The Need for Security

Chapter 2

Information security's primary mission is to ensure that systems and their contents remain the same!

“Organizations must understand the environment in which information systems operate so their information security programs can address actual and potential problems.”

Business Needs First

- Information Security Important Functions
  - Protect the organization's ability to function
  - Enable the safe operation of applications
  - Protect the data
  - Safeguard technology assets

Information security has more to do with management than with technology

?

Threats Basics

- To protect organization’s information
  1. Know the information to be protected and the systems that store, transport and process
  2. Know the threats you face
- Computer Security Institute(CSI)
  - 2009 - 64% of organizations responding malware infections
    - 14% system penetration by outsider
    - Loss = $234K per respondent
    - Downward trend
    - Security is improving
    - Companies declining outsourcing security
      - Climb 59% to 71%
      - i.e. It is staying in house

“Computer systems are not vulnerable to attack. We are vulnerable to attack through our computer systems.”

Robert Seacord

Threats to Information Security

Categories of Threat	Examples
Compromises to intellectual property	Piracy, copyright infringement
Software attacks	Viruses, worms, macros, DoS
Deviations in quality of service	ISP, power, WAN service issues from service providers
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning
Acts of human error or failure	Accidents, employee mistakes

Threats to Information Security

Categories of Threat	Examples
Information extortion	Blackmail or information disclosure
Deliberate acts of theft	Illegal confiscation of equipment or information
Missing, inadequate, or incomplete	Loss of access to information systems due to disk drive failure, without proper backup and recovery plan
Missing, inadequate, or incomplete controls	Network compromised because no firewall security controls
Sabotage or vandalism	Destruction of systems or information

Threats to Information Security

Categories of Threat	Examples
Theft	Illegal confiscation of equipment or information
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Intellectual Property

"the ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person's intellectual property may or may not involve royalty payments or permission, but should always include proper credit."

Inquirer

Software Piracy in Asia Exposed

Intellectual Property

- Includes
    - Trade secrets
    - Copyrights
    - Trademarks
    - Patents
- Breaches constitute a threat
- 2 watch dog agencies
    - Software and Information Industry Association
    - Business Software Alliance
- Most common breach
    - Software piracy
    - 1/3 of all software in use is pirated

Deliberate Software Attacks

- Malicious code
- Malicious software
- Malware
- First business hacked out of existence
  - Denial-of-service attack
  - Cloudnine
    - British Internet service provider

Virus

- Segments of code
- Attaches itself to existing program
- Takes control of program access
- Replication

Worms

- Malicious program
- Replicates constantly
- Doesn’t require another program
- Can be initiated with or without the user download

Other Malware

- Trojan Horse
  - Hide their true nature
  - Reveal the designed behavior only when activated
- Back door or trap door
  - Allows access to system at will with special privileges
- Polymorphism
  - Changes it apparent shape over time
  - Makes it undetectable by techniques that look for preconfigured signatures
- Hoaxes

Espionage or Trespass

- Intelligence Gathering
  - Legal – competitive intelligence
  - Illegal – industrial espionage
  - Thin line
  - One technique – shoulder surfing
- Trespass
  - Protect with
    - Authentication
    - Authorization

Hackers

- 2 levels
  - Experts
    - Develop software scripts
    - Develop program exploits
  - Novice
    - Script kiddie
      - Use previously written software
    - Packet monkeys
      - Use automated exploits

System Rule Breakers

- Crackers
  - Individuals who crack or remove software protection designed to prevent unauthorized duplication
- Phreakers
  - Use public networks to make free phone calls

Forces of Nature

- Pose some of most dangerous threats
- Unexpected and occur with little or no warning

- Fire
- Tornado
- Tsunami
- Electrostatic discharge
- Dust contamination

- Flood
- Earthquake
- Lightning
- Landslide
- Mudslide
- Hurricane/typhoon

Acts of Human Error or Failure

- Acts performed *without* intent or malicious purpose by and authorized user
- Greatest threat to org info security
  - Organization's own employees
  - Closest to the data
  - Mistakes
    - Revelation of classified data
    - Entry of erroneous data
    - Accidental deletion or modification of data
    - Storage of data in unprotected areas
    - Failure to protect information

Acts of Human Error or Failure

- Prevention
  - Training
  - Ongoing awareness activities
  - Controls
    - Require user to type a critical command twice
    - Verification of commands

Deliberate Acts

- Information Extortion
  - Attacker or trusted insider steals information
  - Demands compensation
  - Agree not to disclose information

Missing, Inadequate or Incomplete Controls

- Security safeguards and information asset protection controls are
  - Missing
  - Misconfigured
  - Antiquated
  - Poorly designed or managed
- Make org more likely to suffer loss

Sabotage or Vandalism

- Deliberate sabotage of a computer system or business
- Acts to destroy an asset
- Damage to an image of an organization
- Hackterist or cyber activist
  - Interfere with or disrupt systems
  - Protest the operations, policies, or actions
- Cyber terrorism
- Theft

Theft

- Illegal taking of another’s property
  - Physical
  - Electronic
  - Intellectual
  - Constant
- Problem – crime not always readily apparent

Technical Hardware Failures or Errors

- Best known
  - Intel Pentium II chip
  - First ever chip recall
  - Loss of over $475 million
- Technology obsolescence
  - Can lead to unreliable and   untrustworthy systems

Technical Software Failures or Errors

- Large quantities of code written, published, and sold with bugs
- Bugs undetected and unresolved
- Combinations of software can cause issues
- Weekly patches

Technology Obsolescence

- Outdated hardware or software
- Reliability problems
- Management problem
  - Should have plan in place
- Non-support of legacy systems
- Can be costly to resolve

Attacks

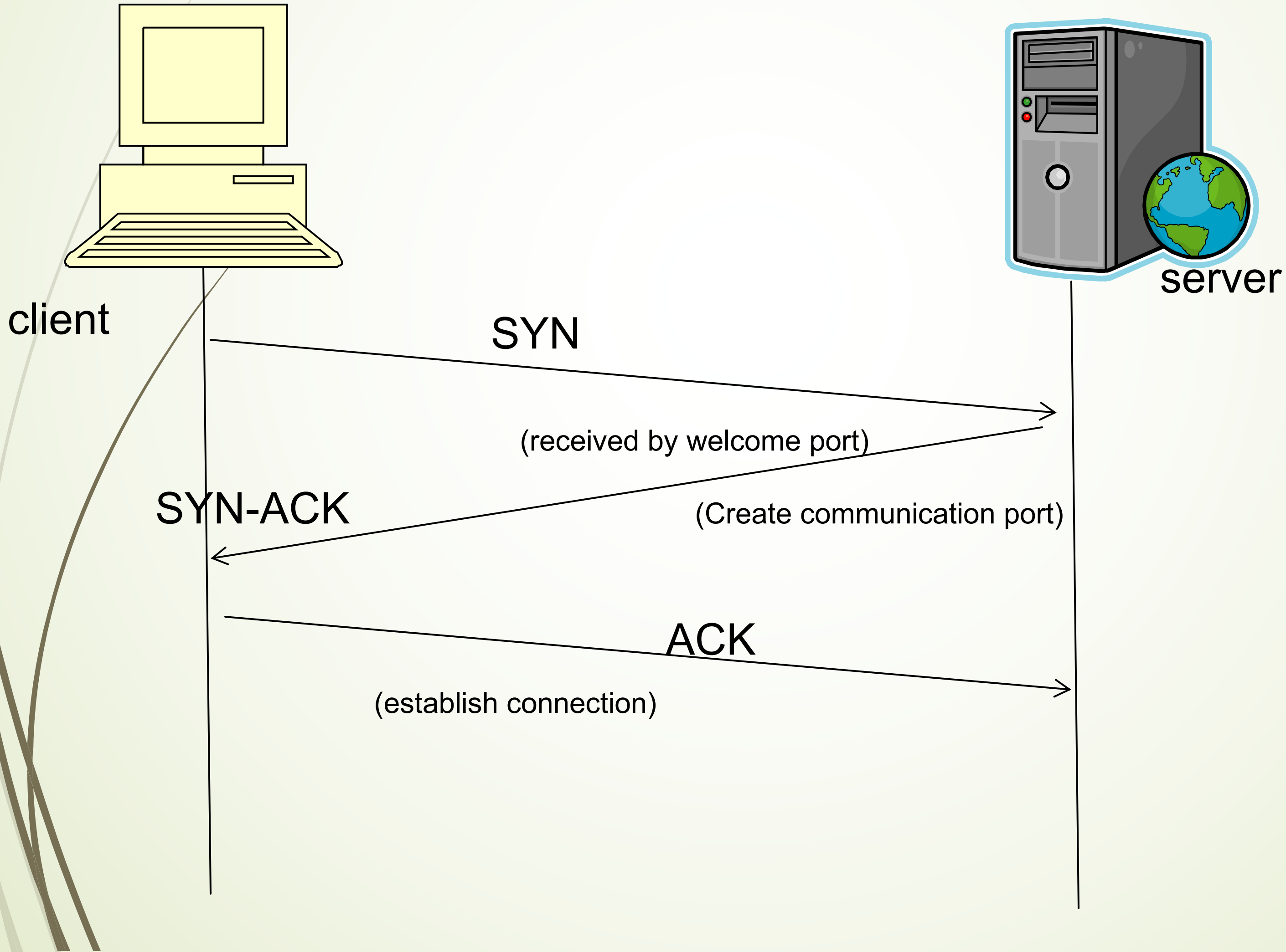
Vector	Description
IP scan and attack	Infected system scans IP addresses and targets vulnerabilities
Web browsing	Infects web content files infectious
Virus	Infect other machines
Unprotected shares	Infects any device that is unprotected
Mass mail	e-mailing to all addresses in an address book
Simple Network Management Protocol (SNMP)	Use common password employed in early versions of the protocol the attacking program can gain control of device

Methods of Attack

- Password Crack
- Brute force
- Dictionary

- The design of the network infrastructure and communication protocols are a major contributor

Initial Communication Three-Way Handshake



Problem

- Half-open socket problem
- Server trusts the client that originates the handshake
- Leaves its port door open
- As long as half-open port remains open, an intruder can enter

Methods of Attack

- Social Engineering
- IP-Spoofing
  - IP address of the source element of the data packets are altered and replaced with bogus addresses
- SYN spoofing
  - The server is overwhelmed by spoofed packets
- Scanning
  - Way of determining which ports are open and can be used

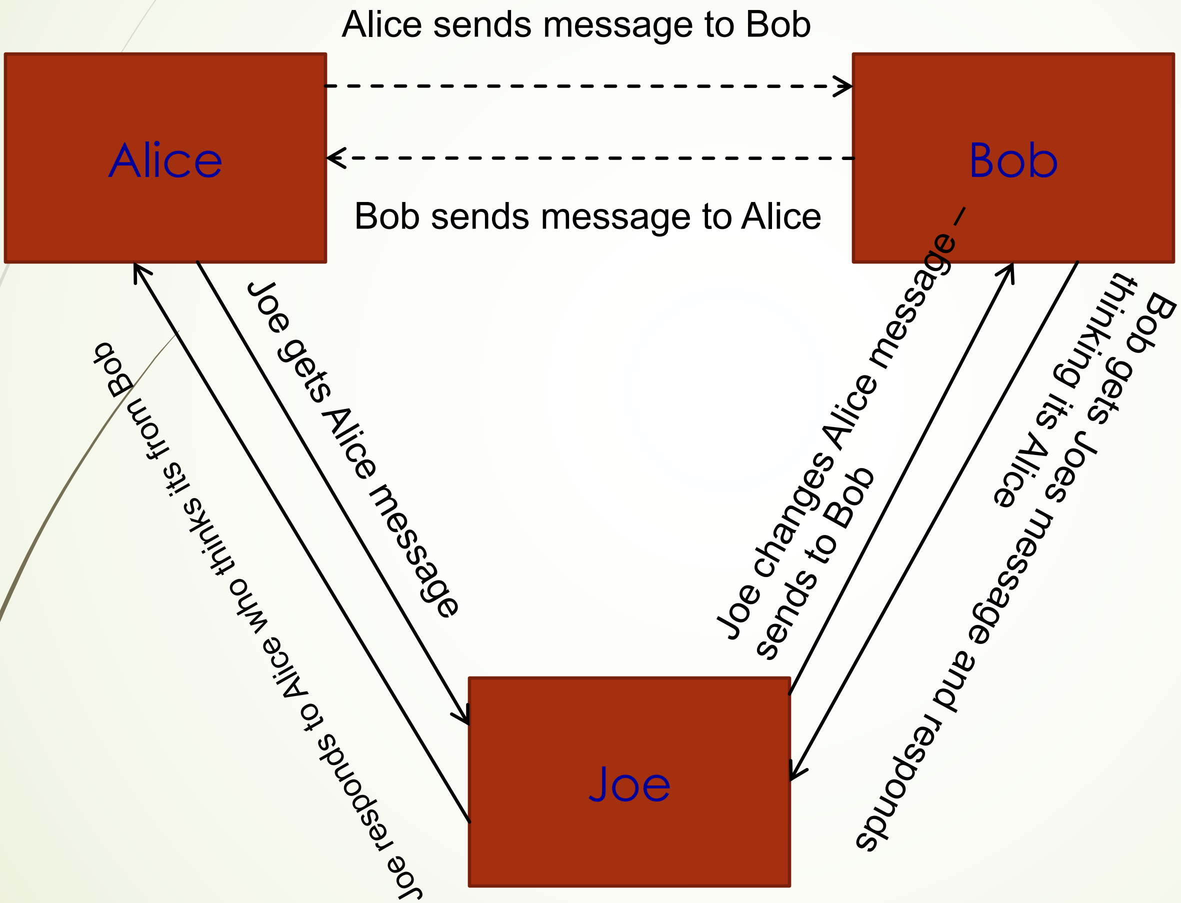
Methods of Attack

- Denial of service
    - Smurf send large amount of spoofed ping packets
    - Overwhelms the system
    - Can stop response
- Spam
- Mail bombing
- Sniffing
    - Monitors data traveling over a network
    - legitimated and non legitimate purposes
    - Packet sniffing

Methods of Attack

- Man-in-the-Middle
  - Monitors or sniffs packets from network
  - Modifies the packets
  - Inserts them back into the network
  - Allows attacker to eavesdrop, change, delete, reroute, add, or divert data.
  - Variant
    - Spoofing involves the interception of an encryption key exchange

Man-in -Middle



Alice

Bob

Joe

Alice sends message to Bob

Bob sends message to Alice

Joe gets Alice message

Joe changes Alice message – sends to Bob

Bob gets Joes message and responds thinking its Alice

Joe responds to Alice who thinks its from Bob

Programming Errors

- Amit Yoran, former director of The Department of Homeland Security's National Cyber Security Division

" *only by improving the quality of our software and reducing the number of flaws can we hope to be successful in our security efforts*"

Programming Errors

- 95 percent of software security bugs come from 19 ‘common, well-understood’ programming mistakes
- Software can be correct without being secure.
- There is an imbalance between our abilities as developers and the abilities and resources of the attacker.

Programming Errors

- January to August, 2003, CERT Coordination Center published 22 security advisories and 9 of them were directly related to buffer overflow.
- The root of the problem
  - Application writes beyond array bounds
  - Stack is corrupted
  - Attacker gets to specify control information.

Other Buffer Overflow Problem

- Mismatch in process rates between 2 entities involved in communication
- Application error
  - More data is sent to a buffer than it can handle
  - Attacker can then make the target system execute instruction
  - Some programming language more vulnerable than others
    - C++ especially vulnerable
    - Java less so
    - Ways of handling

Timing Attack

- Explores the contents of a web browser’s cache
- Allows a Web designer to create a malicious form of cookie that is stored on the client’s system
- Cookie allow designer to collect information on how to access password protected sites