Network Security in Practice

Kai Shen

Dept. of Computer Science, University of Rochester

Recap: Principles of Network Security

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

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)

Outline

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

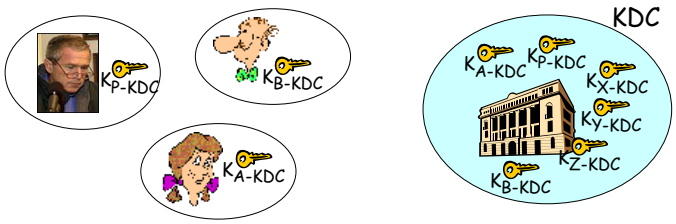
Key Distribution and Certification

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?

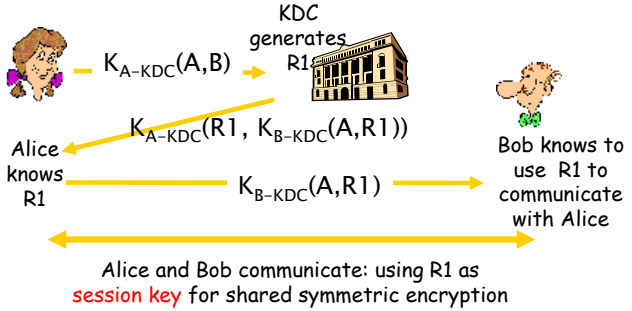
Secret Key Distribution: Key Distribution Center (KDC)

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



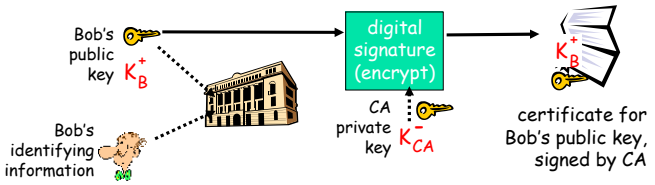
Key Distribution using KDC

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



Public Key Distribution: Certification Authorities

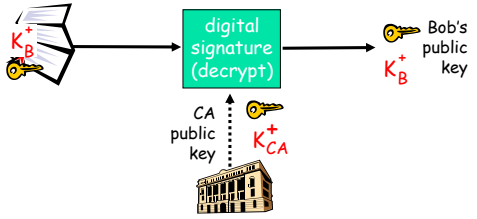
- Certification authority (CA): trustable by everyone; every one knows its public key.
- E (person, router) registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by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



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.



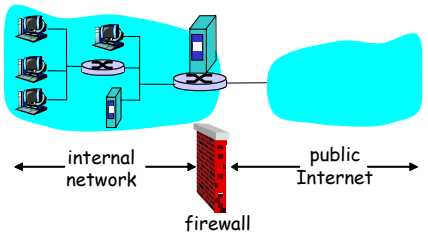
Outline

- 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

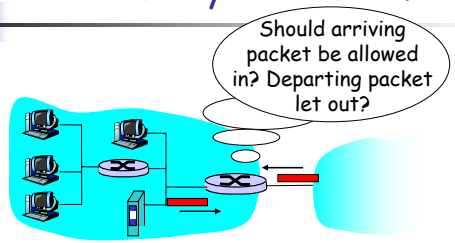
Access Control: Firewalls

firewall

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



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

Policies in Network-layer Packet Filtering

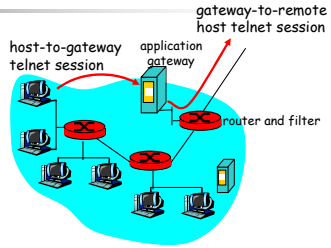
- Example 1: blocking all incoming TCP datagrams with dest port = 80
  - No external clients can access internal Web servers.
- Example 2: blocking all TCP datagrams with source or dest port = 23, except for those with source or dest IP = 128.151.67.155 (a particular internal machine)
  - All incoming 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.

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"

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.

Outline

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

Network Security Threat: Mapping

Mapping:

- before attacking: "scout the area" – find out what services are implemented on network
- Use ping 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)

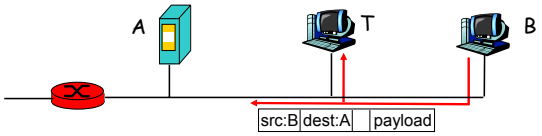
Countermeasures at the firewall:

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

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)



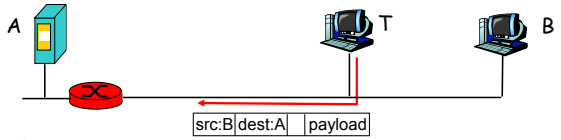
Countermeasures:

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

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



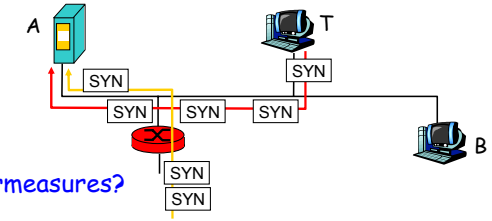
Countermeasures:

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

Network Security Threat: Denial-of-service Attack

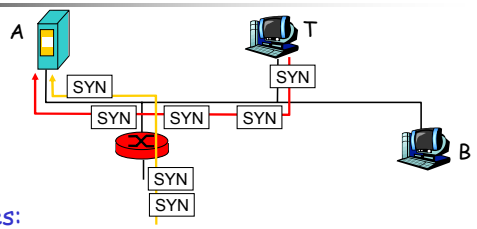
Denial of service (DOS):

- 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?

Countermeasures for DOS Attacks



Countermeasures:

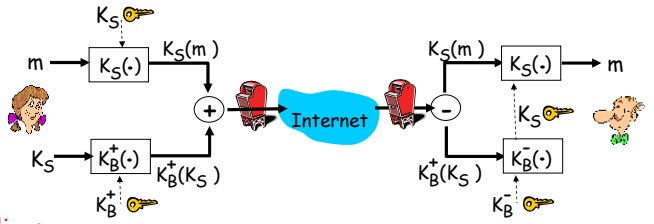
- filter out flooded packets (e.g., SYN): throw out good and bad connections
- trace back to source of floods
  - attack packets with spoofed IPs
  - sources are most likely an innocent, compromised machines
- delayed processing/resource allocation

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

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

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.

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:
  - data encryption
    - Browser generates symmetric session key, encrypts it with server's public key, sends encrypted key to server.
    - Using its own private key, server decrypts session key.
    - All data sent into TCP socket (by client or server) encrypted with session key.

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

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)

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).