BUFFALO STATE
The State University of New York

Overview of Cybersecurity

Prof. Charles Arbutina
&
Prof. Sarbani Banerjee

Computer Information Systems Department

Google CS[4]HS

Did you know that :

- Last year, facebook admitted that since 2012, it has not properly secured the passwords of 600 million users

- More than 3.2 million records were exposed in the first half of 2020, with most occurring at medical or health-care organizations

- Last March, the SamSam virus infested nearly all of Atlanta’s city agencies, knocking out court scheduling, online-bill payments and airport Wi-Fi

Within last 2 weeks :

- Erie Community college restored its website after a malware attack
- It was reported Russia used internet bots and trolls to undermine Britain’s democracy since 2014
- Chinese hackers were indicted for attempted cybertheft of Covid-19 vaccine data
- It was reported Russia broke into the former UK trade secretary’s email account and made off with secret US-UK trade documents

What is Cybersecurity?

Cybersecurity (or Information Technology Security) is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks or cyber attacks by utilizing technologies and processes.

The **objective of cybersecurity** is to prevent or mitigate harm to—or destruction of—computer networks, applications, devices, and data.

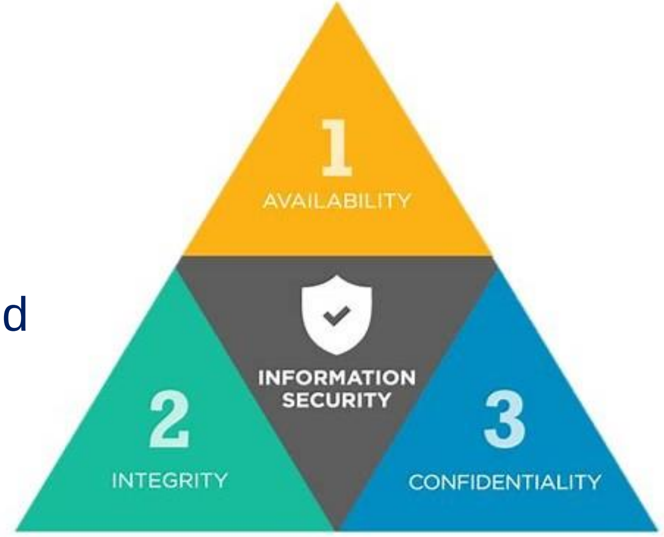
Cybersecurity assures that information retains (ICA):

1. **Integrity**
2. **Confidentiality**
3. **Availability**

CIA Triad: Fundamental Principles of Information Security

The Cybersecurity on a whole is a very broad term but is based on three fundamental concepts, “The CIA Triad“, consisting:

- **Confidentiality:** Keeping secrets secret
- **Integrity:** Ensuring information is not modified
- **Availability:** Keeping electronic doors open and IT shops humming



This model is designed to guide the organization with the policies of Cybersecurity in the realm of Information Security. Three Tenets of Information Security, The CIA Triad, is at the heart of information security.

Importance of Cybersecurity

Cybersecurity is **important** because it protects our sensitive data from theft & damage

- personally identifiable information (PII)
- protected health information (PHI)
- personal information
- intellectual property
- governmental and industry information systems

Cyberattacks can range from installing spyware on a personal computer to attempting to destroy the infrastructure of an entire nation. It has become increasingly sophisticated and dangerous.

Types of Cyber Threats

The threats countered by cybersecurity are three-fold:

1. **Cyber-crime** includes single actors or groups targeting systems for financial gain or to cause disruption.

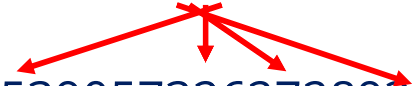
2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyber-terrorism** is intended to undermine electronic systems to cause panic or fear.

Examples of Cybercrime

- Identity theft and invasion of privacy
- Internet fraud
- ATM fraud
- Credit card fraud and wire fraud
- File sharing and piracy
- Counterfeiting and forgery
- Hacking, e-mail hacking and spamming
- Computer viruses
- Denial of service attacks
- Steganography
- Cyber harassment or cyber bullying and stalking
- Distribution of child pornography, human trafficking, spoofing
- Online libel or slander.

Steganography example



ATM card Account numbers	Pin	
1938273030351532	26153905732627289303	pin = 0725
1938694573728303	38273837161930382727	pin = 2017
1938740404938272	83727626406958372672	
1938598271261616	47236162839371618293	
2027337363626272	48937189393937267468	
2027293984443293	59484038271046072834	
2027124948838462	68373940387164050502	
2027847263843844	56274678362904050483	
2027462517282291	56947823729475619849	

Malware : A Malicious Software

Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

Trojans : A type of malware that is disguised as legitimate software, when uploaded to user's computer can cause huge damage.

Spyware: A program that secretly records what a user does, so that cyber- criminals can make use of this information.

Ransomware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Adware: Advertising software which can be used to spread malware.

Botnets: Networks of malware infected computers

Methods Used to Threaten Cybersecurity

Phishing: It is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

SQL injection: An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Man-in-the-middle: An attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service: An attack where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Recent Cyber Threats

Dridex malware: In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide. Dridex is a financial trojan with a range of capabilities.

Romance scams: In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data. The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million.

Emotet malware: In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware. Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

Types of Hackers

There are primarily three types of hackers – White Hat, Black Hat and Gray Hat hackers

Black Hat Hacker: is someone who maliciously searches and exploits vulnerabilities in computer systems or networks using malware and other hacking techniques to do harm.

White Hat Hackers: is a security specialist hired to find vulnerabilities in software, hardware and networks that black hats may target. Known as **ethical hackers**, they disclose all vulnerabilities to mgmt.

Grey Hat Hackers: A fusion of black and white, grey hats exploit security vulnerabilities without malicious intent, like white hats, but may use illegal methods to find flaws.

Red Hat Hackers: Characterized as vigilantes, they seek to disarm black hats. A red hat hacker could refer to someone who targets Linux systems.

Green Hat Hackers: Describes hacker wannabes who, though they lack technical hacking skills and education, are eager to learn the tricks of the trade.

Blue Hat Hackers: In Microsoft's world, blue hats acts much like white hats: They are employed by the company to find vulnerabilities in unreleased products.

Hacktivism: Hacking + Activism

Hacktivism has surfaced as people use the **Internet** to demonstrate for **political or social causes**. Those people are often called **Social Justice Warriors**. Common tactics used in hacktivism are following:

Doxing: Doxing, short for “docs” refers to the process of finding, sharing, and publicizing personally-identifying information of people on the web on a website, forum, or another publicly accessible venue. This could include names, addresses, phone, email and much more.

Denial of Service: This is more common types of hacktivism because it’s so effective. A DoS attack is the coordinated use of many computers to push a huge amount of traffic onto a website or internet-connected device, with ultimate goal being to make that device go completely offline.

Hacktivism: Hacking + Activism (Continued)

Data Breaches: Same as the idea of identity theft. The data breaches encroach on personally identifying information and use this data to commit fraud, apply for loans and credit cards, register fake accounts, and transfer money illegally, stealing intellectual property, launch phishing attacks, and much more.

Hijacking of Online Properties: This is more popular hacktivism activities, cracking the code into the back end of a targeted website with the intended effect of disrupting the website’s message in some way. This could include completely defacing the website itself or disrupting functionality so that users are unable to access it.

This last one also applies to hacking social media properties. Hacktivists gain access to their targets’ social media accounts and post information that supports their messages.

Different Types of Security

Network security: is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Information security: protects the integrity and privacy of data, both in storage and in transit.

Data security: the processes and decisions for handling and protecting data assets and databases.

Web Security: the practice of securing website – secured server (https).

Computer security: focuses on keeping computer devices and its OS free of threats.

Application security: a compromised application could provide access to the data its designed to protect.

Communication security: focuses on securing email, social network, social engineering

Internet of Things security: protects the gadgets and devices connected through Internet.

Cyber Safety Tips: Protect Against Cyberattacks

1. **Update your software and operating system:** This means you benefit from the latest security patches.
2. **Use anti-virus software:** Security solutions will detect and removes threats. Keep your software updated for the best level of protection.
3. **Use strong passwords:** Ensure your passwords are not easily guessable.
4. **Do not open email attachments from unknown senders:** These could be infected with malware.
5. **Do not click on links in emails from unfamiliar websites:** This is a common way that malware is spread.
6. **Avoid using unsecure WiFi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.

Recovery and Prevention

- **Disaster Recovery** defines how an organization responds to a cyber-security incident that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event.

- **Business Continuity** is the plan the organization falls back on while trying to operate without certain resources.

- **End-user Education** addresses the most unpredictable cybersecurity factor: PEOPLE. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives and other lessons is vital for security of any organization.

- **Access control** is primarily of two types: physical and logical.

  Physical access control limits access to buildings, rooms and physical IT assets.

  Logical access control limits connections to computer networks, files and data.

Questions/Comments

Thank You!