CSCI-GA.3205 Applied Cryptography & Network Security

Department of Computer Science
New York University

PRESENTED BY DR. MAZDAK ZAMANI
mazdak.zamani@NYU.edu

Introduction to Security Threats
Malware & Social Engineering Attacks
Application & Networking- Based Attacks

08

NYU

CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition

Chapter 1

Introduction to Security

Challenges of Securing Information

- Securing information
  - No simple solution
  - Many different types of attacks
  - Defending against attacks is often difficult

Difficulties in Defending Against Attacks

- *Universally connected devices*
- *Increased speed of attacks*
- *Greater sophistication of attacks*
- *Availability and simplicity of attack tools*
- *Faster detection of vulnerabilities*

Difficulties in Defending Against Attacks

- *Delays in security updating*
- *Weak security update distribution*
- *Distributed attacks*
- *Introduction of BYOD*
- *User confusion*

Defining Information Security

- **Information security** - the tasks of securing information that is in a digital format:
  - Manipulated by a microprocessor
  - Stored on a storage device
  - Transmitted over a network
- Information security goal - to ensure that protective measures are properly implemented to ward off attacks and prevent the total collapse of the system when a successful attack occurs

Defining Information Security

- Three types of information protection: often called CIA
  - Confidentiality
    - Only approved individuals may access information
  - Integrity
    - Information is correct and unaltered
  - Availability
    - Information is accessible to authorized users

Defining Information Security

- Protections implemented to secure information
  - Authentication
    - Ensures the individual is who they claim to be
  - Authorization
    - Provides permission or approval to specific technology resources
  - Accounting
    - Provides tracking of events

Defining Information Security

- Information security is achieved through a process that is a combination of three entities:
  - Information and the hardware
  - Software
  - Communications
- These entities are protected in three layers:
  - Products
  - People
  - Policies and procedures

Defining Information Security

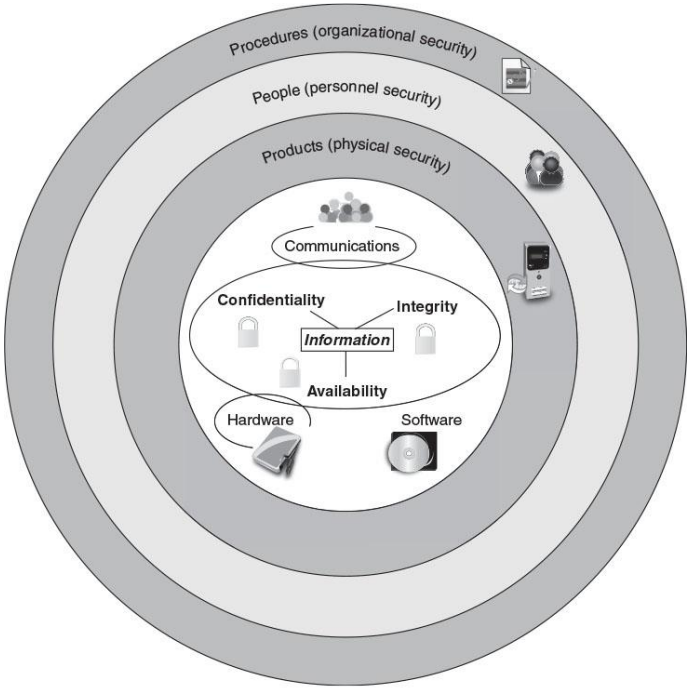

Figure 1-3 Information security layers

Information Security Terminology

- **Asset**
  - Item that has value
- **Threat**
  - Type of action that has the potential to cause harm
- **Threat agent**
  - A person or element with power to carry out a threat
- **Vulnerability**
  - Flaw or weakness that allows a threat agent to bypass security
- **Threat vector**
  - The means by which an attack can occur
- **Threat likelihood**
  - Likelihood that threat agent will exploit vulnerability
- **Risk**
  - A situation that involves exposure to some type of danger

Information Security Terminology

Options to deal with risk:

- **Risk avoidance** - involves identifying the risk but not engaging in the activity
- **Acceptance** - risk is acknowledged but no steps are taken to address it
- **Risk mitigation** - the attempt to address the risks by making risk less serious
- **Deterrence** - understanding the attacker and then informing him of the consequences of his actions
- **Transference** - transferring the risk to a third party

Understanding the Importance of Information Security

- Information security can be helpful in:
  - Preventing data theft
  - Thwarting identity theft
  - Avoiding the legal consequences of not securing information
  - Maintaining productivity
  - Foiling cyberterrorism

Preventing Data Theft

- Preventing data from being stolen is often the primary objective of an organization's information security
- Business data theft involves stealing proprietary business information
- Personal data theft involves stealing credit card numbers

Thwarting Identity Theft

- Identity theft
  - Stealing another person's personal information
    - Usually using it for financial gain
  - Example:
    - Steal person's SSN
    - Create new credit card account to charge purchases and leave them unpaid
    - File fraudulent tax returns

Foiling Cyberterrorism

- Cyberterrorism
  - Any premeditated, politically motivated attack against information, computer systems, computer programs, and data
- Designed to:
  - Cause panic
  - Provoke violence
  - Result in financial catastrophe
- May be directed at targets such as the banking industry, power plants, air traffic control centers, and water systems

Who Are the Attackers?

- *Hacker* - person who uses computer skills to attack computers
- *Black hat hackers*
  - Violate computer security for personal gain and the goal is to inflict malicious damage
- *White hat hackers*
  - Goal to expose security flaws, not to steal or corrupt data
- *Gray hat hackers*
  - Goal is to break into a system without owner's permission, but not for their own advantage

Who Are the Attackers?

- Categories of attackers
  - Cybercriminals
  - Script kiddies
  - Brokers
  - Insiders
  - Cyberterrorists
  - Hactivists
  - State-sponsored attackers

Steps of an Attack

- **Cyber Kill Chain** outlines the steps of an attack:
  - 1. *Reconnaissance* - probe for information about the system: type of hardware or software used
  - 2. *Weaponization* - attacker creates an exploit and packages it into a deliverable payload
  - 3. *Delivery* - weapon is transmitted to the target
  - 4. *Exploitation* - after weapon is delivered, the exploitation stage triggers the intruder's exploit
  - 5. *Installation* - the weapon is installed to either attack the computer or install a remote "backdoor"
  - 6. *Command and Control* - the comprised system connects back to the attacker so that the system can be remotely controlled by the attacker
  - 7. *Action on Objectives* - now the attackers can start to take actions to achieve their original objectives

Defenses Against Attacks

- Five fundamental security principles for defenses:
  - **Layering**: Making it unlikely that an attacker can break through all defense layers
  - **Limiting:** Only those who must use data should be granted access
  - **Diversity:** Layers must be different (diverse)
  - **Obscurity:** Not revealing details of type of computer, operating system version, etc.
  - **Simplicity:** A secure system should be simple from the inside but complex from the outside

CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition

Chapter 2
Malware and Social Engineering Attacks

Attacks Using Malware

- Malicious software (malware)
  - Enters a computer system without the owner's knowledge or consent
  - Uses a threat vector to deliver a malicious "payload" that performs a harmful function once it is invoked
- Malware is a general term that refers to a wide variety of damaging or annoying software

Attacks Using Malware

- Malware can be classified by the using the primary trait that the malware possesses:
  - *Circulation* - spreading rapidly to other systems in order to impact a large number of users
  - *Infection* - how it embeds itself into a system
  - *Concealment* - avoid detection by concealing its presence from scanners
  - *Payload capabilities* - what actions the malware performs

Circulation/Infection

- Three types of malware have the primary traits of circulation and/or infections:
  - Viruses
  - Worms
  - Trojans

Viruses

- Viruses perform two actions:
  - Unloads a payload to perform a malicious action
  - Reproduces itself by inserting its code into another file on the same computer
- Viruses cannot automatically spread to another computer
  - Relies on user action to spread
- Viruses are attached to files
- Viruses are spread by transferring infected files

Virus infection methods

- *Appender infection* - virus appends itself to end of a file (Easily detected by virus scanners
- *Swiss cheese infection* - viruses inject themselves into executable code
- *Split infection* - virus splits into several parts

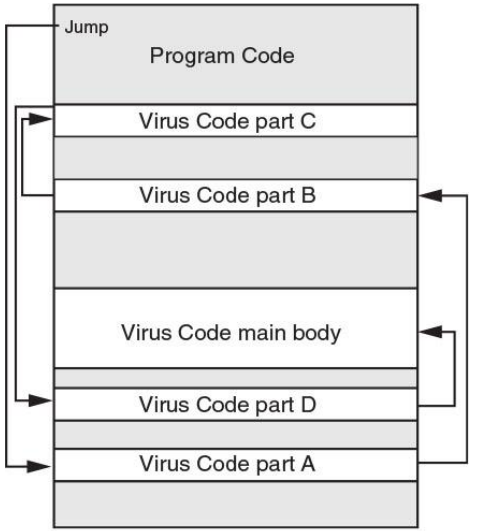

Figure 2-3 Split infection

Worms

- **Worm** - malicious program that uses a computer network to replicate
  - Sends copies of itself to other network devices
- Worms may:
  - Consume resources *or*
  - Leave behind a payload to harm infected systems
- Examples of worm actions
  - Deleting computer files
  - Allowing remote control of a computer by an attacker

Trojans

- **Trojan horse (Trojan)** - an executable program that does something other than advertised
  - Contain hidden code that launches an attack
  - Sometimes made to appear as data file
- Example
  - User downloads “free calendar program”
    - Program scans system for credit card numbers and passwords
    - Transmits information to attacker through network

Concealment

- **Rootkits** - software tools used by an attacker to hide actions or presence of other types of malicious software
  - Hide or remove traces of log-in records, log entries
- May alter or replace operating system files with modified versions that are specifically designed to ignore malicious activity
- Users can no longer trust their computer that contains a rootkit
  - The rootkit is in charge and hides what is occurring on the computer

Payload Capabilities

- The destructive power of malware can be found in its payload capabilities
- Primary payload capabilities are to:
  - Collect data
  - Delete data
  - Modify system security settings
  - Launch attacks

Collect Data

Different types of malware are designed to collect important data from the user's computer and make it available at the attacker:

- **Spyware** - software that gathers information without user consent
- **Keylogger** - captures and stores each keystroke that a user types on the computer's keyboard
- **Adware** - program that delivers advertising content in manner unexpected and unwanted by the user
- **Ransomware** - prevents a user's device from properly operating until a fee is paid

Delete Data

- The payload of other types of malware deletes data on the computer
- Logic bomb - computer code that lies dormant until it is triggered by a specific logical event
  - Difficult to detect before it is triggered
  - Often embedded in large computer programs that are not routinely scanned

Modify System Security

- Backdoor - gives access to a computer, program, or service that circumvents normal security to give program access
  - When installed on a computer, they allow the attacker to return at a later time and bypass security settings

Launch Attacks

- **Zombie** - an infected computer that is under the remote control of an attacker
  - Groups of zombie computers are gathered into a logical computer network called a **botnet** under the control of the attacker (**bot herder**)

Type of attack	Description
Spamming	Botnets are widely recognized as the primary source of spam email. A botnet consisting of thousands of zombies enables an attacker to send massive amounts of spam.
Spreading malware	Botnets can be used to spread malware and create new zombies and botnets. Zombies have the ability to download and execute a file sent by the attacker.
Manipulating online polls	Because each zombie has a unique Internet Protocol (IP) address, each "vote" by a zombie will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way.
Denying services	Botnets can flood a web server with thousands of requests and overwhelm it to the point that it cannot respond to legitimate requests.

Table 2-5 Uses of botnets

Social Engineering Attacks 1

- **Social engineering** - a means of gathering information for an attack by relying on the weaknesses of individuals
- Social engineering attacks can involve psychological approaches as well as physical procedures
- Psychological approaches goal: to persuade the victim to provide information or take action
- **Impersonation** - attacker pretends to be someone else: Help desk support technician

Social Engineering Attacks 2

- **Phishing** - sending an email claiming to be from legitimate source
  - Tries to trick user into giving private information
- **Spam** - unsolicited e-mail: Primary vehicles for distribution of malware
  - Cost spammers very little to send millions of spam messages
- **Hoaxes** - a false warning, usually claiming to come from the IT department

Social Engineering Attacks 3

- **Typo squatting** - redirecting a user to a fictitious website based on a misspelling of the URL (Also called **URL hijacking)**
  - Example: typing goggle.com instead of google.com
- **Dumpster diving**
  - Digging through trash to find information that can be useful in an attack
- **Tailgating**
  - Following behind an authorized individual through an access door
  - An employee could conspire with an unauthorized person to allow him to walk in with him (called piggybacking)
  - Watching an authorized user enter a security code on a keypad is known as **shoulder surfing**

CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition

Chapter 3
Application and Networking-Based Attacks

Application Attacks

- Attacks on the applications in a networked computer system can be directed toward the server, the client, or both

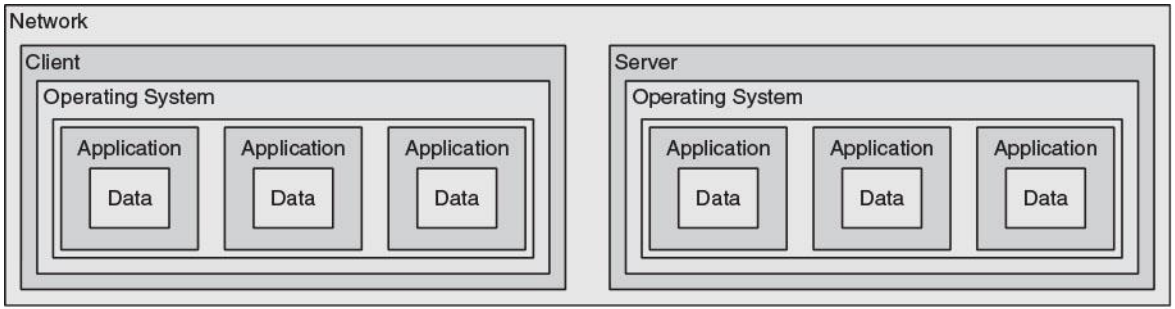

Figure 3-1 Conceptual networked computer system

Server-Side Web Application Attacks

- Securing server-side web applications of often considered more difficult than protecting other systems
- **Zero-day attack** - an attack that exploits previously unknown vulnerabilities, victims have not time to prepare for or defend against the attack
- Many server-side web application attacks target the input that the applications accept from users. Common web application attacks are:
  - Cross-site scripting
  - SQL injection
  - XML injection
  - Command injection/directory traversal

Cross-Site Scripting (XSS)

- Injecting scripts into a Web application server to direct attacks at unsuspecting clients
- When victim visits injected Web site:
  - Malicious instructions are sent to victim's browser
- Some XSS attacks are designed to steal information:
  - Retained by the browser when visiting specific sites
- An XSS attack requires a website meets two criteria:
  - Accepts user input without validating it
  - Uses input in a response

SQL Injection

- Targets SQL servers by injecting malicious commands into them
- SQL (Structured Query Language)
  - Used to manipulate data stored in relational database

```
SELECT fieldlist FROM table WHERE field = 'whatever' or 'a'='a'
```

  - Result: All user email addresses will be displayed

SQL injection statement	Result
whatever' AND email IS NULL; --	Determine the names of different fields in the database
whatever' AND 1=(SELECT COUNT(*) FROM tabname); --	Discover the name of the table
whatever' OR full_name LIKE '%Mia%'	Find specific users
whatever'; DROP TABLE members; --	Erase the database table
whatever'; UPDATE members SET email = 'attacker-email@evil.net' WHERE email = 'Mia@good.com';	Mail password to attacker's email account

Table 3-2 SQL injection statements

XML Injection

- HTML
  - Uses tags surrounded by brackets
  - Instructs browser to display text in specific format
- XML
  - Carries data instead of indicating how to display it
  - No predefined set of tags
- **XML injection** attack
  - Similar to SQL injection attack
  - Attacker discovers a Web site that does not filter user data
  - Injects XML tags and data into the database

Directory Traversal/ Command Injection

- Web server users are typically restricted to the root directory
- Users may be able to access subdirectories:
  - But not parallel or higher-level directories
- **Directory traversal** attack
  - Uses malformed input or takes advantage of software vulnerabilities
  - Attacker moves from root directory to restricted directories
- **Command injection** attack
  - Attacker enters commands to execute on a server

Client-Side Application Attacks

- Web application attacks are server-side attacks
- Client-side attacks target vulnerabilities in client applications that interact with a compromised server or process malicious data
- The client initiates connection with the server, which could result in an attack

Client-Side Attacks

- *Drive-by download*
  - Client computer is compromised simply by viewing a Web page
  - Attackers inject content into vulnerable Web server
- Header manipulation
  - **HTTP header** contains fields that characterize data being transmitted
  - Headers can originate from a Web browser. Browsers do not normally allow this but attacker's short program can allow modification
- Session Hijacking
  - Session token is a random string assigned to an interaction between user and web application
  - Attacker attempts to impersonate user by stealing or guessing session token

Client-Side Attacks

- Cookies
  - Cookies store user-specific information on user's local computer
  - Cookies may be stolen and used to impersonate the user
- Attachments
  - Files that are coupled with email messages
  - Malicious attachments are commonly used to spread viruses, Trojans, and other malware
- Malicious Add-ons
  - Plug-in - a third party library that attaches to a web browser and can be embedded inside a webpage
  - Add-ons or extensions - add functionality to the web browser
  - Attackers can create malicious add-ons to launch attacks against the user's computer

Impartial Overflow Attacks

"Impartial" means they can target either a server or a client

- Buffer overflow attacks
  - Occur when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer and extra data overflows into adjacent memory locations
  - An attacker can overflow the buffer with a new address pointing to the attacker's malware code
- Integer Overflow Attack
  - An *integer overflow* is the condition that occurs when the result of an arithmetic operation exceeds the maximum size of the integer type used to store it
  - An attacker changes the value of a variable to something outside the range that the programmer had intended by using an integer overflow

Networking-Based Attacks

- Attackers place a high priority on targeting networks
  - Exploiting a single vulnerability may expose hundreds or thousands of devices to an attacker
- Types of networking-based attacks:
  - Denial of service
  - Interception
  - Poisoning
  - Attacks on access rights

Denial of Service (DoS)

- Denial of service (DoS): A deliberate attempt to prevent authorized users from accessing a system by overwhelming it with requests
  - Most DoS attacks today are **distributed denial of service (DDoS):** Using hundreds or thousands of zombie computers in a botnet to flood a device with requests
- Ping flood attack: multiple computers rapidly send a large number of ICMP echo requests to a server. Server will drop legitimate connections and refuse new connections
- SYN flood attack: Attacker modifies the source address of each packet to computer addresses that do not exist or cannot be reached
- Smurf attack: An attacker broadcasts a ping request to all computers on the network but changes the address from which the request came from (called **spoofing)**

Interception

- Man-in-the-Middle attacks
  - In a passive attack, data is captured and recorded before sending it on to the original recipient
  - In an active attack contents of transmission are altered before they are sent to the recipient
- Replay attacks: Attacker captures network device's message to server and then later sends original, valid message to server: it establishes a trust relationship between attacker and server

Poisoning

- Poisoning
  - The act of introducing a substance that harms or destroys
- Two types of attacks inject “poison” into a normal network process to facilitate an attack:
  - ARP poisoning
  - DNS poisoning

Poisoning

- ARP Poisoning
  - Attacker modifies MAC address in ARP cache to point to different computer

Device	IP and MAC address	ARP cache before attack	ARP cache after attack
Attacker	192.146.118.200-AA-BB-CC-DD-02	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04
Victim 1	192.146.118.300-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-02
Victim 2	192.146.118.400-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-02

Table 3-4 ARP poisoning attack

Poisoning 1

- DNS poisoning
  - Domain Name System is the current basis for name resolution to IP address
  - DNS poisoning substitutes DNS addresses to redirect a computer to another device
- Two locations for DNS poisoning
  - Local host table
  - External DNS server

Poisoning 2

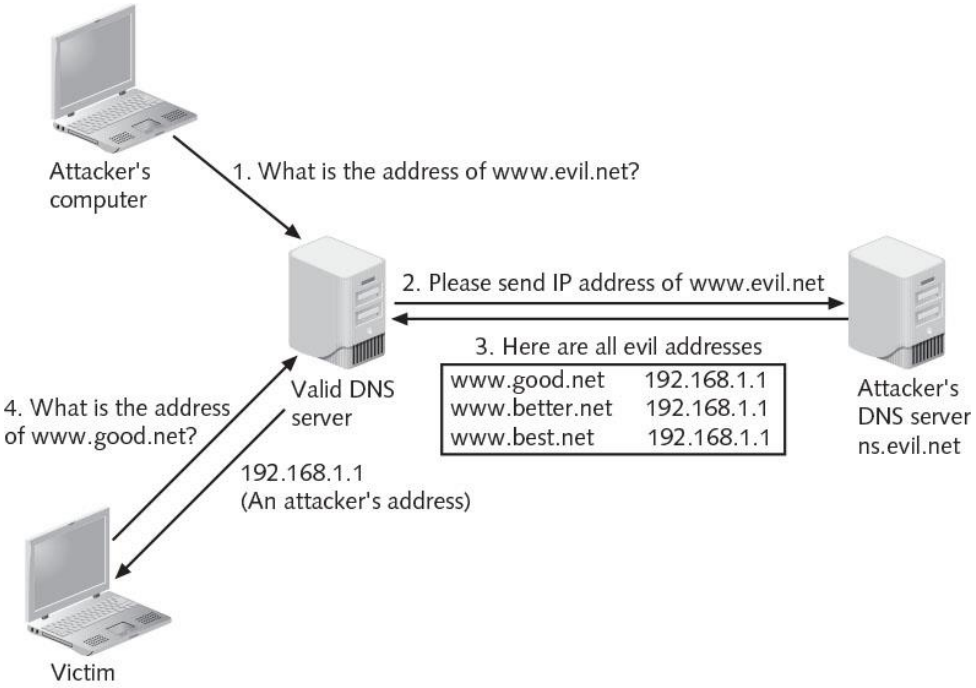

Figure 3-12 DNS poisoning

Attacks on Access Rights

- Privilege escalation
  - Exploiting a software vulnerability to gain access to resources that the user normally would be restricted from accessing
- Transitive access
  - Different users have different access rights, and an attack accesses a third party to gain access rights