Overview of Network Security Administration and Management

Common Network Security Problems

- Denial of service (DoS)
- Information leakage
- Regular file access
- misinformation
- Special file/database access
- Remote arbitrary code executing
- Elevation of privileges

Network security administration vs network security management

- Network security administration- involves configuring hardware, and running cables in a secure manner.
- Network security management- involves making decisions about the security of a network
- Network managers usually start off as network administrators and may still perform network administration duties, but their technical knowledge guides managerial decisions

Security principles

- There are many branches of security, if you consider the field of security as a hierarchy, you have security at the root and many branches leading outwards from that
- Example: national security, information security, and economic security may be considered subsets of the entire discipline of security
- In this course, we are considering **network security**, which is a subset of information security

Security principles

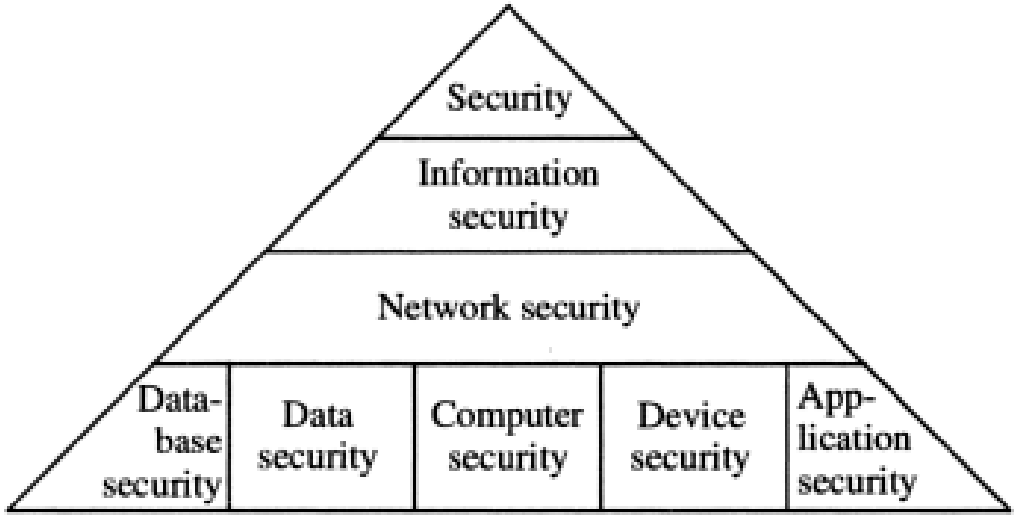


Figure 1.1 The hierarchy of security specializations.

- The field of security is concerned with protecting general assets
- Steps to protect person or property from harm
    - Harm may be intentional or nonintentional
- Sacrifices convenience for safety

Security principles (cont'd.)

Computer security

- Entails the methods used to ensure a system is secure
- Seldom in today's world are computers not connecter to other computers in networks.

Network security

- Network security is concerned with protecting data, hardware and software on a computer network
- Refers to the protection of multiple computers and other devices that are connected together

Security principles (cont'd.)

Information security

- Information security is concerned with protecting information and information resources, such as computer data, and voice communications
- Guarding digitally-formatted information:
  - That provides value to people and organizations

Components of a security infrastructure

4 components of a security infrastructure

The major components of a security infrastructure can be defined as belonging to one of four categories:

- Networks
- Platforms
- Physical
- Process

Network category

- Encompasses firewalls, routers, and switches, remote access devices (such as VPNs, and dialup modem banks) and network-based IDS that add some security features to the overall design
- These components are used to monitor, filter and/or restrict traffic as seen either by their network interfaces or as defined logic in software

Platform category

- Encompasses the server and client side software (such as underlying operating system and security applications controls)
- Devices that perform some electronic operation such as smart cards fit into this platform category
- Application-level access controls, such digital certificates, host-based IDS and analysis, virus detection and event accounting and analysis
- These security functions are used to protect the application that resides within these major infrastructure boundaries

Physical components category

- Include standard door keys and locks, key cards, identification badges, security cameras, motion sensors, cages, fences, guards and systems.
- Biometric components fit into this category as well and include hand geometry readers, facial readers, and retinal-scan cameras
- Network cabling and IPS systems fit into this category as well
- The primary goal of a physical security component is to keep unauthorized persons out and keep infrastructure components supplied with power and network connectivity

Process category

- Includes corporate security policy and procedural documents that governs the creation, used, storage and disposal of corporate data, as well as the systems and networks on which that data resides.
- The purpose of corporate security policy is to define the scope of protection for corporate assets and suggest or require a specific protection mechanism for those assets
- Corporate security procedures, a component of the corporate security policies document, are utilized to guide employee actions in particular circumstances

Goals of security infrastructure

- The primary goal of a security infrastructure design is the protection of corporate assets
- The controls applied in the protection of these assets should be inline with your corporate security goals as well as your corporate security policy documentation
- Each of the following protection goals should be approximately represented and weighted accordingly:
- Data confidentiality
- Data integrity
- Data availability

CIA Triad

- Confidentiality
  - Only approved individuals may access information
- Integrity
  - Information is correct and unaltered
- Availability
  - Information is accessible to authorized users

Securing information

- Protections implemented to secure information
  - Authentication
    - Individual is who they claim to be
  - Authorization
    - Grant ability to access information
  - Accounting
    - Provides tracking of events

Information security terminology

- Asset
  - Item of value
- Threat
  - Actions or events that have potential to cause harm
- Threat agent
  - Person or element with power to carry out a threat

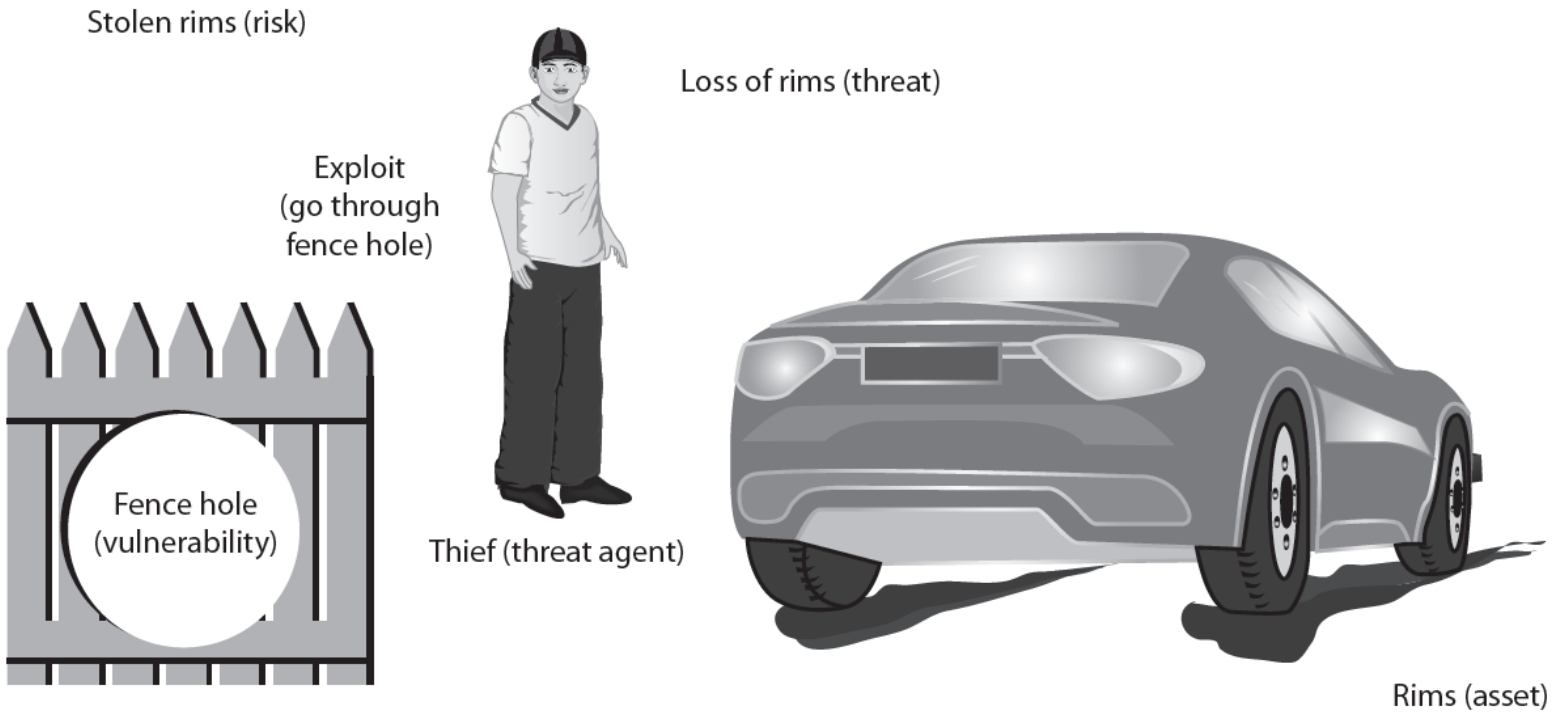
Information technology assets

Element name	Description	Example	Critical asset?
Information	Data that has been collected, classified, organized, and stored in various forms	Customer, personnel, production, sales, marketing, and finance databases	Yes: Extremely difficult to replace
Application software	Software that supports the business processes of the organization	Customized order transaction application, generic word processor	Yes: Unique and customized for the organization No: Generic off-the-shelf software
System software	Software that provides the foundation for application software	Operating system	No: Can be easily replaced
Physical items	Computer equipment, communications equipment, storage media, furniture, and fixtures	Servers, routers, DVDs, power supplies	No: Can be easily replaced
Services	Outsourced computing services	Voice and data communications	No: Can be easily replaced

Information Security Terminology (cont'd.)

- Vulnerability
  - Flaw or weakness
    - Threat agent can bypass security
- Risk
  - Likelihood that threat agent will exploit vulnerability
  - Cannot be eliminated entirely
    - Cost would be too high
    - Take too long to implement
  - Some degree of risk must be assumed

Information security components analogy



Information Security Terminology (cont'd.)

- Options to deal with risk
  - Accept
    - Realize there is a chance of loss
  - Diminish
    - Take precautions
    - Most information security risks should be diminished
  - Transfer risk to someone else
    - Example: purchasing insurance

Understanding the Importance of Information Security

- Preventing data theft
  - Security often associated with theft prevention
  - Business data theft
    - Proprietary information
  - Individual data theft
    - Credit card numbers

Understanding the Importance of Information Security (cont'd.)

- Thwarting identity theft
  - Using another's personal information in unauthorized manner
    - Usually for financial gain
  - Example:
    - Steal person's SSN
    - Create new credit card account
    - Charge purchases
    - Leave unpaid

Understanding the Importance of Information Security (cont'd.)

- Avoiding legal consequences
  - Laws protecting electronic data privacy
    - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - The Sarbanes-Oxley Act of 2002 (Sarbox)
    - The Gramm-Leach-Bliley Act (GLBA)
    - California's Database Security Breach Notification Act (2003)

Understanding the Importance of Information Security (cont'd.)

- Maintaining productivity
  - Post-attack clean up diverts resources
    - Time and money

Number of total employees	Average hourly salary	Number of employees to combat attack	Hours required to stop attack and clean up	Total lost salaries	Total lost hours of productivity
100	$25	1	48	$4,066	81
250	$25	3	72	$17,050	300
500	$30	5	80	$28,333	483
1,000	$30	10	96	$220,000	1,293

Table 1-6 Cost of attacks

Understanding the Importance of Information Security (cont'd.)

- Foiling cyberterrorism
  - Premeditated, politically motivated attacks
  - Target: information, computer systems, data
  - Designed to:
    - Cause panic
    - Provoke violence
    - Result in financial catastrophe

Understanding the Importance of Information Security (cont'd.)

- Potential cyberterrorism targets
  - Banking
  - Military
  - Energy (power plants)
  - Transportation (air traffic control centers)
  - Water systems

Who Are the Attackers?

- Categories of attackers
  - Hackers
  - Script kiddies
  - Spies
  - Insiders
  - Cybercriminals
  - Cyberterrorists

Hackers

- Hacker
  - Person who uses computer skills to attack computers
  - Term not common in security community
- White hat hackers
  - Goal to expose security flaws
  - Not to steal or corrupt data
- Black hat hackers
  - Goal is malicious and destructive

Script Kiddies

- Script kiddies
  - Goal: break into computers to create damage
  - Unskilled users
  - Download automated hacking software (scripts)
    - Use them to perform malicious acts
  - Attack software today has menu systems
    - Attacks are even easier for unskilled users
  - 40 percent of attacks performed by script kiddies

Spies

- Computer spy
  - Person hired to break into a computer:
    - To steal information
- Hired to attack a specific computer or system:
  - Containing sensitive information
- Goal: steal information without drawing attention to their actions
- Possess excellent computer skills:
  - To attack and cover their tracks

Insiders

- Employees, contractors, and business partners
- 48 percent of breaches attributed to insiders
- Examples of insider attacks
  - Health care worker publicized celebrities' health records
    - Disgruntled over upcoming job termination
  - Government employee planted malicious coding script
  - Stock trader concealed losses through fake transactions
  - U.S. Army private accessed sensitive documents

Cybercriminals

- Network of attackers, identity thieves, spammers, financial fraudsters
- Difference from ordinary attackers
  - More highly motivated
  - Willing to take more risk
  - Better funded
  - More tenacious
  - Goal: financial gain

Cybercriminals (cont'd.)

- Organized gangs of young attackers
  - Eastern European, Asian, and third-world regions

Characteristic	Explanation
Strong technical universities	Since the demise of the Soviet Union in the early 1990s, a number of large universities have stopped teaching communist ideology and turned to teaching technology
Low incomes	With the transition from communism to a free market system, individuals in several nations have suffered from the loss of an economy supported by the state, and incomes remain relatively low
Unstable legal systems	Many nations continue to struggle with making and enforcing new laws that combat computer crime
Tense political relations	Some new nations do not yet have strong ties to other foreign countries, and this sometimes complicates efforts to obtain cooperation with local law enforcement

Table 1-7 Characteristics of cybercriminals

Cybercriminals (cont'd.)

- Cybercrime
  - Targeted attacks against financial networks
  - Unauthorized access to information
  - Theft of personal information
- Financial cybercrime
  - Trafficking in stolen credit cards and financial information
  - Using spam to commit fraud

Cyberterrorists

- Cyberterrorists
  - Ideological motivation
    - Attacking because of their principles and beliefs
- Goals of a cyberattack:
  - Deface electronic information
    - Spread misinformation and propaganda
  - Deny service to legitimate computer users
  - Commit unauthorized intrusions
    - Results: critical infrastructure outages; corruption of vital data

Attacks and Defenses

- Wide variety of attacks
  - Same basic steps used in attack
- To protect computers against attacks:
  - Follow five fundamental security principles

Steps of an Attack

- Probe for information
  - Such as type of hardware or software used
- Penetrate any defenses
  - Launch the attack
- Modify security settings
  - Allows attacker to reenter compromised system easily
- Circulate to other systems
  - Same tools directed toward other systems
- Paralyze networks and devices

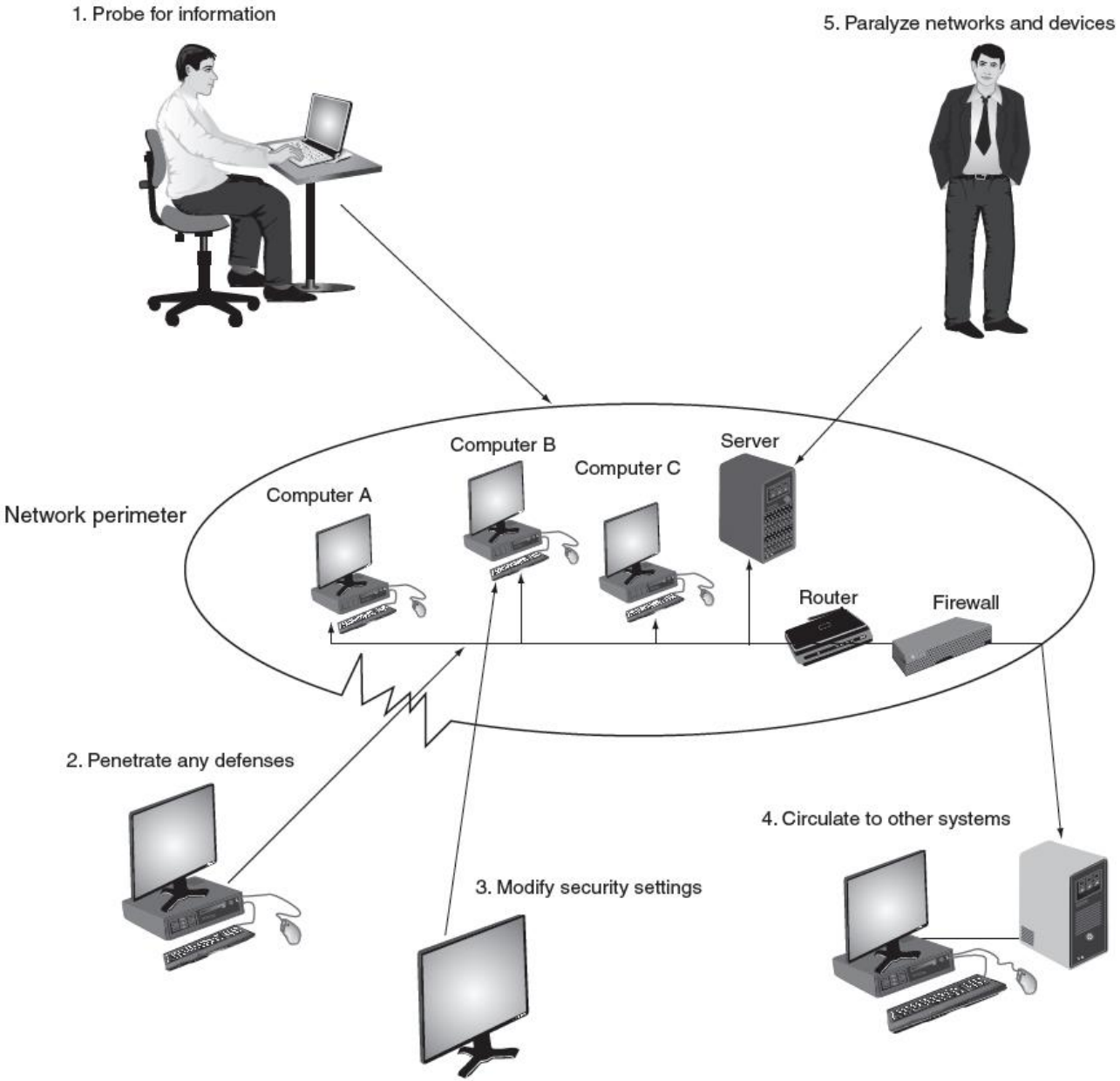


Figure 1-6
Steps of an attack

Defenses Against Attacks

- Fundamental security principles for defenses
  - Layering
  - Limiting
  - Diversity
  - Obscurity
  - Simplicity

Layering

- Information security must be created in layers
  - Single defense mechanism may be easy to circumvent
  - Unlikely that attacker can break through all defense layers
- Layered security approach
  - Can be useful in resisting a variety of attacks
  - Provides the most comprehensive protection

Limiting

- Limiting access to information:
  - Reduces the threat against it
- Only those who must use data granted access
  - Amount of access limited to what that person needs to know
- Methods of limiting access
  - Technology
    - File permissions
  - Procedural
    - Prohibiting document removal from premises

Diversity

- Closely related to layering
  - Layers must be different (diverse)
- If attackers penetrate one layer:
  - Same techniques unsuccessful in breaking through other layers
- Breaching one security layer does not compromise the whole system
- Example of diversity
  - Using security products from different manufacturers

Obscurity

- Obscuring inside details to outsiders
- Example: not revealing details
  - Type of computer
  - Operating system version
  - Brand of software used
- Difficult for attacker to devise attack if system details are unknown

Simplicity

- Nature of information security is complex
- Complex security systems
  - Difficult to understand and troubleshoot
  - Often compromised for ease of use by trusted users
- Secure system should be simple:
  - For insiders to understand and use
- Simple from the inside
  - Complex from the outside

Summary

- Information security attacks growing exponentially in recent years
- Several reasons for difficulty defending against today's attacks
- Information security protects information's integrity, confidentiality, and availability:
  - On devices that store, manipulate, and transmit information
  - Using products, people, and procedures

Summary (cont'd.)

- Goals of information security
  - Prevent data theft
  - Thwart identity theft
  - Avoid legal consequences of not securing information
  - Maintain productivity
  - Foil cyberterrorism
- Different types of people with different motivations conduct computer attacks
- An attack has five general steps