

## Network Security in Practice

Kai Shen

12/7/2009

CSC 257/457 - Fall 2009

1

## Recap: Principles of Network Security

### Cryptography:

- symmetric keys: protocols? weakness?
- public keys: protocol? weakness?

### Confidentiality:

- only sender, intended receiver should "understand" message contents

### Authentication:

- sender, receiver want to confirm identity of each other

### Message Integrity:

- sender, receiver want to ensure message not altered (in transit, or afterwards)

12/7/2009

CSC 257/457 - Fall 2009

2

## Outline

- Key distribution and certification
- Access control: firewalls
- Attacks and counter measures
- Security protocol case studies

12/7/2009

CSC 257/457 - Fall 2009

3

## Key Distribution and Certification

### Symmetric key problem:

- How do Alice and Bob establish shared secret key over network without Trudy's knowledge?

### Public key problem:

- When Alice obtains Bob's public key (from web site, e-mail, diskette), how does she know it is Bob's public key, not Trudy's?

12/7/2009

CSC 257/457 - Fall 2009

4

### Secret Key Distribution: Key Distribution Center (KDC)

- **KDC:** server shares different secret key with *each* registered user (many users).
- Alice, Bob know own symmetric keys,  $K_{A-KDC}$   $K_{B-KDC}$ , for communicating with KDC.

12/7/2009 CSC 257/457 - Fall 2009 5

### Key Distribution using KDC

**Q:** How does KDC allow Bob, Alice to determine shared symmetric secret key to communicate with each other?

Alice and Bob communicate: using R1 as **session key** for shared symmetric encryption

12/7/2009 CSC 257/457 - Fall 2009 6

### Security hole when public keys are not well known

**Man (woman) in the middle attack:** Trudy poses as Alice (to Bob) and as Bob (to Alice)

Trudy gets  $K_T^+(m)$   
 $m = K_T^-(K_T^+(m))$   
 sends  $m$  to Alice encrypted with Alice's public key  
 $m = K_A^-(K_A^+(m))$

12/7/2009 CSC 257/457 - Fall 2009 7

### Public Key Distribution: Certification Authorities

- **Certification authority (CA):** trustable by everyone; every one knows its public key.
- E (person, router) registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by CA - CA says "this is E's public key"

Bob's public key  $K_B^+$   
 CA private key  $K_{CA}^-$   
 digital signature (encrypt)  
 certificate for Bob's public key, signed by CA

12/7/2009 CSC 257/457 - Fall 2009 8

## Certification Authorities (cont.)

When Alice wants to verify Bob's public key:

- gets Bob's certificate (Bob or elsewhere).
- apply CA's public key to Bob's certificate, verify Bob's public key.

12/7/2009      CSC 257/457 - Fall 2009      9

## Outline

- Key distribution and certification
  - key distribution center for distributing secret symmetric keys
  - certification authority for distributing certified public keys
- **Access control: firewalls**
- Attacks and counter measures
- Security protocol case studies

12/7/2009      CSC 257/457 - Fall 2009      10

## Access Control: Firewalls

firewall

isolates organization's internal network from the public Internet through filtering, allowing some data to pass, blocking others.

12/7/2009      CSC 257/457 - Fall 2009      11

## Network-layer Packet Filtering

- firewall is built into the **edge router** connected to the Internet
- router **filters packet-by-packet**, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - TCP SYN and ACK bits

12/7/2009      CSC 257/457 - Fall 2009      12

## Policies in Network-layer Packet Filtering

- **Example 1:** blocking all incoming TCP datagrams with dest port = 80
  - No external clients can access internal Web servers.
- **Example 2:** blocking all TCP datagrams with source or dest port = 23, except for those with source or dest IP = 128.151.67.155 (a particular internal machine)
  - All incoming and outgoing telnet connections have to go through a telnet gateway.
- **Example 3:** blocking all incoming TCP datagrams with ACK bit set to 0
  - Prevents external clients from initiating TCP connections with internal clients, but allows internal clients to connect to outside.

12/7/2009

CSC 257/457 - Fall 2009

13

## More on Network-layer Packet Filtering

- **Advantage:**
  - transparent to network applications
  - incurring little extra overhead/latency
- **Limitation:**
  - relying only on IP/TCP/UDP header info
    - ⇒ not flexible enough
    - ⇒ e.g., firewall can know the IP of the source, but not the "user"

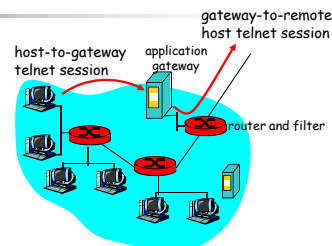
12/7/2009

CSC 257/457 - Fall 2009

14

## Application-layer Gateways

- Access control according to application-layer information.
- **Example:** allow selected internal users to telnet outside.



1. Router filter blocks all telnet connections not originating from gateway ⇒ require all telnet users to telnet through gateway.
2. For authorized users, gateway sets up telnet connection to dest host.

12/7/2009

CSC 257/457 - Fall 2009

15

## Outline

- Key distribution and certification
- Access control: firewalls
  - network-layer firewall
  - application-layer firewall
- Attacks and countermeasures
- Security protocol case studies

12/7/2009

CSC 257/457 - Fall 2009

16

## Network Security Threat: Mapping

**Mapping:**

- before attacking: "scout the area" - find out what services are implemented on network
- Try to determine what host addresses are valid on the network
- Port-scanning: try to establish TCP connection to each port in sequence (see what happens)

**Countermeasures** at the firewall:

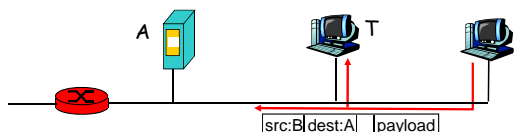
- record traffic entering network
- look for suspicious activity (e.g., IP addresses, ports being scanned sequentially)

12/7/2009 CSC 257/457 - Fall 2009 17

## Network Security Threat: Packet Sniffing

**Packet sniffing:**

- promiscuous NIC reads all packets passing by a broadcast media (e.g. shared-link Ethernet)
- can read all unencrypted data (e.g. passwords)



**Countermeasures:**

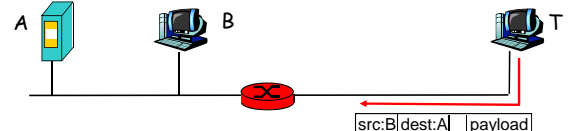
- checks periodically if host interface in promiscuous mode.
- one host per segment of broadcast media (switched Ethernet)
- encrypt all packets.

12/7/2009 CSC 257/457 - Fall 2009 18

## Network Security Threat: IP Spoofing

**IP Spoofing:**

- with root privilege, one can generate "raw" IP packets with any value into IP source address field
- receiver can't tell if source is spoofed
- e.g.: T pretends to be B



**Countermeasures:**

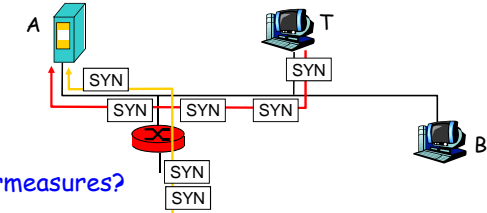
- authentication**
- ingress filtering** - routers should not forward outgoing packets with invalid source addresses

12/7/2009 CSC 257/457 - Fall 2009 19

## Network Security Threat: Denial-of-service Attack

**Denial of service (DOS):**

- SYN flooding: attacker establishes many bogus TCP connections, flood of maliciously generated packets "swamp" receiver
- Distributed DOS (DDOS): multiple coordinated sources swamp receiver
- e.g., T and remote host SYN-attack A



**Countermeasures?**

12/7/2009 CSC 257/457 - Fall 2009 20

### Countermeasure 1: Packet Filtering

**Filtering out attack packets:**

- attack packets carry spoofed IP addresses - hard to filter based on IP address
- if filtering out all SYN packets, then no good connections
- if filtering out some SYN packets, throw out good and bad connections

12/7/2009 CSC 257/457 - Fall 2009 21

### Countermeasure 2: Trace Back

**Trace back to flood source:**

- attack packets with spoofed IPs
- trace back through network statistics
- sources are most likely an innocent, compromised machines

12/7/2009 CSC 257/457 - Fall 2009 22

### Countermeasure 3: Delayed Processing

**Delayed processing or resource allocation:**

- what is the main resource needs triggered by TCP connection?
- data structure allocation and initialization at receipt of real data request, not at receipt of first SYN

12/7/2009 CSC 257/457 - Fall 2009 23

### Stateless TCP

**Stateless TCP** [Shieh et al. NSDI 2005]:

- server side maintains no state about TCP connections.
- **advantage:** TCP connections only require temporary space during packet processing
- state for a TCP connection:
  - receive buffer
  - send buffer
  - various control parameters and network statistics
- how to avoid maintaining such state at server side?
- also useful for transparent server fail-over/migration

12/7/2009 CSC 257/457 - Fall 2009 24

## Outline

- Key distribution and certification
- Access control: firewalls
- Attacks and counter measures
  - mapping, sniffing, spoofing, DOS attack
- Security protocol case studies
  - Application-layer PGP: **secure email**
  - Transport-layer SSL: **secure sockets**
  - Network-layer IPsec: **secure networking**

12/7/2009 CSC 257/457 - Fall 2009 25

## Secure Email: Confidentiality

■ Alice wants to send confidential e-mail,  $m$ , to Bob.

**Alice:**

- generates random *symmetric* private key,  $K_S$ .
- encrypts message with  $K_S$
- encrypts  $K_S$  with Bob's public key.
- sends both  $K_S(m)$  and  $K_B(K_S)$  to Bob.

**Bob:**

- uses his private key to decrypt and recover  $K_S$
- uses  $K_S$  to decrypt  $K_S(m)$  to recover  $m$

12/7/2009 CSC 257/457 - Fall 2009 26

## Secure Email: Sender Authentication and Message Integrity

- How to provide sender authentication and message integrity?
  - generating a digital signature of the message digest using its private key
- Put everything together
  - using one-time session key and the receiver's public key to encrypt a digitally signed message.
  - support confidentiality, sender authentication, and message integrity.
  - PGP (pretty good privacy) for Internet email.

12/7/2009 CSC 257/457 - Fall 2009 27

## Web of Trust: distribution of public keys

- Public key distribution:
  - Certification authority
- Web of trust:
  - If A knows B personally, they can exchange public keys using offline means;
  - If A knows B's public key and trusts B, then A may also take C's public key certificate signed by B.

12/7/2009 CSC 257/457 - Fall 2009 28

## Secure Sockets Layer (SSL)

- **SSL**: transport layer security service to any TCP-based applications
  - used between Web browsers, servers for e-commerce (https).
  - used between IMAP clients and servers.
- **Security services, like before:**
  - data confidentiality by encryption using a symmetric session key, key encrypted with server's public key.
  - source authentication & data integrity by signed message digests
    - an issue: message signing granularity

12/7/2009

CSC 257/457 - Fall 2009

29

## Network Layer Security Protocol IPsec

- Like before:
  - data confidentiality by encryption using a symmetric session key
  - source authentication & data integrity by signed message digests



- Done in a way that is compatible with basic IP routing functions
  - easy deployment - require no router changes

12/7/2009

CSC 257/457 - Fall 2009

30

## Network Security (summary)

### Basic techniques.....

- cryptography (symmetric and public)
- authentication
- message integrity
- key distribution

### .... network security in practice

- firewall
- attacks and countermeasures
- secure application (PGP for email)
- secure transport (SSL)
- secure network (IPsec)

12/7/2009

CSC 257/457 - Fall 2009

31

## Disclaimer

- Parts of the lecture slides contain original work of James Kurose, Larry Peterson, and Keith Ross. The slides are intended for the sole purpose of instruction of computer networks at the University of Rochester. All copyrighted materials belong to their original owner(s).

12/7/2009

CSC 257/457 - Fall 2009

32