Assignment-2 Final

CS 573 A - Introduction to Cyber Security

FALL 2021

Rajat Rajesh Shetty CWID: 10477484

Dept. Cyber Security

Stevens Institute of Technology

State of Global Cyber Security – 2036

Introduction

During the last fifteen years, since 2021, the world has become significantly more digitized, demanding the secure storage of all data and critical things that require cyber security. Cybersecurity involves several departments and organizations, it has proven to be a difficult problem for governments. With the advent of new technology, modern society is surrounded by internet-connected products and services. It's more challenging because of the threats' scattered and diversified nature.

Due to the exponential rise of information technology (IT) and business applications linked with it, Internet linkages have resulted in an increase in cyberattack occurrences, many of which have tragic and severe repercussions. It can occur in a variety of industries, including financial institutions, government institutions, educational institutions, and the health care industry, among others. Telecommunications, emergency communication systems, financial systems, defense systems, space, transport, land records, public essential services and utilities, law enforcement and security, and air traffic control networks, to name a few, are all supported by IT infrastructure. The threat is being increased by the country's growing interconnectedness and accessibility to computer-based systems that are critical to its economy. Cybersecurity will be implemented with the help of Artificial intelligence. Most companies will have a cloud that will have all the data related to the company and the Internet of things would be prevalent and the boundaries of the network wouldn’t exist anymore.

Major Cyber Security Threats

The primary cyber security dangers that our world faces may be divided into two categories:

1. Cybercrime
2. Cyberwarfare

1. Cybercrime:

Cybercrime is defined as the use of cyberspace, such as a computer, the internet, a smartphone, or other technological equipment, to commit a crime by an individual or a group. To carry out their crimes, cybercriminals make use of a variety of weaknesses in cyberspace. They utilize malware to take advantage of flaws in software and hardware architecture.

Cybercrimes can happen through various methods they are:

Attacks on the **Internet of Things** (IoT) — The Internet of Things (IoT) is growing more common by the day (according to Statista.com, the number of devices connected to the IoT has reached up to 120 billion since 2036).
Consumers benefit from connected gadgets, and many organizations are increasingly using them to save money by collecting massive volumes of useful data and improving corporate operations. However, as more devices become linked, the potential of cyber-attacks and viruses increases, making IoT networks increasingly susceptible. IoT devices may be exploited to cause chaos, overload networks, or shut down crucial equipment for financial gain once they are in the hands of hackers. One such example wherein a hacker might exploit the use of IoT would be if they get access to the robots that would be used to do your household works. So through IOT a malware can be installed and programmed in such a way that it might kill the person.

Autonomous Vehicles and Connected Cars – While autonomous vehicles and connected cars are already on the road. Onboard sensors in a connected automobile help it improve its functioning and the comfort of its occupants. According to a research titled "7 Connected Car Trends Fueling the Future," by 2040, an estimated 98% of new cars will be connected to the internet.
This advancement in automotive production and design provides hackers with yet another chance to attack flaws in vulnerable systems to steal sensitive data and/or injure drivers. Connected automobiles have severe privacy problems in addition to safety considerations. One of the prime examples for this threat would be that if an autonomous vehicle is been hacked by an intruder then they will be able to control the vehicle and this can be a life-threatening situation.

An effort to prohibit individuals from accessing a system or network resource is known as a **Denial-of-service** (DDoS) attack. It temporarily or forever pauses or suspends the services of a host connected to the internet.

Malware (malicious code) is computer software that is meant to create computer problems, acquire sensitive data, or gain access to private computer systems. Malware may be propagated through code, scripts, active content, and other applications. Malware refers to a wide range of malicious or intrusive software, including Trojan Horses, rootkits, worms, and adware.

2. Cyberwarfare

Future conflicts, it is claimed, will not be like past warfare waged on land, sea, or air. The revelations of Edward Snowden had indicated that cyberspace will be a

battlefield. During these, the missiles, drones of other countries can be hacked and safety will be a concern.

Major Cyber Security Protections

The major cyber security protections can be grouped into the following ways:

1. Multi-factor Authentication

Multi-factor authentication is a service that adds additional layers of security to the traditional password-based method of online identity. You would ordinarily input your login and password without two-factor authentication. You'll be asked to provide an extra authentication method, such as a Personal Identification Code, a separate password, or even your fingerprint if you utilize two-factor authentication. After entering your username and password, you'll be required to provide more than two additional authentication methods using multi-factor authentication.

2. Cyber Security threat Monitoring

Cyber security threat monitoring describes the process of detecting cyber threats and data breaches. IT infrastructure monitoring is a crucial part of cyber risk management, enabling organizations to detect cyber-attacks in their infancy and respond to them before they cause damage and disruption. As the modern workplace becomes increasingly cloud-focused and digitalized, the traditional network perimeter is blurring. Cyber threats are evolving to take advantage of new vulnerabilities that emerge daily. While the preventative security technology is capable of known signature-based threats, cyber security threat monitoring is required to identify more sophisticated threats that evade these controls.
cyber security monitoring helps organizations to:

- Detect a broader range of threats
- Reduce the time it takes to respond to attacks
- Comply with industry and regulatory requirements
- Prevent **DDoS** Attack

3. Cybersecurity with AI

Since we have already trained our system the AI would predict scenarios and specify prevention measures. AI will recognize sophisticated attacks, stop them and prevent similar attacks in the future and AI can be used to develop an antivirus that is based on

trained data. Also, AI-based configuration systems will be able to design inherently secure systems.

4. MAC Address Detectors of Unknown Devices

So every device that is connected to the internet has a unique MAC address. So when an intruder or a hacker tries to connect to your system or any database around the world we are tracking down that MAC address and filtering them and black them at the same time. By doing this we can keep the hacker getting into our system and thereby protecting our sensitive data.

5. Ensure that your software is up to date

As the data above demonstrate, ransomware assaults were a prominent threat vector for both businesses and consumers. One of the most important cyber security measures for combating ransomware is patching old software. This helps to eliminate major loopholes. Here are some helpful hints to get you started: Set your device to get system updates automatically. Ensure that your desktop web browser automatically gets and installs security updates. Keep your plugins, such as Flash and Java, up to date on your web browser.

6. Be on the lookout for phishing schemes via emails, phone calls, and brochures

Phishing attacks are pretty common and the easiest ones to implement. In phishing, the attacker pretends to be someone other than the sender to trick the receiver into handing out credentials, clicking a malicious link, or opening an attachment that infects the user's computer with malware, trojans, or zero-day vulnerability exploits. A ransomware assault is typically the outcome of this. In actuality, 90% of ransomware outbreaks are caused by phishing attempts.

Recommendations

There are the following recommendations from my side to world leaders:

1. Blockchain

Traditional security solutions are incapable of securing vehicle-to-vehicle communication and handling the massive volumes of data generated by automobiles. Through these information sessions, Attendees will learn how blockchain technology may be utilized to do this throughout the educational session. The secure, decentralized, and distributed ledger has the potential to increase the number of people traveling, the volume of commodities delivered, and the average vehicle speed while reducing traffic, accidents, and the total carbon impact.

2. Multi-Factor Authentication (MFA) is the first step (Add an Extra Layer of Security)

Multi-factor authentication (MFA) is the most secure way to protect your credentials, devices, and data. It adds a second level of verification to the process of acquiring account access. Even if a hacker figured out your password, MFA makes it almost hard for them to access your account since it requires a second and maybe third "factor" of authentication, such as a security token, your mobile phone, your fingerprint, or your voice. Multi-factor authentication offers the most bang for your buck when it comes to cybersecurity. Almost all reputable suppliers provide this as a standard feature or as a necessity.

3. Security Policies:

Security policies are a written collection of regulations established by an organization to guarantee that users having access to corporate technology and information assets follow the rules and standards related to information security. It is a written document in the organization that outlines how to safeguard the organization against dangers and how to deal with them if they arise.

1) It increases efficiency.

2) It upholds discipline and accountability

3) It can make or break a business deal

4) It helps to educate employees on security literacy

4. **Masking Layer of Protection of Email**

We've already gone through how to spot phishing scams and how to defend yourself from them. If you don't want to be conned by a hacker, you should use antivirus software to protect yourself against potentially malicious applications, programs, and software. So implementing a layer that would filter out the spam emails as well as click the link on those spam emails and discard them directly.

5. Offline security includes a reliable and updated antivirus and giving updates on the air.

You should also make use of a bit locker for the hard drive, which encrypts your hard drive if it is lost or stolen. Data extraction from an encrypted device is a difficult task. Also, back up your data so that you can return your gadget to working order in the event of an emergency