

MIS 3360

Chapter 9: Security



Figure 9-1: CSI/FBI Survey

- Survey conducted by the Computer Security Institute (www.gocsi.com).
- Based on replies from 530 U.S. Computer Security Professionals.
- Fewer than twenty firms reported quantified dollar losses.

2

Figure 9-1: CSI/FBI Survey

Had at Least One Security Incident in This Category (May Have Had Several)	Percent Reporting an Incident in 1997	Percent Reporting an Incident in 2003	Number Reporting Quantified Losses in 2003	Average Reported Annual Loss/Firm (1000s) in 1997	Average Reported Annual Loss/Firm (1000s) in 2003
Viruses	82%	82%	254	\$76	\$200
Insider Abuse of Net Access	Not Asked	80%	180	Not Asked	\$136
Laptop Theft	58%	59%	250	\$38	\$47
Unauthorized Access by Insiders	40%	45%	72	Not Asked	\$31
Denial of Service	24%	42%	111	\$77	\$1,427
System Penetration	20%	36%	88	\$132	\$56
Sabotage	14%	21%	61	\$164	\$215

Figure 9-2: Viruses and Worms



- **Viruses:** pieces of code that attach to other programs
 - Virus code executes when infected programs execute
 - Infect other programs on the computer
 - Spread to other computers by e-mail attachments, webpage downloads, etc.
 - Antivirus programs are needed to scan arriving files
 - Users often fail to keep their computer antivirus programs up to date
 - Antivirus filtering on the e-mail server works even if users are negligent

4

Figure 9-2: Viruses and Worms



- **Worms** are complete programs
 - Self-propagating worms identify victim hosts, jump to them, and install themselves
 - Can do this because hosts have vulnerabilities
 - Vendors develop patches for vulnerabilities but companies often fail to apply them
 - Firewalls can stop many worms by forbidding access to most ports
 - E-mail worms can get around antivirus filtering

5

Figure 9-2: Viruses and Worms



- Blended Threats
 - Combine the spreading characteristics of viruses and worms
- Payloads
 - Programs that can do damage to infected hosts
 - Erase hard disks, send users to pornography sites if they mistype a URL
 - **Trojan horses:** exploitation programs disguise themselves as system files

6

Figure 9-3: Human Break-Ins (Hacking)



- Hacking
 - Breaking into a computer
 - Hacking is intentionally using a computer resource without authorization or in excess of authorization
 - Prosecutable if do a certain amount of damage
- Scanning Phase
 - Send attack probes to map the network and identify possible victim hosts
 - Like a robber casing a neighborhood
 - Finds active IP addresses that's vulnerable
 - Identifies type of computer at that address via open ports, etc.
 - [Nmap](#) program is popular (Figure 9-4)

7

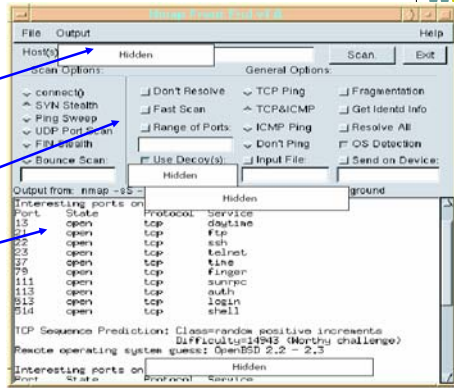
Fig 9-4: Nmap Scanning Output



IP Range to Scan

Type of Scan

Identified Host and Open Ports



Human Break-Ins (Hacking)



- **The Exploit**
 - The Term "Exploit" is Used in Two Ways
 - The actual break-in
 - Exploit is the program used to make the break-in
 - Super user accounts (administrator and root) can do anything
 - If application running with super user privileges is compromised, the attacker gains super user privileges
- **After the Break-In**
 - Become invisible by deleting log files
 - Create a backdoor (way to get back into the computer)
 - Backdoor account—account with a known password and super user privileges
 - Backdoor program—program to allow reentry; usually Trojanized
 - Do damage at leisure

9

Figure 9-3

Denial-of-Service (DoS) Attacks



- An exploding threat
- Make a computer or network unavailable to users
 - Rarely: sending a single message to bring down a computer
 - Usually: overload a victim with a flood of messages
- **Wikipedia**
 - A DoS attack can be perpetrated in a number of ways:
 - consumption of computational resources, such as bandwidth, disk space, or CPU time
 - disruption of configuration information, such as [routing](#) information
 - disruption of physical network components

10

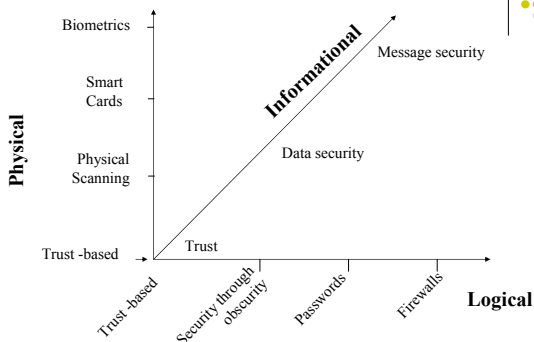
Security Planning Principles



- Security is primarily a Management Issue
 - Without good management, technology cannot be effective.
- Plan-Protect-Respond Cycle
 - Three phases endlessly repeating
 1. **Planning**: preparing for defense
 2. **Protecting**: implementing planned protections
 3. **Responding**: stopping attacks and repairing damage when protections fail

11

3 Dimensions of Network Security



12

Planning Principles



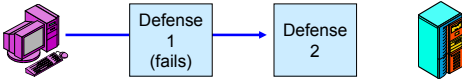
- Risk Analysis
 - Cost of protections should not exceed probable damage
 - Annual probability of damage
 - Damage from a successful incident (Say, \$50,000)
 - Times the annual probability of success (say 10%)
 - Gives the probable annual loss (\$5,000)

13
Figure 9-7

Planning Principles

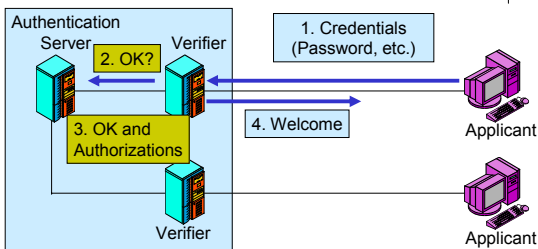


- Defense in Depth
 - Every protection breaks down sometimes
 - Attacker should have to break through several lines of defense to succeed
 - Providing this protection is called **defense in depth**



14
Figure 9-7

Authentication & Authorization



Password Authentication



- Benefits
 - Ease of use for users (familiar)
 - Inexpensive because built into operating systems
- Often weak (easy to crack)
 - Word and name passwords are common
 - Can be cracked quickly with dictionary attack
- Passwords should be complex
 - Mix case, digits, and other keyboard characters (\$, #, etc.)
 - Can only be cracked with brute force attacks (trying all possibilities)
 - Six to eight characters minimum

16
Figure 9-9:

Figure 9-10: Digital Certificate Authentication



- [Digital Certificate](#)
 - User gets secret private key and non-secret public key
 - Digital certificates give the name of a true party and his or her public key



17

Figure 9-10: Digital Certificate Authentication

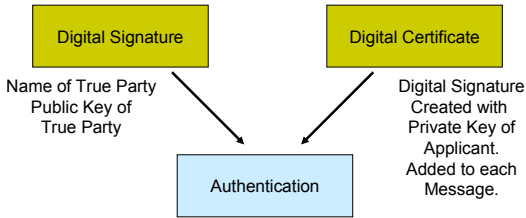


- Testing a [Digital Signature](#)
 - Applicant performs a calculation with his or her private key
 - Verifier tests calculation using the public key found in the true party's digital certificate
 - If the test succeeds, the applicant must be the true party



18

Figure 9-11: Testing a Digital Signature



19

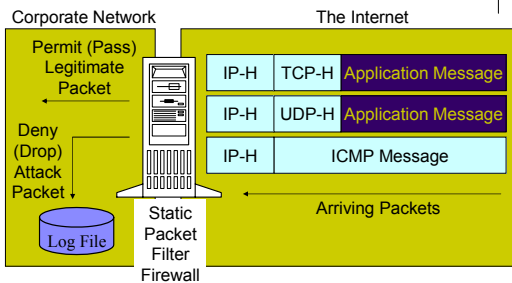
Digital Certificate Authentication



- Strong Authentication
 - The strongest method today
- Expensive and Time-Consuming to Implement
 - Software must be added to clients and servers, and each computer must be configured
 - Expensive because there are so many clients in a firm

20

Figure 9-13: Firewall Operation



21

Access Control List (ACL) for a Packet Filter Firewall



- 1. If destination IP address = 60.47.3.9 AND TCP destination port = 80 OR 443, PASS
 - [connection to a public webserver]
- 2. If ICMP Type = 0, PASS
 - [allow incoming echo reply messages]
- 3. If TCP destination port = 49153 AND 65535, PASS
 - [allow incoming packets to ephemeral TCP port numbers]
- 4. If UDP destination port = 49153 AND 65535, PASS
 - [allow incoming packets to ephemeral UDP port numbers]
- 5. DENY ALL
 - [deny all other packets]

22

Application Firewalls

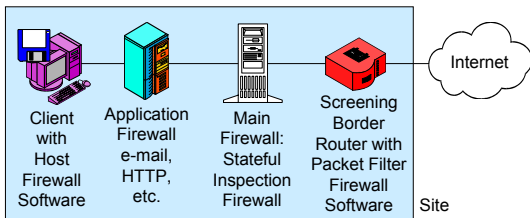


- Application Firewalls
 - Examine application layer messages in packets
 - Packet filter firewalls and stateful firewalls do not look at application messages at all
 - This makes them vulnerable to certain attacks

23

Figure 9-16:

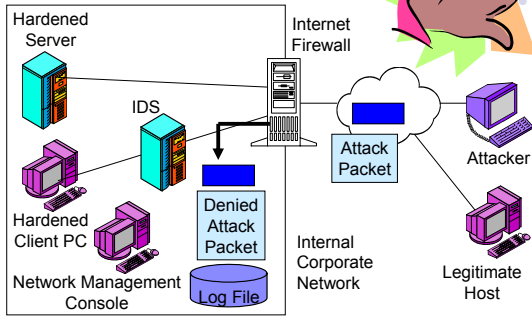
Defense in Depth with Firewalls



24

Figure 9-17:

Figure 9-18: Firewall



Symmetric Key Encryption & Public Key Encryption

Symmetric Key Encryption for Confidentiality

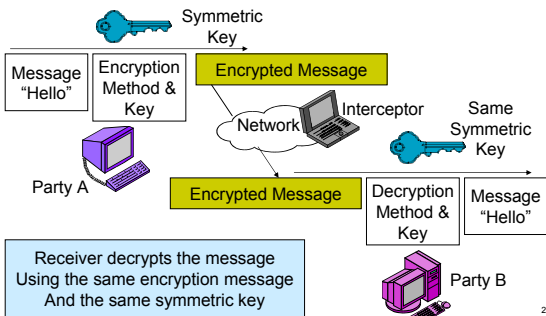


Figure 9-21: Other Aspects of Protection

- **Hardening Servers and Client PCs**
 - Setting up computers to protect themselves
 - **Server Hardening**
 - Patch vulnerabilities
 - Minimize applications running on each server
 - Use host firewalls
 - Backup so that restoration is possible
 - **Client PC Hardening**
 - As with servers, patching vulnerabilities, minimizing applications, having a firewall, and implementing backup

Figure 9-21: Other Aspects of Protection



- Vulnerability Testing
 - Protections are difficult to set up correctly
 - Vulnerability testing is attacking your system yourself or through a consultant
 - There must be follow-up to fix vulnerabilities that are discovered

28

Incident Response



- Response Phases
 - Detecting the attack
 - Stopping the attack
 - Repairing the damage
 - Punishing the attackers

29

Figure 9-22:

Incident Response - Disasters



- Natural and attacker-created disasters
- Can stop business continuity (operation)
- Data backup and recovery are crucial for disaster response
- Dedicated backup facilities versus real-time backup between different sites
- Business continuity recovery is broader
- Protecting employees
- Maintaining or reestablishing communication
- Providing exact procedures to get the most crucial operations working again in correct order

30

Figure 9-22:
