More on Network Security

Kai Shen

Dept. of Computer Science, University of Rochester

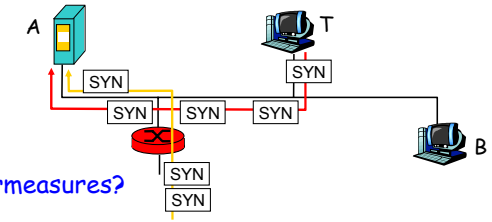
Outline

- Key distribution and certification
- Access control: firewalls
- Attacks and counter measures
  - mapping
  - sniffing
  - spoofing
  - DOS attack
- Security protocol case studies

Network Security Threat: Denial-of-service Attack

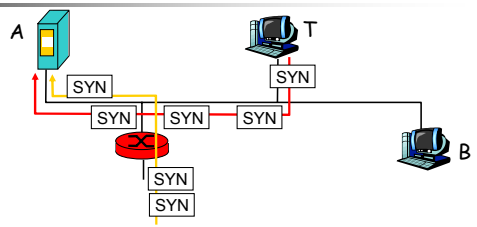
Denial of service (DOS):

- 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?

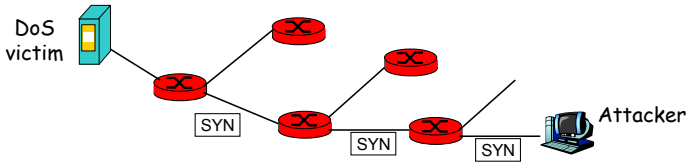
Countermeasure 1: packet filtering



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

Countermeasure 2: Trace Back



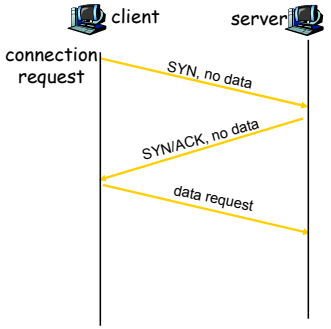
Trace back to flood source:

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

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



Stateless TCP

Stateless TCP [Shieh et al. NSDI 2005]:

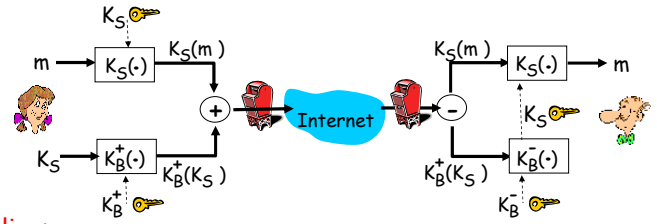
- server side maintains no state about TCP connections.
- advantage: TCP connections only require temporary space during packet processing
- state for a traditional TCP connection:
  - send window buffer
  - various control parameters and network statistics
- how to avoid maintaining such state at server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

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.

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.

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

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).