第21章 网络安全

南京大学计算机系　　黄皓教授

2007年12月4日 星期二

References

- Charles P. Pfleeger, Shari Lawrence Pfleeger. Security in Computing. Pearson Education Asia Limited and China Machine Press， 2004.

  (李毅超等译。信息安全原理与应用。电子工业出版社，2004年7月第1版。)

Threats in Networks

(1) What Makes a Network Vulnerable

(2) Who Attacks Networks

(3) Threat Precursors

(4) Threats in Transit

(5) Impersonation

(6) Spoofing

(7) Message Confidentiality Threats

(8) Message Integrity Threats

What Makes a Network Vulnerable

- **Anonymity**
  - An attacker can mount an attack from thousands of miles away and never come into direct contact with the system，its administrators，or users.
  - The potential attacker is thus safe behind an electronic shield.
  - Disguise the attack’s origin.
- **Many points of attack**
  - One host’s administrator may enforce rigorous security policies，but that administrator has no control over other hosts in the network.
  - An attack can come from any host to any host，so that a large network offers many points of vulnerability.

What Makes a Network Vulnerable

- **Sharing**
  - □ Access controls for single systems may be jnadequate in networks.
- **Complexity of system**
  - □ A network operating/control system is likely to be more complex than an operating system for a single computing system.
  - □ The attacker can use the greater computing power to advantage by causing the victim’s computer to perform part of the attack’s computation.
  - □ Most users do not know what their computers are really doing at any moment.

What Makes a Network Vulnerable

- **Unknown perimeter**
  - A network’s expandability also implies uncertainty about the network boundary.
  - Resources on one network are accessible to the users of the other network as well.
- **Unknown path**
  - A user on host A wants to send a message to a user on host B. That message might be routed through hosts C or D before arriving at host B. Host C may provide acceptable security, but not D.
  - Network users seldom have control over the routing of their messages.

Who Attacks Networks

- **Challenge**
  - Why do people do dangerous or daunting things，like climb mountains or swim across the English Channel or engage in extreme sports? Because of the challenge.
  - The single most significant motivation for a network attacker is the intellectual challenge：
    - He or she is intrigued with knowing the answers to Can I defeat this network?
    - What would happen if I tried this approach or that technique?
    - Robert Morris attacked supposedly as an experiment to see if he could exploit a particular vulnerability.
    - Other attackers，such as the Cult of the Dead Cow, seek to demonstrate weaknesses in security defenses so that others will pay attention to strengthening security.
    - Still other unknown individuals working persistently just to see how far they can go in performing unwelcome activities.

Who Attacks Networks

- **Fame**
  - Some attackers seek recognition for their activities.
  - That is，part of the challenge is doing the deed，all other part is taking credit for it.
  - They may not be able to brag too openly，but they enjoy the personal thrill of seeing their attacks written up in the news media.

Who Attacks Networks

- **Money and Espionage**
  - As in other settings．financial reward motivates attackers，too.
  - Industrial espionage is illegal, but it occurs, in part because gain. Its existence and consequences can be embarrassing for the target companies.
  - Thus, many incidents go unreported, and there are few reliable statistics on how much industrial espionage and “dirty tricks” go on.
  - In addition，38 percent to 53 percent reported they were attacked by a U.S. competitor and 23 percent to 31 percent by a foreign corporation.
  - Not all security attacks come from individual hackers.

Who Attacks Networks

- **Ideology**
  - □ Hactivism: use hacking techniques against a target’s network with the intent of disrupting normal operations but not causing serious damage.
  - □ Cyberterrorism: politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage.

Threat Precursors

- **Port Scan**
  - □ An easy way to gather network information is to use a port scan，a program that，for a particular IP address，reports which ports respond to messages and which of several known vulnerabilities seem to be present．
  - □ which standard ports or services are running and responding on the target system.
  - □ what operating system is installed on the target system，
  - □ what applications and versions of applications are present．
  - □ This information is readily available for the asking from a networked system；it can be obtained quietly，anonymously，without identification or authentication，drawing little or no attention to the scan．

Threat Precursors

- **Social Engineering**
  - □ “Hello．this is John Davis from IT support．We need to test some connections on the internal network． Could you please run the command ipconfig /all on your workstation and read to me the addresses it displays?”
- **Reconnaissance**
  - □ One commonly used reconnaissance technique is called “**dumpster diving**”
  - □ Reconnaissance may also involve eavesdropping.
  - □ Collecting background information yields a big payoff.

Threat Precursors

- **Operating System and Application Fingerprinting**
  - □ Each vendor’s code is implemented independently. So there may be minor variations in interpretation and behavior. The variations do not make the software noncompliant with the standard，but they are different enough to make each version distinctive.
  - □ For example. each version may have different sequence numbers，TCP flags，and new options. For example:

Server: Netscape-Commerce/1.12

Your browser sent a non-HTTP compliant message.

Microsoft ESMTP MAIL Service, Version：5.0, 2195.3779

Threat Precursors

- Bulletin Boards and Chats
- Availability of Documentation

To Catch a Thief

- U.S. FBI launched a program in 1999 to identify and arrest malicious hackers．
- Swallow chose an online identity and began visiting hackers：web sites and chat rooms.
- To be accepted into the club, Swallow had to demonstrate that he personally had hacker skills.
- With permission，he conducted more than a dozen defacements of government web sites to establish his reputation．
- During the eighteen-month sting operations，Swallow and his team gathered critical evidence on several people.
- Proving the adage that “on the Internet．nobody knows you’re a dog”, Swallow，in his 40s，was able to befriend attackers in their teens．

Threats in Transit：
Eavesdropping and Wiretapping

- Cable
  - By a process called inductance(自感应) an intruder can tap a wire and read radiated signals without making physical contact with the cable.
- Microwave
  - A microwave signal is usually not shielded or isolated to prevent interception．Microwave is，therefore，a very insecure medium.
- Wireless

Impersonation

- Authentication Foiled by Guessing
- Authentication Thwarted by Eavesdropping or Wiretapping
- Authentication Foiled by Avoidance
- Nonexistent Authentication
- Well known Authentication

Spoofing

- Masquerade
- Session Hijacking
- Man-in-the-Middle Attack

Message Confidentiality Threats

- Misdelivery
- Exposure
- Traffic Flow Analysis

Message Integrity Threats

- Falsification of Messages
  - replace a message entirely，including the date，time，and sender/receiver identification
  - Reuse (replay) an old message
  - combine pieces of different messages into one
  - change the apparent source of a message
  - redirect a message
  - destroy or delete a message

Other threats

- Buffer Overflows
- Application Code Errors
- Denial of Service
- Connection Flooding
- Traffic redirection
- DNS Attack
- Distributed Denial of Service
- Cookies
- Scripts
- Active Code

Network Vulnerabilities

- Precursors to attack
  - Port scan
  - Social engineering
  - Reconnaissance
  - OS and application fingerprinting
- Authentication failures
  - Impersonation
  - Guessing
  - Eavesdropping
  - Spoofing
  - Session hijacking
  - Man-in-the-middie attack
- Programming flaws
  - Buffer over flow
  - Addressing errors
  - Server-side include
  - Cookie
  - Malicious active code：JavaSeript，ActiveX
  - Malicious code：virus，worm，Trojan horse
  - Malicious typed code

Network Vulnerabilities

- **Confidentiality**
  - Protocol flaw
  - Eavesdropptng
  - Passive Wiretap
  - Misdelivery
  - Exposure within the network
  - Traffic flow analysis
  - Cookie
- **Integrity**
  - Protocol flaw
  - Active wiretap
  - Impersonation
  - Falsification of message
  - Noise
  - Web site defacement
  - DNS attack
- **Availability**
  - Protocol flaw
  - Transmission or component failure
  - Connection flooding
  - DNS attack
  - Traffic redirection
  - Distributed denial of service

Network Security Controls

- Security Threat Analysis
- Design and Implementation
- Architecture
- Encryption
- Content Integrity
- Strong Authentication
- Access Control