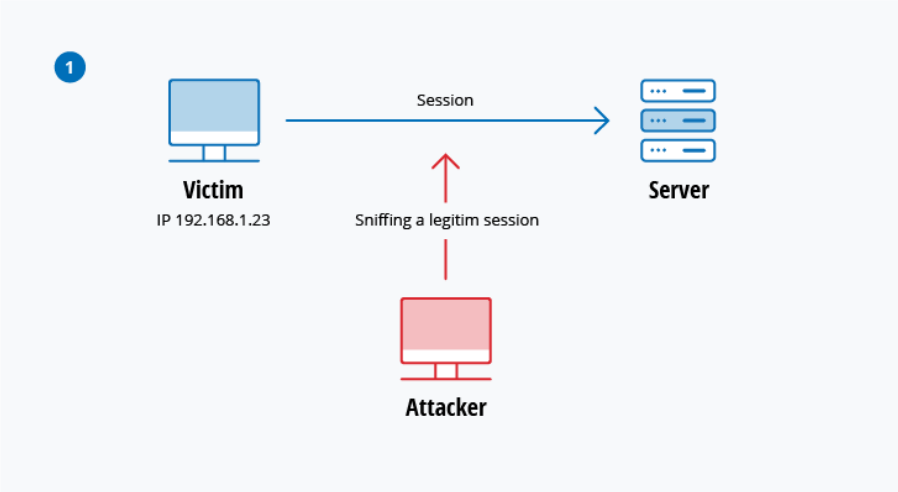
A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Here are some common types of man-in-the-middle attacks:

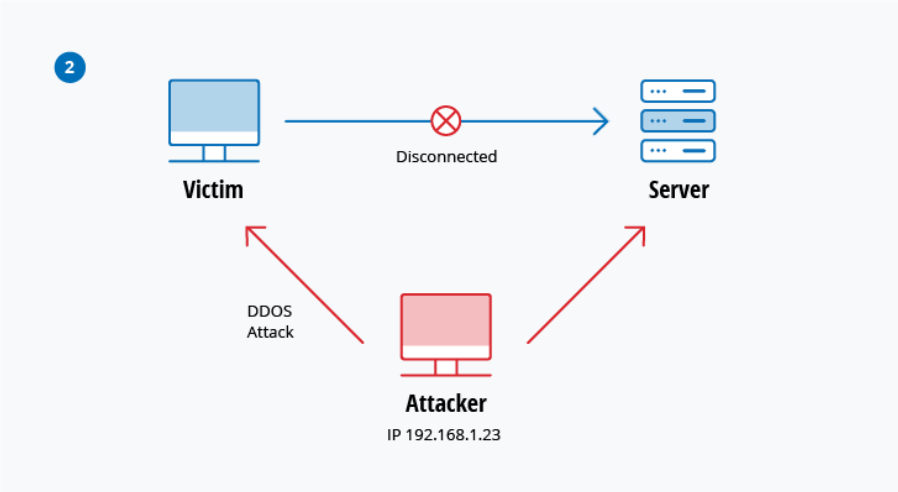
Session hijacking

In this type of MitM attack, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client.

For instance, the attack might unfold like this:

- A client connects to a server.
- The attacker's computer gains control of the client.
- The attacker's computer disconnects the client from the server.
- The attacker's computer replaces the client's IP address with its own IP address and spoofs the client's sequence numbers.
- The attacker's computer continues dialog with the server and the server believes it is still communicating with the client.





IP Spoofing

IP spoofing is used by an attacker to convince a system that it is communicating with a known, trusted entity and provide the attacker with access to the system. The attacker sends a packet with the IP source address of a known, trusted host instead of its own IP source address to a target host. The target host might accept the packet and act upon it.

Replay

A replay attack occurs when an attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants. This type can be easily countered with session timestamps or nonce (a random number or a string that changes with time).

Currently, there is no single technology or configuration to prevent all MitM attacks. Generally, encryption and digital certificates provide an effective safeguard against MitM attacks, assuring both the confidentiality and integrity of communications. But a man-in-the-middle attack can be injected

into the middle of communications in such a way that encryption will not help — for example, attacker "A" intercepts public key of person "P" and substitute it with his own public key. Then, anyone wanting to send an encrypted message to P using P's public key is unknowingly using A's public key. Therefore, A can read the message intended for P and then send the message to P, encrypted in P's real public key, and P will never notice that the message was compromised. In addition, A could also modify the message before resending it to P. As you can see, P is using encryption and thinks that his information is protected but it is not, because of the MitM attack.

So, how can you make sure that P's public key belongs to P and not to A? Certificate authorities and hash functions were created to solve this problem. When person 2 (P2) wants to send a message to P, and P wants to be sure that A will not read or modify the message and that the message actually came from P2, the following method must be used:

- P2 creates a symmetric key and encrypts it with P's public key.
- P2 sends the encrypted symmetric key to P.
- P2 computes a hash function of the message and digitally signs it.
- P2 encrypts his message and the message's signed hash using the symmetric key and sends the entire thing to P.
- P is able to receive the symmetric key from P2 because only he has the private key to decrypt the encryption.
- P, and only P, can decrypt the symmetrically encrypted message and signed hash because he has the symmetric key.
- He is able to verify that the message has not been altered because he can compute the hash of received message and compare it with digitally signed one.
- P is also able to prove to himself that P2 was the sender because only P2 can sign the hash so that it is verified with P2 public key.

Phishing and Spear Phishing Attack

Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.

Spear phishing is a very targeted type of phishing activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against. One of the simplest ways that a hacker can conduct a spear phishing attack is email spoofing, which is when the information in the "From" section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company. Another technique that scammers use to add credibility to their story is website cloning — they copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials.

To reduce the risk of being phished, you can use these techniques:

- **Critical thinking** — Do not accept that an email is the real deal just because you're busy or stressed or you have 150 other unread messages in your inbox. Stop for a minute and analyze the email.
- **Hovering over the links** — Move your mouse over the link, but do not click it! Just let your mouse cursor h over over the link and see where would actually take you. Apply critical thinking to decipher the URL.
- **Analyzing email headers** — Email headers define how an email got to your address. The "Reply-to" and "Return-Path" parameters should lead to the same domain as is stated in the email.
- **Sandboxing** — You can test email content in a sandbox environment, logging activity from opening the attachment or clicking the links inside the email.

Drive- by Attack

Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike many other types of cyber security attacks, a drive-by doesn't rely on a user to do anything to actively enable the attack — you don't have to click a download button or open a malicious email attachment to become infected.

A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack of updates.

To protect yourself from drive-by attacks, you need to keep your browsers and operating systems up to date and avoid websites that might contain malicious code. Stick to the sites you normally use — although keep in mind that even these sites can be hacked.

Don't keep too many unnecessary programs and apps on your device. The more plug-ins you have, the more vulnerabilities there are that can be exploited by drive-by attacks.

Password Attack

Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing. The last approach can be done in either a random or systematic manner:

- Brute-force password guessing means using a random approach by trying different passwords and hoping that one work some logic can be applied by trying passwords related to the person's name, job title, hobbies or similar items.

- In a dictionary attack, a dictionary of common passwords is used to attempt to gain access to a user's computer and network. One approach is to copy an encrypted file that contains the passwords, apply the same encryption to a dictionary of commonly used passwords, and compare the results.

In order to protect yourself from dictionary or brute-force attacks, you need to implement an account lockout policy that will lock the account after a few invalid password attempts. You can follow these account lockout best practices in order to set it up correctly.

SQL Injection Attack

SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for example, instead of the login or password) in order to run predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system.

For example, a web form on a website might request a user's account name and then send it to the database in order to pull up the associated account information using dynamic SQL like this:

"SELECT * FROM users WHERE account = '" + userProvidedAccountNumber +"';"

While this works for users who are properly entering their account number, it leaves a hole for attackers. For example, if someone decided to provide an account number of "' or '1' = '1'", that would result in a query string of:

"SELECT * FROM users WHERE account = '' or '1' = '1';"

Because '1' = '1' always evaluates to TRUE, the database will return the data for all users instead of just a single user.

The vulnerability to this type of cyber security attack depends on the fact that SQL makes no real distinction between the control and data planes. Therefore, SQL injections work mostly if a website uses dynamic SQL. Additionally, SQL injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. J2EE and ASP.NET applications are less likely to have easily exploited SQL injections because of the nature of the programmatic interfaces available.

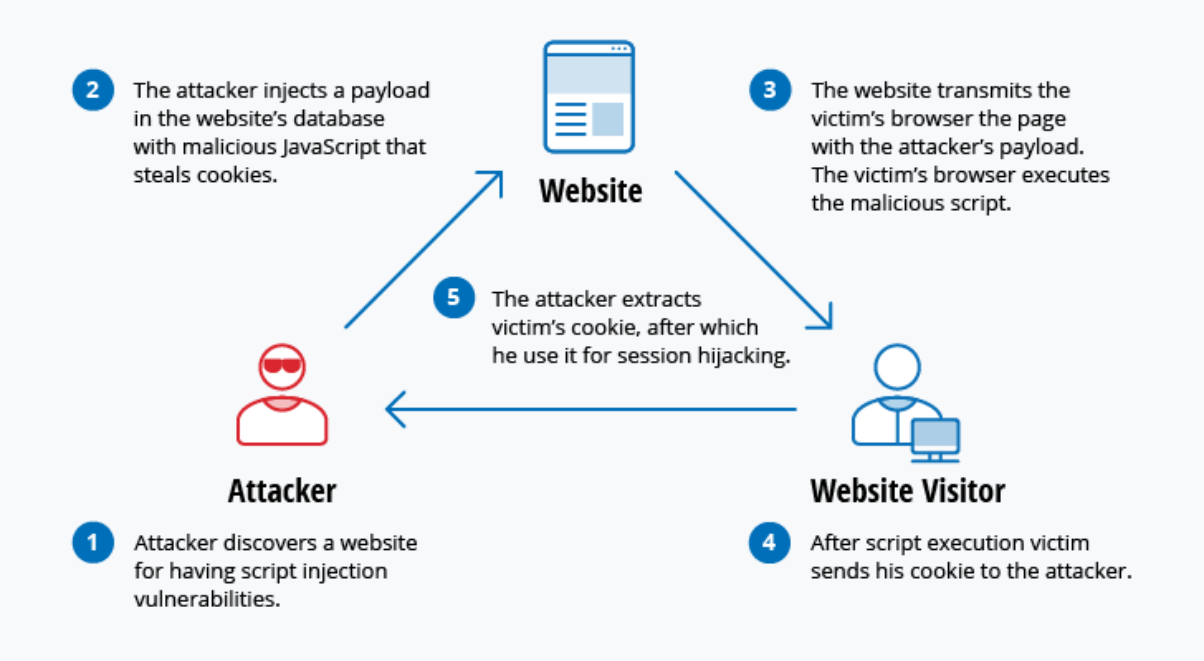
In order to protect yourself from a SQL injection attacks, apply least0privilege model of permissions in your databases. Stick to stored procedures (make sure that these procedures don't include any dynamic SQL) and prepared statements (parameterized queries). The code that is executed against

the database must be strong enough to prevent injection attacks. In addition, validate input data against a white list at the application level.

Cross-site scripting (XSS) Attack

XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website's database. When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script.

For example, it might send the victim's cookie to the attacker's server, and the attacker can extract it and use it for session hijacking. The most dangerous consequences occur when XSS is used to exploit additional vulnerabilities. These vulnerabilities can enable an attacker to not only steal cookies, but also log key strokes, capture screenshots, discover and collect network information, and remotely access and control the victim's machine.



While XSS can be taken advantage of within VBScript, ActiveX and Flash, the most widely abused is JavaScript — primarily because JavaScript is supported widely on the web.

To defend against XSS attacks, developers can sanitize data input by users in an HTTP request before reflecting it back. Make sure all data is validated, filtered or escaped before echoing anything back to the user, such as the values of query parameters during searches. Convert special characters such as ?, &, /, <, > and spaces to their respective HTML or URL encoded equivalents. Give users the option to disable client-side scripts.

Eavesdropping Attack

Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network. Eavesdropping can be passive or active:

- **Passive eavesdropping —** A hacker detects the information by listening to the message transmission in the network.
- **Active eavesdropping —** A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.

Detecting passive eavesdropping attacks is often more important than spotting active ones, since active attacks requires the attacker to gain knowledge of the friendly units by conducting passive eavesdropping before.

Data encryption is the best countermeasure for eavesdropping.

Birthday Attack

Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature. A message processed by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message; this MD uniquely characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user's message with his, and the receiver will not be able to detect the replacement even if he compares MDs.

Malware Attack

Malicious software can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet. Here are some of the most common types of malware:

- **Macro viruses —** These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.
- **File infectors —** File infector viruses usually attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded. Another version of a file infector associates itself with a file by creating a virus file with the same name, but an .exe extension. Therefore, when the file is opened, the virus code will execute.
- **System or boot-record infectors —** A boot-record virus attaches to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.
- **Polymorphic viruses —** These viruses conceal themselves through varying cycles of encryption and decryption. The encrypted virus and an associated mutation engine are

initially decrypted by a decryption program. The virus proceeds to infect an area of code. The mutation engine then develops a new decryption routine and the virus encrypts the mutation engine and a copy of the virus with an algorithm corresponding to the new decryption routine. The encrypted package of mutation engine and virus is attached to new code, and the process repeats. Such viruses are difficult to detect but have a high level of entropy because of the many modifications of their source code. Anti-virus software or free tools like Process Hacker can use this feature to detect them.

- **Stealth viruses —** Stealth viruses take over system functions to conceal themselves. They do this by compromising malware detection software so that the software will report an infected area as being uninfected. These viruses conceal any increase in the size of an infected file or changes to the file's date and time of last modification.
- **Trojans —** A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers. For example, a Trojan can be programmed to open a high-numbered port so the hacker can use it to listen and then perform an attack.
- **Logic bombs —** A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.
- **Worms —** Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. Worms are commonly spread through email attachments; opening the attachment activates the worm program. A typical worm exploit involves the worm sending a copy of itself to every contact in an

infected computer's email address In addition to conducting malicious activities, a worm spreading across the internet and overloading email servers can result in denial-of-service attacks against nodes on the network.

- **Droppers —** A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.
- **Ransomware —** Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.
- **Adware —** Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically.
- **Spyware —** Spyware is a type of program that is installed to collect information about users, their computers or their browsing habits. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.

Activity

Trainer will take the participants to the computer lab and ask the participants to do internet research on CyberAttack.
