CS 640 Introduction to Computer Networks

Lecture24

Network security (continued)

- Key distribution
- Secure Shell
  - Overview
  - Authentication
  - Practical issues
- Firewalls
- Denial of Service Attacks
  - Definition
  - Examples

Key Distribution – a first step

- How can we be sure a key belongs to the entity that purports to own it?
- Solution = certificates
  - special type of digitally signed document:

    "I certify that the public key in this document belongs to the entity named in this document, signed X."
  - X is the name of the entity doing the certification
  - Only useful to the entity which knows the public key for X
  - Certificates themselves do not solve key distribution problem but they are a first step
- Certified Authority (CA)
  - administrative entity that issues certificates
  - useful only to someone that already holds the CA's public key
  - can trust more than one CA

Key Distribution (cont)

- Chain of Trust
  - if *X* certifies that a certain public key belongs to *Y*, and *Y* certifies that another public key belongs to *Z*, then there exists a chain of certificates from *X* to *Z*
  - someone that wants to verify *Z*'s public key has to know *X*'s public key and follow the chain
  - X.509 is a standard for certificates
- Certificate Revocation List
  - Means for removing certificates
  - Periodically updated by CA

Key Distribution (cont.)

- PGP (Pretty Good Privacy) provides email encryption and authentication
- Uses "web of trust" instead of "chain of trust"
  - You assign various levels of trust to public keys (e.g. if you got the key when you met face to face you trust it a lot)
  - People certify others' public keys
  - You trust a public key if it has enough "chains of trust"
    - The more disjoint paths in the trust graph the better
    - The shorter the paths the better
    - The more you trust the heads of the paths the better

Network security (continued)

- Key distribution
- Secure Shell
  - Overview
  - Authentication
  - Practical issues
- Firewalls
- Denial of Service Attacks
  - Definition
  - Examples

Secure Shell (SSH) Overview

- SSH is a **secure** remote virtual terminal application
  - Provides encrypted communication over an insecure network
    - Assumes eavesdroppers can hear *all* communications between hosts
    - Provides different methods of authentication
    - Encrypts data exchanged between hosts
  - Intended to replace insecure programs such as telnet, rsh, etc.
  - Includes capability to securely transfer file
    - SCP
  - Can forward X11 connections and TCP ports securely
- Very popular and widely used
  - Not invulnerable!

SSH authentication

- Client authenticates server
  - The client caches the public keys of all servers it talks to
    - User can add new keys to the cache
    - Otherwise the user is warned when first connecting to a given server
- Server authenticates client
  - Through user's password
  - Public RSA key the user puts ahead of time on the server
  - Other, riskier methods
- At connection setup server and client agree on a session key used to encrypt communication
  - Many algorithms allowed (IDEA, Blowfish, Triple DES, etc.)

SSH in Practice

- Host public/private key is generated when SSH is installed
  - Public key must be in ~/.ssh/known_hosts on remote systems
- *ssh-keygen* command is used to generate users public/private keys
  - Public key copied to ~/.ssh/authorized_keys on remote systems
  - Each private key in ~/.ssh/identity requires a pass phrase when used
    - *Ssh-agent* eliminates need for repeated typing of pass phrase
- Password authentication is vulnerable to guessing attacks
  - Server logs all unsuccessful login attempts
- X11 and port forwarding enable encrypted pipe through the Internet
  - Can be used to securely access insecure application eg. SMTP
  - Can be used to circumvent firewalls

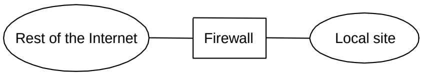
Network security (continued)

- Key distribution
- Secure Shell
  - Overview
  - Authentication
  - Practical issues
- Firewalls
- Denial of Service Attacks
  - Definition
  - Examples

Firewalls – overview

- Firewalls restrict communication between an organization’s computers and the outside world
  - Keep the bad guys on the outside from exploiting vulnerabilities on the inside
  - Without restricting legitimate traffic
- NAT boxes implement a popular firewall policy
  - Allow internal clients to connect to outside servers
  - Do not allow inbound connections
- Two types of firewalls
  - Filter based (layer 4)
  - Proxy based (application layer)

Firewalls



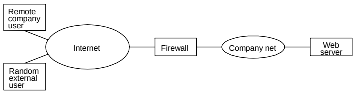
- Filter-Based Solution
  - Apply a set of rules to packets
    - Look at packet headers
  - Example of rules

action	ourhost	port	theirhost	port	comment
block	*	*	BLASTER	*	We don’t trust this system
allow	OUR_GW	25	*	*	Connects to our SMTP srvr

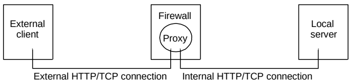
  - Default: forward or not forward?
  - How dynamic?

Proxy-Based Firewalls

- Problem: complex policy
- Example: web server



- Solution: proxy



- Design: transparent vs. classical
- Limitations: attacks from within

Network security (continued)

- Secure Shell
  - Overview
  - Authentication
  - Practical issues
- Firewalls
- Denial of Service Attacks
  - Definition
  - Examples

Denial of Service (DoS) Attacks

- A general form of attacking inter-networked systems
  - Based on overloading end systems (or network)
  - Result is sever reduction in performance or complete shutdown of target systems
- Focus of attack can be links, routers (CPU) or end hosts
- Flooding attacks pretty common nowadays
- Other most general form of attack is a break-in
  - Port scans
  - Buffer overflows
  - Password cracking…

Overloading a System

- The goal of DoS is to drown legitimate traffic in a sea of garbage traffic
  - Clients experience delays due to congestion
    - Dropped packets lead to exponential backoff in timeouts
  - Routers can become overloaded
- Servers become overloaded by increased number of connect requests
  - TCP connection setup requires state on server
  - Server is required to respond to SYN from clients
  - Clients don’t respond to server’s response

IP Spoofing

- Insert a different source IP address in TCP and IP headers
  - DoS attackers spoof for two reasons
    - They don’t want to be discovered
    - Spoofing can add additional load
- If attacker spoofs a legitimate IP address
  - Reset can be triggered by either attacked host or actual IP host
    - Frees resources immediately on server
  - Carefully chosen sequence #s block new connections from host
- Attackers spoof with random IP addresses
  - Server response to client SYN will be lost
  - Server will not free resources for 75 seconds (typically)
  - SYN cookies on allow server kernel not to keep state

Key Elements of DoS Attack

- Expansion in required work
  - Easy for me, harder for you
  - Expansion in IP spoofing
    - Me: generate SYNs as fast as possible (microseconds)
    - You: Timeout a SYN open every 75 seconds
- Best effort protocols
  - Drop tail queues
  - No source specificity
  - Clients can be starved or slowed to crawl

DoS Attack Characteristics

- Expansion makes a only a few systems necessary
  - DDoS: attack from as many places as possible
    - Enables better utilization of network resources
    - Helps to prevent countermeasures
    - Helps to obscure attackers
- DoS software readily available
  - Most found in IRC chat rooms
- DoS attacks frequently preceded by break-ins to install DoS software onto “zombies”
  - Enables even more anonymity for attacker

CS 640

Things making DoS Attacks easy

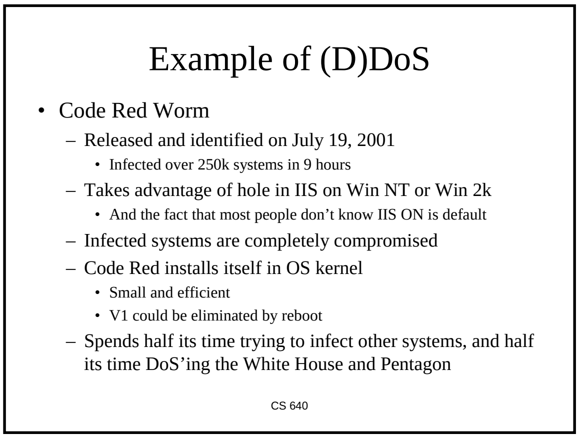
- Lots of systems
- Large networks
- Naïve users with high speed Internet access
- Savvy bad guys
- Lots of free DoS software
- Poor operating and management policies
- Hugely complex software (on endhosts) with lots of well publicized holes
- Lack of means for stopping attacks

CS 640

Dealing with DoS Attacks

- Don’t reserve state until receipt of client ACK
  - DOS attackers using spoofing don’t send these
    - Otherwise they would have to keep state
  - Use of crypto to avoid saving state
    - Send one-use key with server response to SYN
    - Response ACK must return key
- Intrusion detection tools
  - Cut off an attack at a firewall if you recognize it
  - Bro, Snort
- IP traceback methods
- There are lots of companies in this space!

CS 640



Example of (D)DoS

- Code Red Worm
  - Released and identified on July 19, 2001
    - Infected over 250k systems in 9 hours
  - Takes advantage of hole in IIS on Win NT or Win 2k
    - And the fact that most people don’t know IIS ON is default
  - Infected systems are completely compromised
  - Code Red installs itself in OS kernel
    - Small and efficient
    - V1 could be eliminated by reboot
  - Spends half its time trying to infect other systems, and half its time DoS’ing the White House and Pentagon