Overview of Cybersecurity Threats, Vulnerabilities and Attacks

Tech-Webinar
On 12th May 2020 organized jointly by IETE and SETS

Speaker:
Dr. Reshmi TR
Scientist,
Society for Electronic Transactions and Security (SETS),
Chennai, India

Outline

1. Introduction
2. Malwares and Malicious Codes
3. Deception Techniques
4. Attacks
5. Managing Cyber Threats and Risks
6. Conclusion

Introduction

Need for Cybersecurity

- There are numerous examples of cyber hacks in the current internet.
- Enterprise systems keeps updating their security product designs and substantially upgrades the cybersecurity technologies and practices.
- Additionally, governments and industries are also introducing more regulations and mandates better data protection and security controls to help guard big data generated into internet.

Cybersecurity

- The **Cyberattacks** are aimed at accessing, changing, or destroying sensitive information
- **Cybersecurity** is the practice of protecting systems, networks, and programs from attacks.
- A **Cybersecurity threat** is the possibility that a harmful event, such as an attack, will occur
- **Cyber vulnerability** is a weakness that makes a target susceptible to an attack
- Cyber threats are particularly dangerous to certain industries and the type of information they collect and protect. https://threatmap.checkpoint.com/

Cybersecurity Threats

Internal Security Threats

They may also have knowledge of security countermeasures, policies and higher levels of administrative privileges.

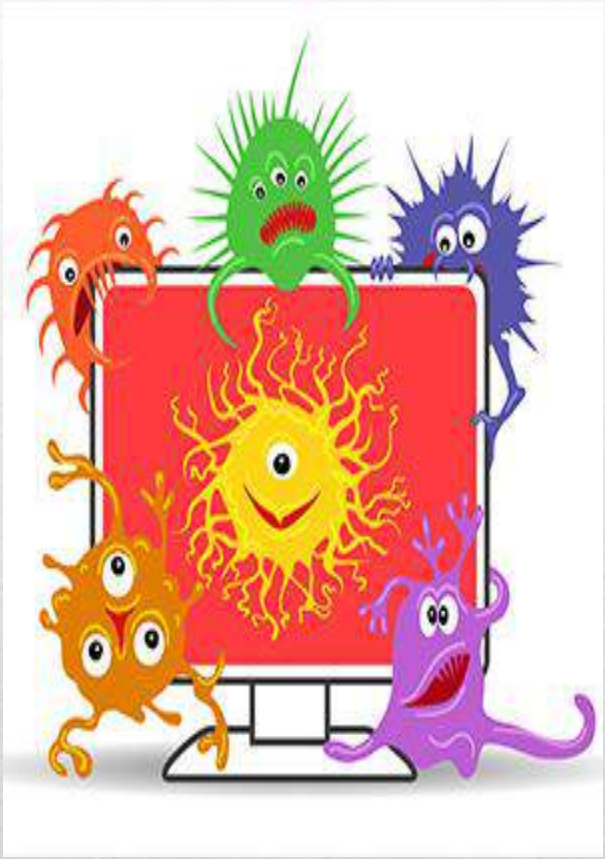
External Security Threats

External threats from amateurs or skilled attackers can exploit the weaknesses or vulnerabilities to gain access to internal resources.

Malwares and Malicious Code

Malwares

- Malware is the **collective name** for a number of malicious software variants, including viruses, ransomware and spyware.
- Delivered in the form of a **link or file** over email or other sources and requires the user to click on the link or open the file to execute the malware.
- **Creeper virus** - first appeared in early 1970s
- Now the world is under attack from hundreds of thousands of different malware variants, all with the **intent of causing the most disruption and damage** as possible.



Types of Malwares

Cyber criminals target user's end devices through the installation of malware.

Viruses - A virus is **malicious executable code attached to another executable file**, such as a legitimate program. Most viruses require end-user initiation, and can activate at a specific time or date.

Worms - Worms are malicious code that **replicates by independently exploiting vulnerabilities** in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, worms no longer require user participation.

Trojan horse - A Trojan horse is malware that **carries out malicious operations under the appearance of a desired operation** such as playing an online game. A Trojan horse differs from a virus because the Trojan binds itself to non-executable files, such as image files, audio files, or games.

Types of Malwares (Cont.)

- **Logic Bomb** - A logic bomb is a malicious program that **uses a trigger to awaken the malicious code.** For example, triggers can be dates, times, other programs running, or the deletion of a user account. The logic bomb remains inactive until that trigger event happens.
- **Ransomware** - Ransomware holds a computer system, or the data it contains, captive until the target makes a payment. Ransomware usually **works by encrypting data** in the computer with a key unknown to the user.
- **Backdoors and Rootkits** - The **backdoor bypasses the normal authentication** used to access a system. A rootkit modifies the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely.

Email and Browser Vulnerabilities & Attacks

Email is a universal service used by billions worldwide and has become a major vulnerability to users and organizations.

Spam - Spam, also known as **junk mail**, is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content.

Spyware - Spyware is software that enables a criminal to **obtain information about a user's computer activities**. Spyware often includes activity trackers, keystroke collection, and data capture.

Email and Browser Vulnerabilities & Attacks

Adware **displays annoying pop-ups** to generate revenue for its authors. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.

Scareware **encourages the user to take a specific action based on fear.** Scareware forges pop-up windows that resemble operating system dialogue windows.

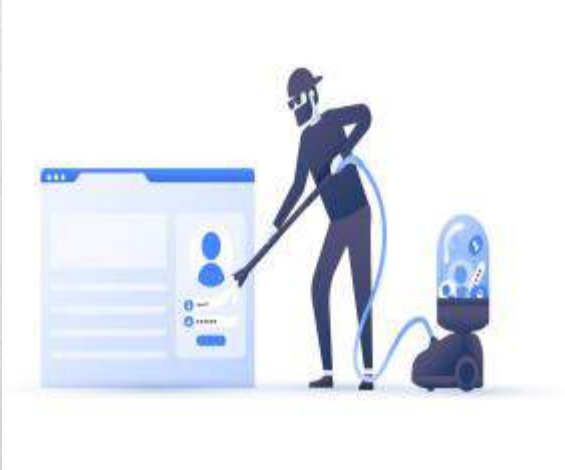
Email and Browser Vulnerabilities & Attacks

Phishing -. In Phishing, a malicious party sends a **fraudulent email disguised as being from a legitimate, trusted source**. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

Spear phishing - Spear phishing is a **highly targeted phishing attack**. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person.

Email and Browser Vulnerabilities & Attacks

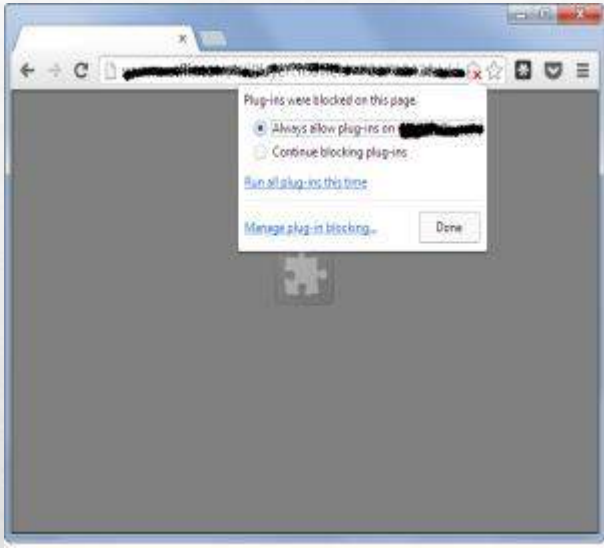
Vishing - Vishing is **phishing using voice communication** technology. Criminals can spoof calls from legitimate sources using voice over IP (VoIP) technology. Victims may also receive a recorded message that appears legitimate. https://www.youtube.com/watch?v=lc7scxvKQOo&feature=youtu.b



Pharming - Pharming is the **impersonation of a legitimate website** in an effort to deceive users into entering their credentials.

Whaling - Whaling is a phishing attack that **targets high profile** within an organization such as senior executives.

Email and Browser Vulnerabilities & Attacks



Plugins – There are plugins which **enhance the look and feel of a web page.** Attacker execute malicious codes through these plugins.

SEO Poisoning - SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. While many legitimate companies specialize in optimizing websites to better position them, SEO poisoning uses SEO to make a **malicious website appear higher in search results.**

Browser Hijacker - A browser hijacker is **malware that alters a computer's browser settings to redirect** the user to websites of cyber criminals. Browser hijackers usually install without the user's permission and is usually part of a drive-by download.

Top 10 OWASP vulnerabilities in 2020

1. Injection - sends invalid data to the web application
2. Broken Authentication - bad session management prone to username enumeration
3. Sensitive Data Exposure - compromising data that should have been protected
4. XML External Entities (XXE) - XML input with reference to an external entity is processed by a weakly configured XML parser
5. Broken Access control – Misconfigured access policies
6. Security misconfigurations – Misconfiguration in different levels such as application, network, server etc.
7. Cross Site Scripting (XSS) – injection into running script in client end
8. Insecure Deserialization – Converting byte strings to objects in an insecure environment
9. Using Components with known vulnerabilities – using vulnerable components/assets
10. Insufficient logging and monitoring – insufficient administrative steps for security

Deception Techniques

The Art of Deception

Deception is an act of making someone believe something that is not true. The deception techniques used to launch attacks are:

Social Engineering - Social engineers often rely on people's willingness to be helpful but also **prey on people's weaknesses.** These are some types of social engineering attacks:

Pretexting - This is when an attacker **calls an individual and lies to them in an attempt to gain access** to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

Something for Something (Quid pro quo) - This is when an attacker **requests personal information from a party in exchange for something**, like a gift.

Types of Deception Techniques

Shoulder Surfing and Dumpster Diving – refers to picking up PINs, access codes or credit card numbers. An attacker can be in **close proximity to his victim** or the attacker can use binoculars or closed circuit cameras to shoulder surf.

Impersonation and Hoaxes - Impersonation is the action of **pretending to be someone else.** For example, the phone scam targeting taxpayers.

Piggybacking and Tailgating - Piggybacking occurs when a **criminal tags along with an authorized person** to gain entry into a secure location or a restricted area. Tailgating is another term that describes the same practice.

Attacks

Types of Cyber Attacks

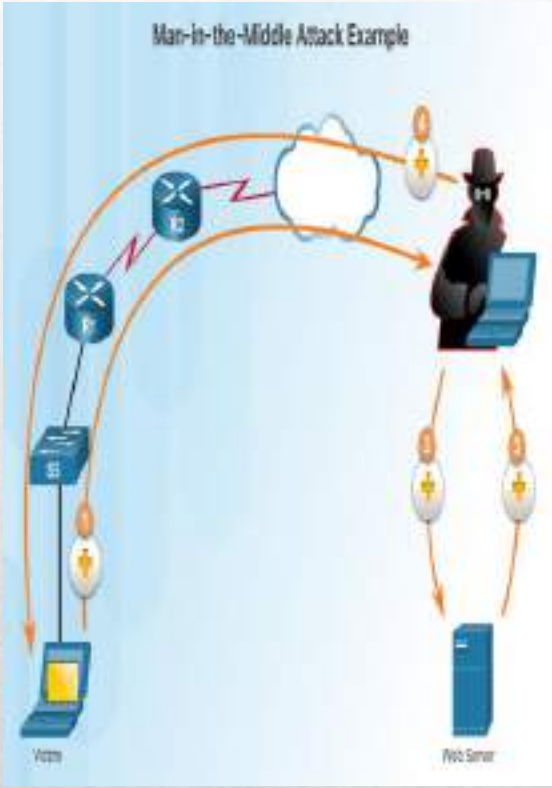
Denial-of-Service (DoS) Attacks - **cause interruption of services to users, devices, or applications.** DoS attacks are a major risk because they can easily interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled attacker.

Sniffing - Sniffing is similar to **eavesdropping on someone**. It occurs when attackers examine all network traffic as it passes through their communicating media, independent of whether or not the traffic is addressed to them or not.

Spoofing - Spoofing is an **impersonation attack, and it takes advantage of a trusted relationship between two systems.** If two systems accept the authentication accomplished by each other, an individual logged onto one system might not go through an authentication process again to access the other system.

Types of Cyber Attacks

Man-in-the-middle - The criminal **intercepts communications** between computers to steal information crossing the network. They can also **manipulate messages and relay false information** between hosts since the victim hosts are unaware that a modification to the messages occurred. The criminal take over the control of device without the user's knowledge.



Zero-Day Attacks is a computer attack that tries to **exploit software vulnerabilities that are unknown or undisclosed by the software vendor.**

Keyboard Logging - is a software program that **records or logs the keystrokes** of the user of the system. It can be a software installed or hardware physically attached to a computer. The keystrokes captured in the log file can reveal usernames, passwords, websites visited, and other sensitive information.

Wireless and Mobile Attacks

Grayware and SMiShing

- Grayware includes applications that behave in an annoying or undesirable manner. Grayware may be **unrecognizable malware concealed** within, but it still may pose a risk to the user.
- SMiShing is short for SMS phishing. It uses Short Message Service (SMS) to **send fake text messages**. Unsuspecting victims may then provide sensitive information such as credit card information or unknowingly download malwares.

Wireless and Mobile Attacks (Cont.)

Rogue Access Points - A rogue access point is a wireless access point installed on a secure network **without explicit authorization**.

RF Jamming - Wireless signals are susceptible to deliberate jamming. Radio frequency (RF) jamming **disrupts the transmission of a radio or satellite station** so that the signal does not reach the receiving station.

Bluejacking and Bluesnarfing - Bluejacking is the term used for **sending unauthorized messages** to another Bluetooth device. Bluesnarfing occurs when the **attacker copies the victim's information from his device**. This information can include emails and contact lists.

Wireless and Mobile Attacks (Cont.)

Wired Equivalent Privacy (WEP) is a security protocol used in WLAN

- For a layman the encryption is secure enough, but a person with bit of knowledge on wireless transmission protocols and the right tools **can decode the encryption key.**

Wi-Fi Protected Access (WPA), WPA2 and WPA3 - came out as improved protocols in each versions.

- WPA and WPA2 use a four-way handshake for authentication, which is vulnerable to an **offline attack**
- The attacker **exploit the option for downgrading** and using EAP authentication method these are also found to be vulnerable
- Moreover, in WPA3 an attacker can still **exploit a side channel attack** and determine encoding timing and execution information

Application Attacks

Cross-site scripting (XSS) - is a vulnerability found in web applications. XSS allows criminals to **inject scripts into the web pages** viewed by users. This script can contain malicious code. Cross-site scripting has three participants: the criminal, the victim, and the website.

Code Injections Attacks - There are several different types of databases such as a Structured Query Language (SQL) database or an Extensible Markup Language (XML) database. Both XML and SQL injection attacks **exploit weaknesses such as not validating database queries properly.**

Buffer Overflow - Buffers are memory areas allocated to an application. By **changing data beyond the boundaries of a buffer**, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.

Application Attacks

Remote Code Executions vulnerabilities allow a cybercriminal to **execute malicious code and take control of a system** with the privileges of the user running the application. Remote code execution allows a criminal to execute any command on a target machine.

ActiveX Controls and Java controls provide the capability of a plugin to Internet Explorer.

- ActiveX controls are **pieces of software installed by users** to provide extended capabilities. Third parties write some ActiveX controls and they may be malicious. They can monitor browsing habits, install malware, or log keystrokes. Active X controls also work in other Microsoft applications.
- Java operates through an interpreter, the Java Virtual Machine (JVM). The JVM enables the Java program's functionality. The JVM sandboxes or isolates untrusted code from the rest of the operating system. There are vulnerabilities, which **allow untrusted code to go around the restrictions imposed by the sandbox.**

Managing Cyber Threats and Risks

Managing Cyber Threats & Risks

An organization needs to **know what hardware and software assets** they have in order to protect them. This means that the organization needs to know all of components that can be subject to security risks, including:

- Every hardware system
- Every operating system
- Every hardware network device
- Every network device operating system
- Every software application
- All firmware
- All language runtime environments
- All individual libraries

.

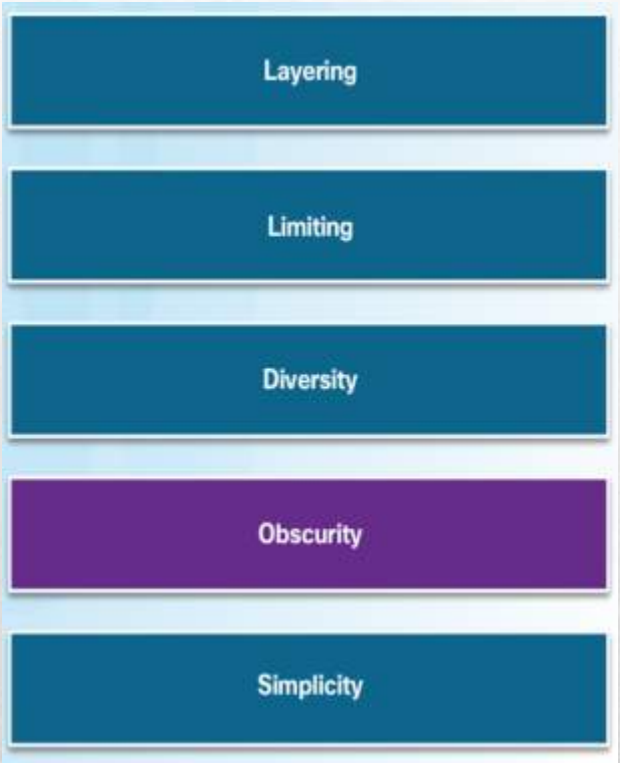
Managing Cyber Threats & Risks (Cont.)

- **Asset Classification -** **assigns all resources of an organization into a groups** based on common characteristics. An organization should apply an asset classification system to documents, data records, data files, and disks.
- **Asset Standardization** - as part of an IT asset management system, an organization **specifies the acceptable IT assets** that meet its objectives
- **Threat Identification** – The Common Vulnerabilities and Exposures (CVE) contains threats identified and each **CVE identification** contains a standard identifier number with a brief description and references. The threat identified by organization is analyzed with the vulnerability reports and advisories.
- **Risk Analysis -** is the process of **analyzing the dangers posed** by natural and human-caused events to the assets of an organization.
- **Mitigation -** involves **reducing the severity of the loss or the likelihood of the loss** from occurring. Many technical controls mitigate risks including authentication systems, file permissions, and firewalls.

Defense in Depth

Any defense in depth will not provide an impenetrable cyber shield, but help an organization to minimize risks

- **Layering** is creating a barrier of **multiple defenses** that coordinate together to prevent attacks.
- **Limiting** in an organization should **restrict access** so that users only have the level of access required to do their job.
- **Diversity** refers to **changing the controls and procedures** at different layers. Breaching one layer of security does not compromise the whole system.
- **Obscuring** can also protect data and information. An organization **should not reveal any information** that cyber criminals can use to figure out loop holes.
- **Simplicity** can actually **improve availability**. Complexity does not necessarily guarantee security and sometime cause misconfigurations or failure to comply



Conclusion

- The presentation discussed the requirement for cybersecurity.
- The presentation explained the threat of malwares and malicious codes.
- The presentation discussed the types of deception techniques used by cyber criminals
- The presentation explained the types of attacks.

Understanding these types of possible threats allows an organization to identify the vulnerabilities that the cyber attacker may target to launch the attack. The organization can then learn how to **defend itself against cybersecurity trickery and maneuvering.**

References

1. https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html
2. Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In *Proceedings of the 2020 IEEE Symposium on Security and Privacy-S&P 2020)*. IEEE.
3. http://www.whoishostingthis.com/blog/2015/06/01/8-worst-viruses/
4. http://www.howtogeek.com/228828/7-ways-to-secure-your-web-browser-against-attacks
5. https://www.consumer.ftc.gov/scam-alerts
6. https://www.consumer.ftc.gov/articles/0038-spam
7. http://www.exterminate-it.com/malpedia/ransomware-category
8. http://www.informit.com/articles/article.aspx?p=1350956
9. https://yourstory.com/2020/04/zoom-hacked-accounts-selling-dark-web-privacy-nightmare
10. https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/