NETWORK INTRUSION

Information Security in Systems & Networks

Public Development Program

Sanjay Goel

University at Albany, SUNY

Fall 2006

Network Attacks

Learning Objectives

- Students should be able to:
  - Recognize different mechanisms for ARP Poisoning and Session Hijacking.
  - Identify vulnerabilities associated with these types of attacks.
  - Decide upon defenses to protect against these attacks.

Network Attacks

ARP

- Each node connected to the Ethernet LAN has two addresses MAC address & IP address
- MAC address is hardwired into the specific network interface card (NIC) of the node
  - MAC addresses are globally unique and with this address the Ethernet protocol sends the data back and forth.
  - Ethernet builds data frames that contain the MAC address of the source and destination computer.
- IP address is a virtual address and is assigned by software.
  - IP communicates by constructing packets which are different from frame structure.
  - These packets are delivered by the network layer (Ethernet) that splits the packets into frames, adds an Ethernet header and sends them to a network component.

Network Attacks

ARP

- IP and Ethernet work together. Packets are sent over Ethernets.
  - Ethernet devices do not understand the 32-bit IPv4 addresses.
  - They transmit Ethernet packets with 48-bit Ethernet addresses.
- An Ethernet frame is built from IP packet, but for the construction of Ethernet frame the MAC address of the destination computer is required.
- An IP driver must translate an IP destination address into an Ethernet destination address.
  - The Address Resolution Protocol (ARP) is used to determine these mappings.
  - For efficiency the ARP allows the address translation to be cached in the routers.

Network Attacks

ARP

- There is considerable risk here if un trusted nodes have write access to the local net. Such a machine could emit phony ARP queries or replies and divert all traffic to itself; it could then either impersonate some machines or simply modify the data streams *en passant*.
- This is called ARP *spoofing*

Network Attacks

ARP Poisoning

- In ARP poisoning the hacker updates the target computer's ARP cache with a forged ARP request and reply packets in an effort to change the MAC address to one that the attacker can monitor.
  - Since ARP replies are forged, the target computer sends frames that were meant for the original destination to the attacker's computer first so the frames can be read. A successful ARP attempt is invisible to the user

Network Attacks

ARP Poisoning

- Static ARP table entries
  - Scalability Issues
    - Critical Machines Only
    - Separation of Servers and Workstations
  - Permanent not always permanent
    - RFC compliance
- Network Segmentation
  - Economic Factors
  - Added Complexity
- Attack Detection
  - Packet Anomalies
  - ARP Traffic Anomalies
    - Ethernet Fields\ARP fields do not match
    - Monitor for ARP Reply\Request matches
    - Monitor ARP traffic for abnormally high percentages of certain MAC addresses

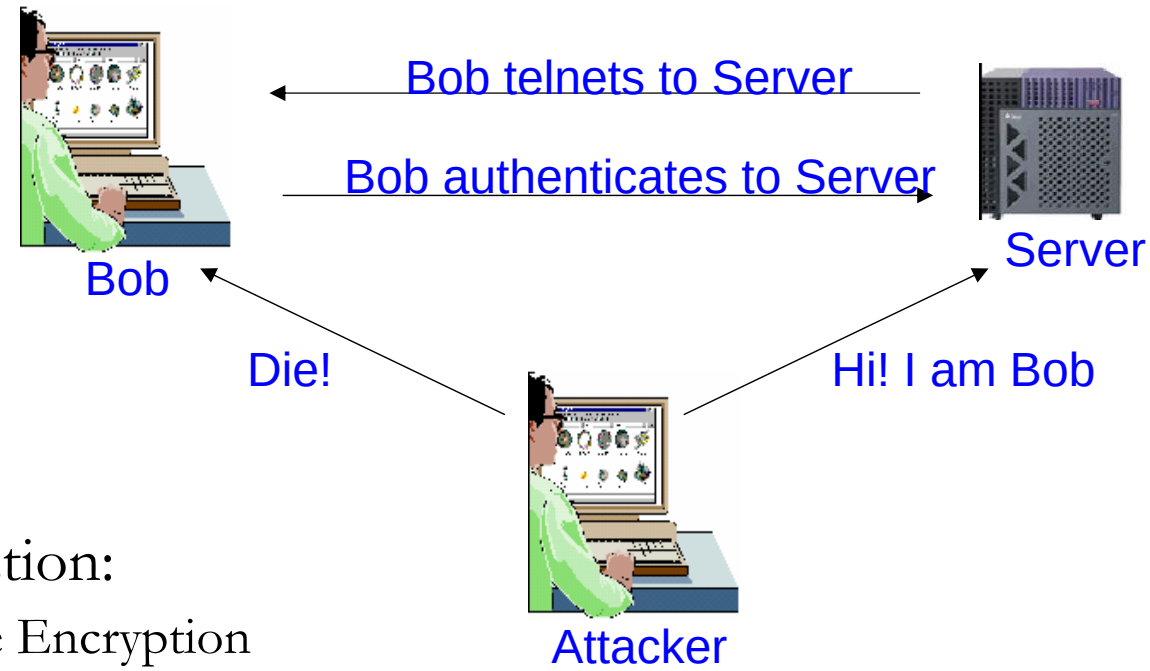
Network Attacks

Session Hijacking: Definitions

- Definition: Hacker takes over an existing active session and exploits the existing trust relationship
- Process:
  - User makes a connection to the server by authenticating using his user ID and password.
  - After the user authenticates, the user has access to the server as long as the session lasts.
  - Hacker takes the user offline by denial of service
  - Hacker gains access to the user by impersonating the user
- Typical Behaviors: Attacker usually monitors the session, periodically injects commands into session and can launch passive and active attacks from the session.

Network Attacks

Session Hijacking: Process



- Protection:
  - Use Encryption
  - Use a secure protocol
  - Limit incoming connections
  - Minimize remote access
  - Have strong authentication

Session Hijacking

Process

- Reliable Transport
  - At sending end file broken to packets
  - At receiving end packets assembled into files
- Sequence numbers are 32-bit counters used to:
  - Tell receiving machines the correct order of packets
  - Tell sender which packets are received and which are lost
- Receiver and Sender have their own sequence numbers

Session Hijacking

Process

- When two parties communicate the following are needed:
  - IP addresses
  - Port Numbers
  - Sequence Number
- IP addresses and port numbers are easily available
  - Hacker usually has to make educated guesses of the sequence number
  - Once attacker gets server to accept the guessed sequence number he can hijack the session.

Session Hijacking

Popular Programs

- Juggernaut
  - Network sniffer that that can also be used for hijacking
  - Get from http://packetstorm.securify.com
- Hunt
  - Can be use to listen, intercept and hijack active sessions on a network
  - http://lin.fsid.cvut.cz/~kra/index.html
- TTY Watcher
  - Freeware program to monitor and hijack sessions on a single host
  - http://www.cerias.purdue.edu
- IP Watcher
  - Commercial session hijacking tool based on TTY Watcher
  - http://www.engrade.com

Session Hijacking

Protection

- Use Encryption
- Use a secure protocol
- Limit incoming connections
- Minimize remote access
- Have strong authentication

Network Intrusions (Other)

Summary

- The network protocols were not designed with intrinsic security
  - Weaknesses in the protocols can be exploited to launch attacks
- Two attacks that have been discussed
  - ARP Attacks
  - Session Hijacking attacks