

Security Overview

(1) Risks and Defending Measures

- ❖ Risks
 - Computer is controlling many important systems.
 - Medical information system, ATM, business servers, banking systems.
 - Air traffic controller
 - Why are there risks?
 - Adversaries
 - They are intelligent and dedicated
 - There are many of them
 - Their identity is mostly unknown
 - Their motivation evolves from “for fun” to “for profit”: e.g. Zombie networks.
 - Computer systems need interaction
 - You can't build a castle around it
 - Even if you can, the castle might not be built correctly and securely
 - Networked computers can be accessed remotely
 - How did people deal with risks when protecting their cities
 - Building walls, putting soldiers at the entrances
 - What can go wrong?
 - Remember the Trojan War story: *Trojan horse*.
 - The soldiers are corrupted: *Social engineering*.
 - The soldiers are incompetent: *Vulnerabilities*
 - The walls are not strong enough: *Vulnerabilities*
 - There are holes on the wall: *Vulnerabilities*
 - Enemies can dig a tunnel underneath the wall: *Vulnerabilities*
 - Some resident opened another gate (or tunnel) for convenience reasons: *Backdoors*
 - ◆ Some employee installs a wireless access point or a dial-in modem within his company's protected network: *Backdoors*.
 - Vulnerabilities: the most common attack is to exploit known operating system vulnerabilities.
 - The Morris Worm example: exploited known vulnerabilities in *fingerd* and *sendmail*.
- ❖ Defending Methods (Three lines of defense)
 - Prevention
 - Prevent it: make it impossible
 - Deter it: make it harder
 - Deflect it: make other targets more attractive, e.g. honeypot.
 - Detection
 - monitoring
 - intrusion detection

- Recovery
 - recover the data
 - identify the damage
 - find the culprit: forensics
 - The focus of this course: prevention and detection
 - ❖ How does prevention work?
 - Policies (IST courses)
 - Encryption (only basics are covered in this course)
 - Not just the encryption. Examples include digital cash, time-stamping, secure multiparty computation, e-voting, e-bidding, etc.
 - Applied Cryptography covers these.
 - Control (the key component of this course)
 - hardware control
 - software control
 - Examples: make sure that only those with security clearance can read this file.
 - ❖ How could prevention not work correctly? After putting all the controls and protections, are we safe?
 - People make mistakes
 - When they design, implement, configure those controls and protections: *vulnerabilities*
 - When they use computers: *infect virus, install trap door, etc.*
 - Malicious hackers are intelligent and motivated
 - They find all means to bypass, defeat, and fool systems and users
 - There is an army race between good guys and bad guys.
 - Like chess game, except that bad guys often get the last move.
 - Fail to anticipate attacks
 - ❖ How to achieve a better protection and prevention?
 - Good principles:
 - Principle of least privilege,
 - Writing good codes,
 - Security testing,
 - Integrate security from the beginning rather than treat it as an add-on feature,
 - Understand the risk in your environment,
 - Anticipate future attacks and think like an attacker.
 - Good security hygiene: don't install untrusted executable files; don't open word files from untrusted senders; don't use root account if not necessary; understand the security consequence of your actions; etc.
-

(2) The meaning of security

- ❖ When we talk about " security", we mean that we are addressing three very important aspects of any computer-related system
 - Confidentiality

- Integrity
- Availability
- ❖ For different applications, the interpretation of CIA is different.
- ❖ Confidentiality: access (reading, viewing, printing, knowing, etc.)
 - Contents : encryption (cryptography)
 - Existence of data: steganography
 - e.g. stock investigation, prisoner, spy, watermarking
 - Resource hiding: operating system information and configuration
 - Fingerprinting
 - Identity: (anonymity)
- ❖ Integrity: modification (includes writing, changing, changing status, deleting, and creating).
 - Data integrity
 - Program integrity
 - System integrity
 - Identity integrity (non-repudiation)
 - Origin (location) integrity (network traceback)
- ❖ Availability.
 - denial of service
- ❖ Example: *what category do they belong to?*
 - TCP SYN flooding
 - Sniffing
 - Faked identity
 - ATM machine
 - Saving passwords in a plaintext file

(2) Network Security: An Overview

- ❖ Network security issues: networks have security problems for the following reasons:
 - Sharing: more users have the potential to access network systems than single computers. Access controls for single systems may be inadequate in networks.
 - Complexity of system: when a system is complicated, it is difficult to make sure that the design and implementation are correct.
 - Unknown perimeter: the expandability of a network also implies uncertainty about the network boundary. One host may be a node on two different networks, so that resources on one network are accessible to the users of the other network as well.
 - Many points of attack: a simple computing system is a self-contained unit. Access controls on one machine preserve the secrecy of data on that processor. However, when a file is stored in a network host remote from the user, the file may pass through many hosts to get to the user. Although the administrator of one host may enforce rigorous security policies, that administrator has no control

over other hosts in the networks. The user has to depend on the access control mechanisms of all of these systems.

- Anonymity: an attacker can mount an attack from thousands of miles away and thus never have to touch the system. The attack can be passed through many other hosts, in an effort to disguise from where the attack originated.
- Unknown path: there may be many paths from one host to another. Network users seldom have control over the routing of their messages.
- Vulnerabilities of network protocols:

❖ Security threat analysis

Figure 9-12 from Pfleeger's Book

- Read communications from A to B: confidentiality
- Modify communications from A to B: integrity
- Forge communications allegedly from A to B: integrity
- Inhibit communications from A to B: availability
- Prevent B from receiving packets: availability
- Read/Modify/Destroy data at C or D: Malicious users can impersonate A (who is authorized to access data at C or D).
- ❖ How are all of these threats accomplished?
 - Wiretapping
 - Impersonation
 - Message confidentiality violations
 - Message integrity violations
 - Hacking
 - Code integrity violations
 - Denial of service
- ❖ Vulnerabilities in TCP/IP
 - ARP protocols and ARP cache poisoning
 - IP protocols, fragmentation, IP spoofing.
 - ICMP protocols and risks.
 - UDP protocols and risks.
 - TCP protocols, TCP session hijacking, SYN flooding attack, and TCP DoS attacks.
 - DNS protocols and risks.
 - Buffer overflow vulnerabilities.
- ❖ Network security controls and mechanisms
 - Hiding: usually does not work

- Hiding operating system types: OS fingerprinting
 - Hiding ports: port scanning
 - Hiding encryption algorithms: the security of an encryption algorithm should depend on the secrecy of the key, rather than the algorithm.
- Encryption: keep in mind that there are certain things in network packets that cannot be encrypted. For example, IP addresses. Moreover, if users on the other end are malicious, encryption offers no help.
- Encryption algorithms, IPSec.
- Access control:
- Port protection: dial-in ports are big risks; unnecessary ports (e.g., telnet, ftp) are also risk and should be closed.
 - Network traffic: firewalls.
- Authentication in distributed systems
- Password authentication, Kerberos.
- Data integrity:
- Digital signature, checksum.
- Firewall
- Its goal is to block undesirable traffic
 - Firewalls are not complete solutions. Many things cannot be achieved by firewalls. There are ways to bypassing firewalls.
- Intrusion detection system (IDS)
- Detecting intrusion.
 - There are ways to bypassing IDS
 - An ideal IDS still does not exist.
- Network forensics: e.g., IP traceback. How to find the intruders?