Learning Outcomes

Upon completion this module, students will be able to:
• Recall significant evolution of cybersecurity
• Recall principles of cybersecurity
• Distinguish Confidentiality, Integrity, and Availability concepts
• Recall different types of vulnerabilities of cyber systems
• Distinguish different cyber threats
• Explain countermeasures

Module Outline

• Evolution of cyber
• Basic principles of cybersecurity
• Related concepts of vulnerability, actors, and threats
• Countermeasures

Evolution of Cyber
**Evolution of Cybersecurity – First Uses**

Cybernetics: It is coined in the late of 1940s. Cybernetics is the field of communication and control systems in live beings and machine. The origin of the word comes from the Greek phrase “kubernetes”, steersman, and cyber from “kubernan” to steer [Oxford Dictionary].

Cyberspace: the term was first coined by William Gibson, a science fiction author, in his novel Neuromancer in 1984 [Carr, 2009].

- Later, cyber got a lot of attention and has been used as a prefix like cyberfriend, cybersnob, cyborg, cybersecurity, cyber-crime, cyberwarfare and so on [New York Magazine, 1993].

What was cyberspace like back in 1990s?
- https://www.youtube.com/watch?v=4I­fMM9RESSM

**Current Importance of Cyber**

- **Business perspective**
  - Critical infrastructures, business continuity
  - E-commerce
  - Blue prints, digital assets, trade secrets
  - Employee information

- **Individual perspective**
  - We have a digital persona that can shop, read, communicate, and work in cyber domain.
  - Bank accounts
  - Privacy

**Current Importance of Cyber (Cont.)**

WEF (2016) Global risks perception survey; Top 5 trends that determine global developments:

- Rising income and wealth disparity
- Changing climate
- Increasing polarization of societies
- Rising cyber dependency
- Ageing population

**Exercise 1**

- Hardly a day goes by without media talking about “Cybersecurity”. Write a short perspective in response to “what is a cybersecurity”?

- Who should care the most about cybersecurity? Individuals, IT specialists, organizations, businesses, governments etc.?
Cyber and Security

- Now cyber means: "of, relating to, or involving computers or computer networks" according to Merriam-Webster dictionary.
- Cybersecurity is the protection of the systems, network, data, information stored or transmitted electronically or the measures to prevent insecurity

Importance of Cybersecurity

- In 2017, global cybersecurity spending is expected to be $120B whereas it was $3.5B in 2004 (Morgan, 2017).
- Cybercrime cost are expected to be $2.1 trillion globally by 2019 (Morgan, 2016).
- As cybercrime cost mounts, organizations invest more in cybersecurity to protect their trade secrets, business continuity, and supply-chain network.

Importance of Cybersecurity (Cont.)

- In 2015, U.S. firms ranked cyber as their 5th most important risk (AON Inpoint, 2017).
- World Economic Forum (2016) defined cyber attacks were in the top 5 cyber attacks in 2014 in terms of likelihood, as well as Critical information infrastructure breakdown in terms of impact.

Data Breaches and Its Cost

- Target, 2013, 70 million customers credit card information were stolen,
- Chase, 2014, 83 million customers information,
- Home Depot, 2014, 56 million customers credit cards were stolen
- Office of Personnel Management, 2015, 25 million people affected, security clearance info were stolen
- Ashley Madison, 40 million users’ confidential information were stolen
- Ukraine power grids, 2016, blackout for 1 hour
Basic Principles of Cybersecurity

CIA – Confidentiality, Integrity, and Availability

Information (cyber) security includes three overarching characteristics:

- Confidentiality
- Integrity
- Availability

Confidentiality

Illegitimate users cannot read sensitive information on a computer or while it is moving across a network. Encryption techniques and tools provide confidentiality, thus, malefactors cannot read data or information.

Integrity

Integrity ensures that malicious actors cannot adjust or destroy information, whether it is on a computer or traveling across a network. If information is changed or destroyed, receiver can find out what is changed.
Availability

Availability ensures maintaining authorized people to access information. Distributed Denial of Service attacks are one of the attacks that prevent legitimate users to access the server, or file by compromising availability of networks or systems.

Exercise 2

Match each statement with the relevant term of confidentiality, integrity and availability.

1. I need to encrypt my emails to prevent unauthorized access.
2. Someone changed my Facebook profile photo without my knowledge.
3. I cannot print out my papers since I have no connection to the printer.

General Types of Cyber Insecurity

- Malicious
- Non-malicious
- Sequence & combinations of both types of cyber insecurity

Physical Impacts of Cyber Attacks

- Cyber attacks are more than stealing credit card information, passwords or hacking websites. For a while, cyber attacks cause physical impacts such as shutting down power grids in Ukraine (2016), malfunctioning centrifuges in a nuclear plant in Iran (year), or Australian sewage plant case
- As dependency of the Internet increases in professional world, it also poses a great threat.
- Smart homes, smart cities and so on can make human life more comfortable but can also lead to a chaos.
- Stuxnet was the first case that a cyber attack can cause a physical loss/damage/impact.
- Later, other cyber attacks caused more physical impact such as hardware loss through gaining control over Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs).
How Stuxnet Worked? (Kushner, 2013)

1. Infection: Stuxnet infects a system via a USB removable disk and proceeds to infect other Microsoft Windows machines. With a valid counterfeit digital certificate, it evaded detection.
2. Search: Stuxnet checks if a machine was part of the targeted industrial control system made by Siemens. Iran employed Siemens products to run its high speed centrifuges that help to enrich nuclear fuel.
3. Update: if the malware was in correct version it tried to access the Internet to download the updated version of itself. If the system was not a target, then, it did nothing.
4. Compromise: the worm exploited zero-day vulnerabilities.
5. Control: it took command and control of the centrifuges to degrade the centrifuges.
6. Deceive and Destroy: after it got the control, it was able to generate false feed-back that deceived engineers.

The malware’s goal was slowing down the process rather than shutting it down (Nakashima and Warrick, 2012). The failure of the centrifuges made Iranian engineers thought that the failure was caused by a technical error.

Impact of Stuxnet

- Stuxnet did not only has impact on Iran but also Indonesia, India, Azerbaijan, USA, Pakistan and other countries (Shearer, 2013)
- The malware damaged about 1,000 of Iran’s 6,000 centrifuges. The engineers thought it was a technical failure but it was a malware. Iran spent money to renew its damaged centrifuges.
- The malware slowed down Iran for two years and kept them from developing a nuclear bomb.
- Stuxnet is a milestone in cyberattack that caused physical loss.
- 50,000 infected Windows computers and 14ICS systems in Germany, according to Siemens report. (Scheiner, 2010)

Major Concepts of Cybersecurity

- Vulnerabilities
- Actors
- Threats
Cyber Vulnerabilities

Vulnerability

- Generic definition: openness to attack or damage
- In the context of cybersecurity: openness (of a system) to attack or damage affecting confidentiality, integrity, and availability of information

Bases of Vulnerabilities

- People
- Process
- Technology

Technology-Based Vulnerabilities

- Vulnerability is a flaw in a software that provides a means for malware to be installed and executed, often without signaling its presence
- Therefore suppliers create and publish software “patches” to close known vulnerabilities.
- Vulnerabilities pose exploits. A threat agent exploits a vulnerability by carrying out a threat.
- Hackers go after the low hanging fruits.
  - Example: hacked smart toilets in Japan (IoT) Link: https://www.youtube.com/watch?v=b0RInnX7FEd
  - These easily hacked systems have in common poor or no authentication, and weak, default, or hard-coded passwords
  - Unsecure security cameras: insecam.org
Exercise 3

When do you change your passwords?
- Periodically
- Rarely
- Never

How strong are your passwords?
- Very Strong (it includes numbers, symbols, upper-case and lower-case letters)
- Strong
- Fair
- Weak

People-Based Vulnerabilities

- Is Human center of the universe? Is human weakest chain of the link?
- Social Engineering: “any act that infulences a person to take an action that may or may not be in their best interest.” www.social-engineer.org, 2017.
- Based on the emotions of humans, social engineering means might cause more damage than other sophisticated attack types.
- They are different types of social engineering types in terms of cyber
  - Baiting, smishing, vishing, phishing and spear phishing

Social Engineering Types

Social engineering is a very old trick apart from cybersecurity. Based on the feelings such as fear, ambition, anxiety, targets might fall into the trap.

One of the oldest social engineering trick is Trojan Horse that mentioned in Iliad of Homer. Greeks couldn’t win the war which lasted 10 years, but then, they came up with an idea. Building a horse made of ships’ wood and presented to Trojans as a sign of regret and glory of Trojans. Of course, Trojans took the bait, and took the horse in the castle. However, in the night, Greek soldiers hidden in the horse came out of the horse and opened the doors to Greek soldiers and eventually Greeks conquered the city of Troy.

Hackers use other tools to get private info of the targets:
- Baiting: Social engineering threats do not have to be online. They can also occur offline. Another way to influence victim is giving USB stick which is already infected with a worm, trojan etc. as a gift or deliberately dropping it. When someone plug it into her computer, and open the files, then malware inject itself onto the computer.

Social Engineering

- Smishing: it involves text messages instead of emails occur in phishing. The goal is same; retrieve the confidential information of the victim such as passwords, user name etc. Since the use of smart phone is more than computer, smishing poses greater danger than phishing. There are more than 200 million smartphone users in the US (Statista, 2017)
- Hackers use text messages to deceive targets sending a link in the text messages. It is easy for victims to fall into trap of fraudulent text messages which might look like genuine or from a trusted source.
- Vishing: deceiving people over telephone
Video: https://www.youtube.com/watch?v=ic7scxwKQOs
Social Engineering (cont’d)

**Phishing:** sending emails seem coming from a legitimate and trustable source to influence targets to click on the link or download the file. They are generally sent in bulk. They include general information instead of specific information of targets.
- Phishing emails might look like it is coming from your bank, school, job, or government.
  Scammers want you to type your user name, answer security questions, phone number etc. Emails look like genuine but when you pay attention to details like language of the email, color of the symbols, or the sender, it would not be hard to recognize they are fake. Subject title might deceive many people but focusing on detail helps to identify the phishing scammers.
- **Spear-phishing:** if targets enter some of her/his personal information on phishing emails, then, they are more vulnerable to specific phishing emails. Spear-phishing attacks are targeted at individuals or small group of people. Spear phising emails contain more specific information about victims and that make them more vulnerable to take the bait.
- attackers might get victims’ information via phishing emails, social media scan, trash box, and so on. According to the information the attacker gathers, s/he craft an email such as coming from his/her boss or physician or professor or bank. The emails might contain documents or links. It is more likely to believe in those emails (spear-phishing) than phishing emails.

Process-Based Vulnerabilities

- Prominent cybersecurity expert Bruce Schneier (2000) said “Security is a process, not a product.”
- Hiring security expert or purchasing the state of the art security does not solely solve the problems. Security process or design is maybe the most overlooked step for maintaining the security of enterprises.
- Security process is that what strategy the organization adapt to keep networks secure. It has no cost to design a security architecture/framework yet it has a great cost at the expense of organizations.

Cyber Actors

**Actors**

- Functional users
- Security Experts
- Insiders
- Hackers
- Penetration testers
- Organized crime
- Competitors
- Hacktivists and cyber-terrorists
- Law enforcement
- Nation states
- ...
Actors - Functional Users

- Individuals or organizations for whom the cyber system was meant to be functional
- Ex: Bank depositor for ATM machines, Students for university’s email service

Actors - Security Experts

- Individuals or organizations which generate strategies, defense tools, products and techniques against hackers and malware.
- Ex: CERT, McAfee, Bruce Scheiner

Exercise 4

Support or refute:

- All hackers are bad.
- Some hackers are useful.

Actors - Hackers

- Black hat hackers: malicious hacker
- Grey hat hackers: break into a system without permission and demand money to fix it, if rejected then might not damage the system.
- Crackers: break into systems with malicious intent. Gains unauthorized access, damage integrity of vital data or make systems unavailable.
- Script kiddies: use scripts created by sophisticated hackers to attack computer and network systems, and deface websites. Script kiddies have low technical skills and they are more dangerous because of their high numbers and available tools and scripts.
- White hat hackers: pen-testers to test the vulnerabilities of the organization with their permission – also falls under own Actor category
Motivation for Hacking

- According to "Bug Bounty Hacker Report 2016", hackers hack for:
  - 72% money
  - 70% fun
  - 66% challenge
  - 51% "to do good in the world"
  - 28% of hackers are full time students, and 15% are self-employed

Actors - Insiders

- IT personnel of a company may cause a great disturbance to organizations.
- S/he may sell confidential information or break into systems herself to destroy the organization. Since she would have the accessibility, it would be very easy to shut down the system.
- A current or a former employee can cause loss of money, reputation, hardware or software as an act of revenge.
- Therefore, to mitigate the risks, security processes should be established such as:
  - need to know principle
  - canceling former employees access
  - limiting current employees' access
  - changing password periodically

A Case Study on Insider’s Threat

Maroochy Shire sewage spill case (Australia, 2001), (Abrams and Weiss, 2008)

Timeline
- 1997-1999: Boden worked for Hunter Watertech firm
- December 1999: Boden resigned from Hunter Watertech
- December 1999: Boden applied for a position at Maroochy Shire Council
- January 2000: Boden was turned down by the city council
- February 9 – April 23, 2000: several errors of SCADA system
- March 2000: Hunter Watertech expert performed a system troubleshooting
- April 19, 2000: system program was run more than 30 times according to the logs
- April 23, 2000: Boden managed to disable alarms at four pumping stations. He used the identification of pumping station 4
- April 23, 2000: A police officer pulled him over and all equipment were found in the car
- 2001: Boden was sentenced to 2 years

Actors: Penetration Testers

- Penetration testers check security vulnerabilities of web-based applications, networks, and systems with the permission of that organization.
- It could be a proactive way to find out vulnerabilities before they are exploited by a hacker.
Actors: Organized Crime

- A group of criminals that target victims to demand money, extort information. These groups may carry out for someone else who pays them to get confidential information, trade secrets or blueprints.
- Ex: Ransomware attacks

Actors: Hacktivist

- An individual or a group that carries out cyberattack to draw attention to humanitarian or global problems such as global climate, freedom of speech, etc.
- Anonymous, conducted cyberattack to protest internet cut for Julian Assange.
- Telecomix provided Internet access using landlines to avoid state blockages of broadband networks during the Egyptian Revolution of 2011.
- LulzSec defaced PBS website and inserted a page included the title "FREE BRADLEY MANNING".

Actors: Cyber-Terrorists

- Group of hackers organize cyberattack to cause alarm, fear, or panic with a political ideology.
- Cyber-terrorist attacks aim more severe and permanent damage than hacktivism.

Actors: Competitors

- Competitors can be the sponsor of a cyberattack. Competitors could get competitive advantage of hacking other firms or slow down their service.
- There is a black market for ordering DDoS attack.
- Cost of renting botnets to initiate a high intensity DDoS attack of 50-100 Gbps on a commercial website for 24 hours is about $200,000 (RMS, 2016)
Actors: Law Enforcement

- Organizations that monitor cybercrimes.
- Ex: INTERPOL, NSA.

Actors: Nation States

- The attack is carried out by state-sponsored hackers.
- Important actors: USA, Russia, China, Israel.
- Examples:
  - Russians carried out a cyberattack to Georgia due to conflict between Russia and Georgia government. (DDoS attack to Georgian president's website, 2008)
  - Russia- Estonia: a series of cyberattack to slow down Estonian banks, public websites, newspapers and so on. The reason for the cyberattack was relocating the Bronze Soldier of Tallinn. Later, NATO Center of Excellence for Cyber Defense was founded in 2008 in Estonia.
  - Stuxnet case: a malware slowed down uranium enrichment projects in a nuclear plant of Iran. However, Iran was not the only victim. India was affected by the malware, too. Possible attackers were: US, Israel,

Security Processes

- Principle of least privilege: limit the privilege. An associate has access only to do his/her task.
- Continuously monitoring the end-points: watching firewalls, intrusion detection systems, routers, servers, keeping data logs.
- Risk analysis: according to risk score, secure the weakest chain in the link. Use the budget more wisely based on the risk score and vulnerabilities.
- Defense in depth: using multiple security tools, products and techniques.
- Content filtering: for spam or phishing emails
- Employee training: increase the awareness of employees against social engineering
- Set up a respond mechanism: define the protocol in case of attack or breach
- Pen testers or bounty hackers
- Watch the alerts, new malwares and security updates

Example of Technology-Based Vulnerability: Zer0-Day Vulnerabilities

- Zer0-day vulnerability: it refers to a flaw in a program that is unknown to producer.
- Zer0-day attack: vulnerabilities of a software resolved by releasing updates or patches by the producer firm. A firewall or antivirus program can only stop attacks what it is designed for. A zer0-day attack is that exploits a vulnerability that is not discovered yet by a firewall or antivirus program. Therefore, software update or patches are very important to keep the cyber security.
- Companies generally are vulnerable to zero-day attacks. A signature-based firewall can only stop this kind of attack after the signature of the attack is determined and put into the firewall.
Cyber Threats

Exercise 5

Name your top two security concerns when using the internet?

Threat

- Generic description: circumstance with the potential to adversely impact operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations
- In the context of cybersecurity: circumstance with the potential to adversely impact confidentiality, integrity, and availability of information
- In the military context:
  - Threat= capability x intent
  - Ex: for an aircraft, intent is anticipated with the flight pattern or situation of its active sensors (trackers) and capability is its payload.

Threat Taxonomy

- Physical attack: fraud, sabotage, theft, vandalism, information leak, terrorist attack
- Unintentional damage: due to human error; maintenance, third party, using unreliable sources, loss of information on cloud or on disks, lack of a proper planning
- Natural disasters: earthquake, flood, fire, radiation leak, explosion
- Failures / malfunction: failure of hardware or software
- Outage: absence of employee, internet outage
- Cyber-criminal/abuse: denial of service, identity theft, malware injection, social engineering, manipulating hardware or software, unauthorized activities, manipulating DNS, remote control, Advanced Persistent Threat
- Legal threats: violation of rules and regulations, failure to meet contractual requirements, abuse of personal data
- (Adapted from ENISA Threat Taxonomy, 2016)
Exercise 6a: Threat or Vulnerability?

- Cloud: a single entry point that can be accessed from anywhere
- This access can be abused in different ways:
  - Theft or destruction of data
  - DoS attacks
  - Hijacking of cloud service traffic and redirecting it to other sources of malicious content

Exercise 6b: Threat or Vulnerability?

- Social Media: could help hackers to gain information about victims and carry out social engineering attacks

Exercise 6c: Threat or Vulnerability?

- Exploit Kits: Exploit kits install malicious payload on attacked devices to exploit vulnerabilities. They are primary tools to install malware. They are developed not to be detected. Exploit kits are sold to people have less technical knowledge (so-called script kiddies) in underground market.

Threat Agents

- When threat actors realize the threat, they exploit the vulnerability. Every vulnerability does not have to be exploited. Hackers use very few of them to exploit a software or a system.
- Even physical security is important to maintain cybersecurity. Locking computers while leaving the desk might save organization from a chaos.
- Insiders have greatest danger potential. Since they have access to the network, they can infect the systems without detected.
- From a script kid to nation states, there are so many actors in cyber environment. The accessibility of malware can boost the number of incidents. Because as over time, attack sophistication roofed, yet, required knowledge to carry out those attacks significantly decreased.
Threats: examples

Exercise 7

What do you do when you receive a message from unknown sender with a link to an article that seems interesting?

- Click on the link.
- Delete the email.
- Just ignore it.
- Another action? Explain?

Malware

- Generic term for Malicious Software
- Hides with some useful software, message, document or data as a mask to exploit a vulnerability in systems

Malware Types

- Viruses, Trojan horses, Spyware, and Rootkits need a host program to keep their tracks hidden.
- Worms, Automated viruses, and Zombies (Botnets) live and spread out independently.*
Virus

- A kind of malware that attach itself to a legitimate program on the computer
- When infected programs are transmitted to other computers and run then, virus will attach itself to programs on those computers
- Can corrupt the system or damage the data.
- Payload a piece of code within a virus that carry out the damage

Trojan Horse

- Requires user interaction to launch
- Executable code embedded in an application and are launched when the application is launched
- E.g. a Trojan buried in a Word file attached to an email is launched when the Word file is opened
- May look like a legitimate system file, therefore, it is hard to detect
- It deletes a system file and take on the name of system file to hide itself
- Remote Access Trojans (RAT) gives the hacker remote control of computer of the victim

Spyware

- Tracks how a user use a computer and the internet and reports it to the spyware owner
- Can log keystrokes to capture your sensitive ID/password combinations or credit card number
- Types of spyware:
  - Cookies
  - Keystroke loggers
  - Password stealing spyware
  - Data mining spyware

Rootkits

- A set of programs on a system take control of the administrator via hiding from file system detection
- Can lead to access to all functions and services of the operating system
- Can allow actors to modify programs, delete files, or manage network traffic
- A rootkit can be categorized as (Stallings, Bauer, & Hirsch, 2013):
  - Persistent
  - Memory based
  - User mode
  - Kernel mode
  - Virtual machine based
  - External mode
Worms

- Spread without user interaction
- Stand-alone programs that do not link themselves to other programs
- Direct-propagation worms jump directly to computers that have vulnerabilities; they then use these computers to jump other computers

Adware

- Programs with embedded advertising, often delivered as a browser pop-up ad
- E.g., a malicious adware so-called Fireball infected 250 million computers worldwide. A China-based company Rafotech employees have been arrested. The company was accused of not only distributed the adware but also installing browser-hijacking malware on people’s system to spy on them.

Denial of Service Attack

- DoS occurs when an attacker tries to block the legitimate users to access information services via targeting computer and its network connections
- Compromise the Availability principle. Thus a legitimate user cannot access the website until the attack is mitigated (US-CERT, 2013).
- As a sample; an attacker can “flood” a Web server with so many fake requests. When those requests exceed the response capacity of the server, it would be unavailable to respond of legitimate users (Stallings&Brown, 2014).

Distributed Denial of Service (DDoS) Attacks

- Attacker takes control of other computers via a program called bots and becomes the botmaster and the other computers become botnets (Zombies)
- Botmaster defines where botnets will send illegitimate request and flood the server
- If network bandwidth of the server or network is not enough to respond all those request, then it will become unavailable and cannot respond request of valid users
Types of DDoS Attack (RMS, 2016):

- Volumetric attacks - a target network is flooded with data packets that cripple the available network bandwidth. These data packets result in very high volumes of traffic congestion, and cause disruption of the service, thus, legitimate users cannot access the server.
- Application-based attacks (aka Layer 7 attacks) - Application-based attacks that use covert instructions that modify functions or specific features of a website to excess to disable them.

Types of DDoS Attacks (Cont.)

- Protocol-based (TCP Connection) attacks - An attacker sends numerous TCP SYN segments to the victim server.
- Fragmentation attack - employs internet protocols for data re-aggregation as an attack vector to overload the processing power of a server.

Cost of DDoS Attacks

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume (gigabits per second)</td>
<td>1-10 Gbps</td>
<td>10-50 Gbps</td>
<td>50-100 Gbps</td>
<td>100+ Gbps</td>
</tr>
<tr>
<td>Website Vulnerability Threshold (number of visitors per month)</td>
<td>1 million</td>
<td>10 million</td>
<td>100 million</td>
<td>1 billion</td>
</tr>
<tr>
<td>Approximate global website ranking for vulnerability threshold</td>
<td>Top 100,000</td>
<td>Top 10,000</td>
<td>Top 1,000</td>
<td>Top 100</td>
</tr>
<tr>
<td>Daily attack rate (2014)</td>
<td>962</td>
<td>101</td>
<td>3.53</td>
<td>0.40</td>
</tr>
</tbody>
</table>

Main target of DDoS attacks are financial services, technology companies, public sector, and industrial companies (Ponemon Institute, 2016). Also, Ponemon report states DDoS attacks are more costly than other cyber attacks like malicious insiders, malicious code, web-based attacks, viruses, and so on.

Attack Maps
Ransomware

- Information are locked and encrypted through a clicked link or an installed malware
- Hackers threaten the users to pay money to decrypt the information and make it available again. If not paid, hackers might erase the info permanently.
  - Hackers use Bitcoin to be paid for ransomware
  - IBM study says more than 4,000 ransomware attacks were carried out each day of 2016.
  - Wannacy ransomware attack
  - Petya ransomware
- Social Engineering attacks

Exercise 8: Threat and Security Failure

Why are these threats to cyber security?

<table>
<thead>
<tr>
<th>Threats</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Worm</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trojan Horse</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DDoS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ransomware</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Common Countermeasures

- Encryption
- Hashing
- Authentication
- Authorization
- Accounting
Encryption (Reference)

- Cryptography comes from Greek kryptos “hidden, secret” and graphein “writing” (www.etymonline.com)
- The study of coding and patterns, includes cryptology and cryptanalysis
- A third party or adversaries cannot understand the communication between two parties

Kerckhoff’s Principle

- Secrecy of the key enables security. The principle was shaped at the end of 19th century by Dutch cryptographer Auguste Kerckhoffs.
- “A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.”
- In his article published in “Le Journal des Sciences Militaires”
- The concept is now applied in most encryption algorithms (DES, AES, and so on). The secrecy of the key is the provider of the security of the encrypted message.

Security Through Obscurity

- Security through obscurity (STO) is the philosophy that keeping the design or implementation of the system secret to outsiders. An example to STO concept is given by Bruce Schneier, Beyond Fear: thinking Sensibly About Security in Uncertain World pp. 211:
  - “At 3,106 carats, a little under a pound and a half, the Cullinan Diamond was the largest undamaged diamond ever discovered. It was extracted from the earth at the Premier Mine, near Pretoria, South Africa, in 1905. Appreciating the literal enormity of the find, the Transvaal government bought the diamond as a gift for King Edward VII. Transporting the stone to England was a huge security problem, of course, and there was much debate on how best to do it. Detectives were sent from London to guard it on its journey. News leaked that a certain steamer was carrying it, and the presence of the detectives confirmed this. But the diamond on that steamer was a fake. Only a few people knew of the real plan; they packed the Cullinan in a small box, stuck a three-shilling stamp on it, and sent it to England anonymously by unregistered parcel post.”
- Systems can have so many vulnerabilities, if no one knows its flaw, based on security through obscurity philosophy, systems can be protected. However, this idea is not welcomed in today information security concepts.
Symmetric and Asymmetric Encryption

Symmetric encryption
• Employs same key for both encrypting and decrypting
• Fast but has security concern: key distribution problem.
• DES, 3DES, RC4
• AES (Advanced Encryption Standard)

Asymmetric encryption
• Uses two keys, public and private
• No key distribution problem but slower than symmetric encryption
• Also known as Public Key Cryptography
• Public key is used to encrypt the message, and private key is used to decrypt the ciphertext.
• RSA: most popular employed

Both encryption methods can be combined. Public key encryption can be used to exchange keys, to encrypt communication and protect symmetric keys. Symmetric key encryption can be used when the performance is priority.

Hashing

• Hashing is the principle fall under Integrity. Integrity means that receivers get the exact message that senders transmit.
• Hashing provides that no bits are changed while messages are in transit.
• Hashing algorithms include: variable length input, fixed length output.
• Hashing is irreversible unlike encryption.
• A hashing algorithm is employed to a bit string of any length. Hash is the result of the calculation and all hashes have same length.
• Confidential information like passwords should always be kept in databases in hashed format. Thus, illegitimate users are prevented to get the passwords when they are stored or transmitted.

Hashing (Cont.)

• Paraphrase: The weakness of hashing algorithm or when a hashing algorithm should be retired is when it becomes easy to find multiple inputs that produce the same output message digest.
• MD5 and SHA-1 experienced this case
• Widely used hashing algorithms:
  • MD5
  • SHA-1
  • SHA-256 or SHA-2
• SHA-2 is more common today which is more secure than SHA-1

Authentication

• Authentication means users prove their identity to log in a system.
• Users need to type their password, use finger prints, retina scan (biometrics), or key fobs.
• If a user merges more than one of these methods, then, it is called multifactor authentication.
• Multifactor authentication is much safer than single authentication methods. Hackers would need both your password and key fob or finger print and so on. Therefore, multifactor authentication is union of one digital and one physical.
Exercise 9

What authentication methods do your bank use before you access your online or mobile banking account?

- Password only
- Password and one-time verification code text.
- Password and security questions.
- Another method? Explain?

Authorization

- After the authentication process, based on the user’s credentials, the system lets the user to access the network, websites and so on.
- Principle of least privilege prevents users unnecessarily to access confidential files and requires admin permission.
- Authorization beyond normal job tasks could help hackers to get confidential information and to violate confidentiality, integrity, and availability.

Principle of Least Privilege

- Principle of least privilege, principle of minimal privilege or principle of least authority is the notion that a user or a program should only have the minimum privileges required to carry out its duty. A user can only access the files that she needs and she is prohibited to access the files that requires admin permission.
- Benefits of the Principle of Least Privilege (Nate Lord)
  - Better security
  - Minimized attack surface
  - Limited malware propagation
  - Better stability
  - Improved audit readiness

Accounting

- Keeping records of logs and failed logins might help to solve a cybersecurity incident and provide valuable information to investigations.
- Data logs can help to understand change in pattern which could help to detect abnormal events.
Advanced Persistent Threat

- Advanced Persistent Threat (APT) is a type of cyberattack conducted by state-sponsored hackers to continuously steal data from a high-value organization without being detected or damaging the victim system.
- The aim of the attack is to get the secrets, financial advantage, reports, designs from industries like defense, entertainment, healthcare or pharmaceutical.
- Attackers conduct reconnaissance through search engines or social media. Then, they conduct social engineering attacks trying to get into the system. They generally targets admins or executives who have more accessibility.
- Once they get into the system, they create back doors to gain access to the compromised system. Then, they exploit zero-day vulnerability, JAVA vulnerability, Adobe or Microsoft, or SQL injection.

APT Example

- Mandiant revealed and located an APT group in China and named it APT1 which is connected to People’s Liberation Army
- According to the findings of Mandiant, APT1 stole hundreds of terabytes of data from more than 140 organizations
  - Intellectual property, business plans, pricing documents, emails, contacts, test results, and so on.
  - APT1 kept accessing to victim networks on average 356 days. The longest duration was 1764 days.
  - From 2011 to 2013, APT1 established at least 937 Command and Control servers mostly registered to China and the U.S.
  - It is estimated that APT1’s attack infrastructure has more than 1,000 servers.
- The headquarter employs thousands that includes linguists, researchers, malware and industry experts, soldiers
- They mostly carried out attacks on Information technology, aerospace, public administration, and satellites and telecommunications mostly using spear-phishing technique
- Yet, the emails had grammatical errors or typos

Summary

What is covered so far:
- Definition of cyber and cybersecurity
- Basic principles of cybersecurity- CIA
- Threats - Vulnerabilities - Exploits
- Actors in cybersecurity
- Case studies - Stuxnet and Maroochy Shire Sewage Spills
- Types of cyberattacks - tools and techniques
- Countermeasures - encryption, hashing, authentication, authorization, accounting
- Advanced persistent threats

References (1)

References (2)


• Risk Management Solutions, Inc., 2016; Managing Cyber Insurance Accumulation Risk; report prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge.


References (3)


• Burkett, R. (2013). An alternative framework for agent recruitment: From mice to rats


References (4)


• Weissman, J. (2017). Certificate Authority | 3.1 Cryptography | CYBER501x Courseware | edX. Retrieved August 28, 2017, from https://courses.edx.org/courses/course:/v1/RIT+edX/CYBER501x+1T2017/courseware/7e288565d3de36c0f139979f7c0a0c8d7/aaa6c5b0ba5114465a1532653706ce45?activate_block_id=block_10

References (5)


• DfVyzzypzVvyKruyo3TtZ05WBpEU4dWksQj2yAHSWHuW4IGywiUHdU9hU4hU9hG00MkVYTounpE8
References (6)