CSIS 4222

Ch 23: ICMP

Ch 30: Security

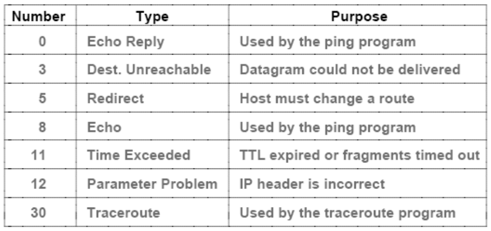
IP Error Handling

- IP uses "best-effort" delivery (datagrams can be lost, duplicated, delayed, or delivered out of order)
- Error detection in IP:
  - Header checksum is used to verify that the header arrived intact
  - The IP header contains a TIME TO LIVE field used to prevent a datagram from circulating forever if router forwarding tables incorrectly introduce a circular path

Internet Control Message Protocol (ICMP)

- Response to a checksum error:
  - The receiver cannot know which header bits were altered, so the datagram must be discarded (receiver cannot send an error message back - the source address in the header could be corrupt)
- ICMP is a companion protocol (of IP) used to report errors back to the original source
- IP and ICMP are co-dependent
  - IP depends on ICMP to report errors
  - ICMP uses IP to carry error messages

Internet Control Message Protocol (ICMP)



Number	Type	Purpose
0	Echo Reply	Used by the ping program
3	Dest. Unreachable	Datagram could not be delivered
5	Redirect	Host must change a route
8	Echo	Used by the ping program
11	Time Exceeded	TTL expired or fragments timed out
12	Parameter Problem	IP header is incorrect
30	Traceroute	Used by the traceroute program

Figure 23.6 Examples of ICMP messages with the message number and purpose.

Internet Control Message Protocol (ICMP)

ICMP has two kinds of messages:

<u>Reporting errors</u>

- Destination unreachable: no route exists to the address
- Datagram times out: TTL count in the header expires or datagram fragments don't arrive before the timer expires

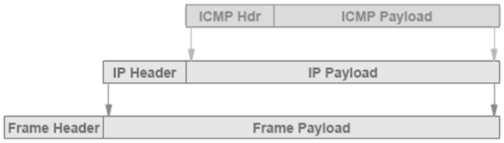
<u>Obtaining information</u>

- Echo Request and Echo Reply used by the ping to test connectivity
- An echo reply carries the same data as the request

ICMP Message Format

ICMP uses IP to transport error messages:

- When a router has an ICMP message to send it creates an IP datagram and encapsulates the ICMP message in it



ICMP Messages

ICMP messages are forwarded like any other datagram, with one exception

- If an ICMP error message causes an error, no error message is sent
- Otherwise, the Internet could become congested with messages about error messages

Questions Regarding Security

- What are the major Internet security problems and threats?
- What technical aspects of protocols do criminals exploit?
- What are the key aspects of security?
- What technologies are available to help increase security?

Network Intrusions

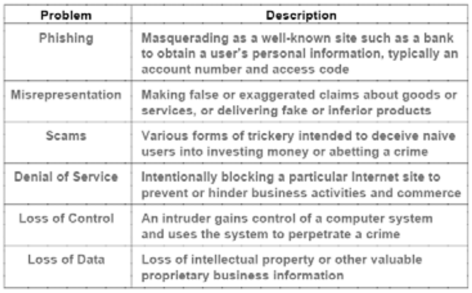
> "The easiest way into a computer is usually through the front door, which is to say, the *login* command."
> *Firewalls and Internet Security, 2nd ed., Cheswick, Bellovin, Rubin*

- Social engineering – Convince someone to let you in, phishing
- Password cracking – Dictionary attack, brute force
- Packet sniffing – Eavesdrop on telnet, FTP, etc. with Wireshark

Network Intrusions

- Vulnerable software – Buffer overflow to insert malicious code or cause a crash
  - Services running and open ports can be like open doors and windows.
    - Use `netstat -a` on Linux or Windows to see them
- Viruses – Malicious code usually exchanged via email attachments, worms
- Wireless vulnerabilities – War driving, weak encryption

Criminal Exploits and Attacks



Problem	Description
Phishing	Masquerading as a well-known site such as a bank to obtain a user's personal information, typically an account number and access code
Misrepresentation	Making false or exaggerated claims about goods or services, or delivering fake or inferior products
Scams	Various forms of trickery intended to deceive naive users into investing money or abetting a crime
Denial of Service	Intentionally blocking a particular Internet site to prevent or hinder business activities and commerce
Loss of Control	An intruder gains control of a computer system and uses the system to perpetrate a crime
Loss of Data	Loss of intellectual property or other valuable proprietary business information

Criminal Exploits and Attacks

- First step is to gather information
- Attacks can be more focused and less likely to be detected
  - Mapping
    - Find info such as IP addresses, OS's used, services offered
    - ping can be used to determine IP addresses
    - *Port scanning* sequentially contacts port numbers to see which respond

Criminal Exploits and Attacks

Packet Sniffing

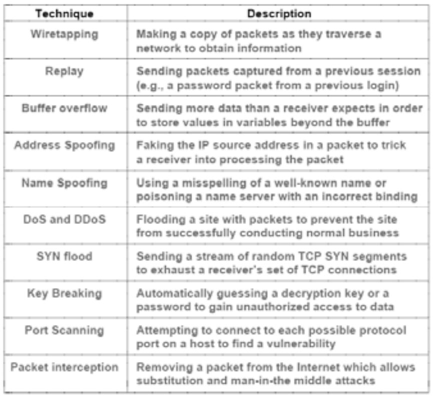
- Wireshark
  (Carnivore - the FBI’s packet sniffing tool)
- Eavesdrop on user names and passwords from telnet or ftp sessions
  - Encrypt everything, particularly passwords!
- Detect packet sniffing by detecting network interfaces running in promiscuous mode
  - Ping reply is likely to have correct IP address but wrong MAC address

Criminal Exploits and Attacks

- It is important to distinguish between
  - A conventional crime that is committed using the Internet in an incidental way
    (The most widespread by far)
  - A crime that is specific to the Internet
- Our discussion will focus on:
  - Ways that criminals exploit technology
  - Technologies that have been created to make crime more difficult

Figure 30.2

Techniques used in security attacks



Technique	Description
Wiretapping	Making a copy of packets as they traverse a network to obtain information
Replay	Sending packets captured from a previous session (e.g., a password packet from a previous login)
Buffer overflow	Sending more data than a receiver expects in order to store values in variables beyond the buffer
Address Spoofing	Faking the IP source address in a packet to trick a receiver into processing the packet
Name Spoofing	Using a misspelling of a well-known name or poisoning a name server with an incorrect binding
DoS and DDoS	Flooding a site with packets to prevent the site from successfully conducting normal business
SYN flood	Sending a stream of random TCP SYN segments to exhaust a receiver's set of TCP connections
Key Breaking	Automatically guessing a decryption key or a password to gain unauthorized access to data
Port Scanning	Attempting to connect to each possible protocol port on a host to find a vulnerability
Packet interception	Removing a packet from the Internet which allows substitution and man-in-the middle attacks

Criminal Exploits and Attacks

Wiretapping

- An unauthorized third party listens to an ongoing conversation
- Conversation scripts/data can be captured
- Captured data can be used in replay attacks
- Wiretapping is especially easy when packets travel across a wireless LAN because a physical connection is not required

Criminal Exploits and Attacks

Packet Interception

An intermediary can modify packets as they pass from source to destination

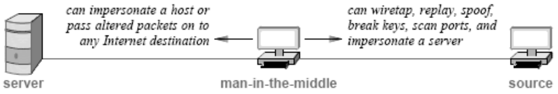

can impersonate a host or pass altered packets on to any Internet destination
can wiretap, replay, spoof, break keys, scan ports, and impersonate a server
server
man-in-the-middle
source

Figure 30.4 A man-in-the middle configuration and the attacks it permits.

Criminal Exploits and Attacks

Spoofing

- Impersonate a trusted host in order to launch various attacks
- Example, address spoofing in ARP:
  - Attacker broadcasts an ARP reply that binds an arbitrary IP address, *A*, to the attacker's MAC address
  - When any host on the network sends a packet to *A*, the packet will be forwarded to the attacker instead

Criminal Exploits and Attacks

IP Spoofing

– Attacker modifies protocol to place an arbitrary IP address in source field

– This is often used in denial-of-service attacks to hide the originators of the attack

Countermeasure: Use *ingress filtering* on router to check that incoming datagram IP address is in the range of addresses known to be reachable from that interface

Criminal Exploits and Attacks

Name Spoofing

Using a routing protocol to send incorrect routes

– Such as sending a DNS message that stores an incorrect binding in a DNS server

– It can use a slight misspelling of a well-known domain to give a user the impression that they have reached a trusted site (phishing attacks)

Criminal Exploits and Attacks

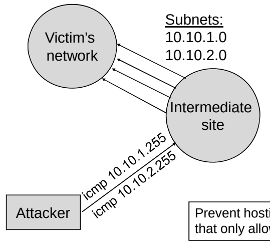
Denial of Service (DoS)

Create so much work for a network or host that it cannot perform

– The attacker consumes the server's resources

- Legitimate users experience long delays or have their connections rejected

Denial-of-Service : Smurf Attack



Cisco router command to block intermediate site:

```
no ip directed broadcast
```

Prevent hosting attacker by using access lists on routers that only allow src on that network to pass through

Spoof src address to be in Victim's network
Packets sent to broadcast address of subnets

Criminal Exploits and Attacks

SYN flooding

– Send huge number of TCP SYN segments with spoofed source addresses

– Receiver allocates a TCP control block for each connection, sends a SYN + ACK, and waits for a response (which never comes)

– Eventually, all control blocks are allocated

– No further connections can be opened

– Most *current* OS's prevent this

Criminal Exploits and Attacks

Distributed Denial of Service (DDoS)

Many hosts throughout the Internet each send a stream of packets and bring down a server

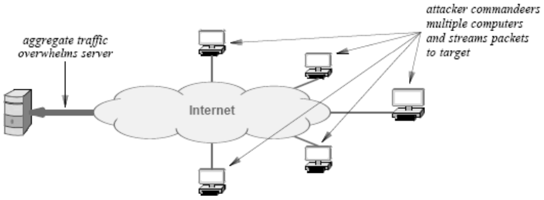

attacker commandeers multiple computers and streams packets to target
aggregate traffic overwhelms server
Internet

Figure 30.3 Illustration of a Distributed Denial of Service attack.

DDoS Attack

- Do port scan to find vulnerable open ports on numerous hosts across the Internet
- Gain access to user accounts on these hosts
- Install and run a malicious program at each host
- Master program instructs these programs to launch a DoS attack at the same target
  - Feb 2000: eBay, Yahoo, CNN, etc. were attacked this way

Criminal Exploits and Attacks

Hijacking

- Suppose Alice and Bob have an ongoing connection and Eve is monitoring packets (knows sequence number, ACK number, receiver window, etc…)
- Eve hijacks connection and launches DoS attack on Alice
- Eve spoofs IP datagrams to Bob

How to Take Out a Win 95/NT Box

Ping of Death

- Send an illegal sized ICMP datagram

```
ping -l 65510 ip.address
```

- Most systems won't allow sending this size ICMP, but Win 95/NT did
- Gets fragmented, but reassembly tends to overflow buffers and cause crashes

Security Policy

What is a *secure* network?

- Each organization defines the level of access that is permitted or denied

- Security policies are complex
  - They must state clearly and unambiguously the items that are to be protected
  - Involves human behavior as well as computer/network facilities
  - Need to assess the costs and benefits of various security policies
  - The policy does not specify how to achieve protection

Security Policy Considerations

Integrity

- Protection from change
- Is the data that arrives at a receiver identical to the data that was sent?

Availability

- Protection against disruption of service
- Does data remain accessible for legitimate uses?

Confidentiality

- Is data protected against unauthorized access?

Privacy

- Ability of a sender to remain anonymous
- Is the sender's identity revealed?

Responsibility and Control

Accountability

- How an audit trail is kept: who is responsible for each item of data?
- How to keep records of access and change?

Authorization

- Responsibility for each item of information
- Who is responsible for where information resides?
- How does a responsible person approve access and change?

Responsibility and Control

- An organization must control access to information
- A key aspect of control concerns authentication
  - Validation of identity
  - Different users may have different authorization for accessing and changing data

Access Control and Passwords

- Which users or application programs can access data?
  - Some OSs implement an access control list (ACL) for each object that specifies who is allowed to access the object
  - In other systems, each user is assigned a password for each protected resource
- When extending ACLs and passwords across a network steps must be taken to:
  - prevent unintentional disclosure
  - assure that passwords are not easy to guess

Hashing: An Integrity and Authentication Mechanism

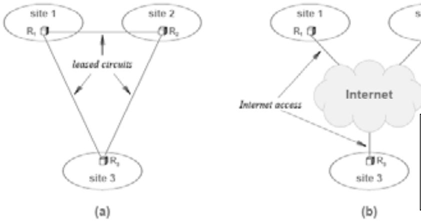
Used to guarantee the integrity of messages against intentional change

- Message authentication code (MAC)
- Typical encoding use cryptographic hashing
- Digital signatures use a secret key where the sender
  - uses the key to compute a hash *H* of input message
  - transmits *H* along with the message
- Receiver knows a message that arrives with a valid hash *H* is authentic

Virtual Private Networks (VPN)

- Two approaches to building corporate intranet for an organization with multiple sites:
  - Private network connections (confidential)
  - Public internet connections (low cost)
- Virtual Private Network
  - Achieve both confidentiality and low cost
  - Implemented in software

Virtual Private Networks



VPN software in router at each site gives appearance of a private network

Figure 30.10 Sites connected by (a) leased circuits and (b) the Internet.

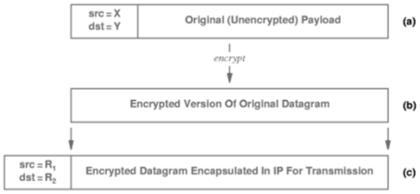
Virtual Private Network

- Obtain internet connection for each site
- Choose router at each site to run VPN software
- Configure VPN software in each router to know about the VPN routers at other sites
- VPN software acts as a packet filter; next hop for outgoing datagram is another VPN router (can also add firewall)
- Each outgoing datagram is encrypted

Tunneling

- Want to encrypt entire datagram so source and destination addresses are not visible on the Internet
- How can internet routers do proper forwarding?
- Solution: VPN software encrypts entire datagram and places inside another for transmission
- Called IP-in-IP tunneling (encapsulation)

Tunneling


src = X
dst = Y
Original (Unencrypted) Payload
(a)
encrypt
Encrypted Version Of Original Datagram
(b)
src = R_1
dst = R_2
Encrypted Datagram Encapsulated In IP For Transmission
(c)

- Datagram from computer X at site 1 to computer Y at site 2
- Router R_1 on site 1 encrypts, encapsulates in new datagram for transmission to router R_2 on site 2