Introduction to Intelligent Security Systems

Alvin Lin

August 2018 - December 2018

Computer Security Basics

Computer Security revolves around the CIA triad of **confidentiality**, **integrity**, and **availability**.

- Confidentiality: the protection of information from unauthorized disclosure. Enforced through access controls, cryptography, and resource hiding.
- Integrity: the protection from unauthorized modification of information. This involves data integrity and origin integrity. Prevention mechanisms prevent unauthorized access and detection mechanisms report when information is no longer trustworthy.
- Availability: resources and services are usable and operational during a given time period despite attacks or failures.

Data can be made 100% confidential simply by destroying it, but then it is no longer available. Security involves availability because data must be available to authorized individuals in order to be secure.

Why is security important?

In the beginning, there was no external threat. Computer security was not an issue. Now, nearly all devices are networked and attackers no longer have to physically be at your computer in order to attack it.

Severity of Cyber Attacks

According to the US CERT:

- 4882 vulnerabilities were reported in 2005, with 79% launched remotely, and 62% leading to a disruption of service.
- 6604 vulnerabilities were reported in 2006, with 85% launched remotely, and 65% leading to a disruption of service.

In December 2006, NASA was forced to block emails with attachments before shuttle launches out of fear that they would be hacked. Many other large companies and organizations have also been breached, compromising large amounts of data.

Security and Privacy

In 2013, Edward Snowden copied and leaked classified information from the NSA. His disclosures revealed numerous global surveillance programs run by the NSA in cooperation with foreign governments and telecommunications agencies.

By now, we're all aware of the Equifax breach that exposed the social security numbers and sensitive information of 143 million Americans. The breach was discovered on July 29th, but hackers had breached their system from mid-May, giving them a month to work with all the leaked data.

The Dark Web

The Dark Web is a term that refers to a collection of websites that exist on an encrypted network and can not be accessed using traditional web browsers. Typically, these sites hide their identity using Tor. The rise of cryptocurrency has lead to the growth of the dark web by allowing anonymized money exchange.

Purposes of Cyber Attacks

- **Reconnaissance Attack**: an attempt to gather sensitive information about network services and systems. Ex: packet sniffers, ping sweep, port scan, queries regarding internet information.
- **Denial of Service Attack**: a network attack designed to slow down or crash a system by flooding it with useless traffic. Ex: ping of death, teardrop attack.

- **Access Attacks**: attacks try to uncover exploits and vulnerabilities in FTP, web services, and network authentication in order to get access to a system's network.

Active attacks allow the attacker to block the communication channel between participants on a network or permit him to send data to all parties at once. **Passive attacks** are when an intruder with unauthorized access actively eavesdrops on a communication.

Attack Scope

Malicious large scale attacks are offensive attempts to create chaos and disrupt services. Non-malicious small-scale attacks are often unintentional attacks or accidental damage due to human operational error that may cause system crashes or data loss.

Any crime that encompasses a network or computer can be deemed as cyber crime. The practice of gathering secrets with the consent of the information holder is termed as cyber espionage. Terrorism in the cyberspace domain is classified under cyber terrorism.

Threats Against Assets

	Availability	Confidentiality	Integrity
Hardware	equipment is stolen or disabled		parts are replaced without authorization
Software	code or programs are removed	an unauthorized copy of software is made and could be executed	code is modified, causing it to fail during execution or cause unintended side effects
Data	files are deleted or hidden, denying access to users	an unauthorized read of data is performed	existing files are modified or replaced with new files
Communication channels	messages are destroyed or deleted or the communication channel is brought down	messages are copied or read without authorization	messages are modified, delayed, reordered, duplicated, or fabricated

Network Security Issues

Information must be protected when travelling across a network. Only authorized access should be allowed to a node. Nodes handle security appropriately within the node itself since firewalls don't provide complete protection.

Malicious Activities

- **Threat**: the potential for violation of security, which exists when there is a circumstancec, capability, action, or event that could breach security and cause harm.
- **Vulnerability**: a weakness in a product that could allow an attacker to compromise the confidentiality, integrity, or availability of the product.
- **Risk**: the product of the level of threat with the level of vulnerability, which establishes the likelihood and impact of a successful attack.
- **Attack**: an attempt to exploit a vulnerability to make a threat a reality.
- **Malicious code**: programs such as viruses, worms, or Trojans that are covertly inserted into programs for the purpose of destroying data, stealing sensitive information, or compromising the security and integrity of a computer's data.
- **Spam zombies**: remotely controlled compromised systems designed to send out high volumes of junk or unsolicited messages for the purpose of delivering malicious code or phishing attempts.
- **Bot-infected computers**: compromised computers that are remotely controlled by an attacker to launch coordinated attacks with.
- **Network attack origins**: measures the originating sources of attacks from the Internet.
- **Web-based attack origins**: measures attack sources delivered through the web or HTTP. Typically, legitimate websites are compromised and used to attack unsuspecting visitors.
- **Disclosure/Compromise**: unauthorized disclosure of information.
- **Deception**: acceptance of false data.

- **Disruption**: interruption or prevention of correct operation.
- **Usurpation**: unauthorized control of some part of the system.
- **Snooping**: passive unauthoried viewing with the threat of disclosure.
- **Sniffer**: computer software or hardware that can intercept and log traffic passing over a digital network or part of a network.
- **Modification/Alteration**: active unauthorized tweaking with threat of disruption or usurpation.
- **Masquerading/Spoofing**: passive or active impersonation with threat of deception and usurpation.
- **Social engineering**: the act of manipulating people into performing actions or divulging confidential information.
- **Brute force**: a cryptanalysis technique or other kind of attack method involving an exhaustive search procedure.
- **Repudiation of origin**: denial that a party sent or created something.
- **Denial of receipt**: denial that a party received a message.
- **Delay**: temporarily inhibit a service.
- **Denial of service**: long term inhibition of service.
- **Distributed denial of service**: a distributed attack involving multiple compromised systems attacking a target in a parallel way.

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech