Network Security in Practice (cont.)

Kai Shen

Network Security Threat: Denial-of-service Attack

- 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 innocent, compromised machines
Countermeasure 3: Delayed Processing

Delayed processing or resource allocation:
- Data structure allocation and initialization at receipt of real data request, not at receipt of first SYN
- What if attacker sends SYN, waits for SYNACK, and then sends some dummy data?

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

Practices of Network Security

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

Secure Email: Confidentiality

Alice wants to send confidential e-mail, m, to Bob.
- encrypts message with Bob's public key, all problems solved?
Secure Email: Confidentiality

Alice:
- generates symmetric 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

- Sender authentication and message integrity:
  - generates a digital signature of the message digest using his/her private key
- Put everything together
  - uses one-time session key and the receiver’s public key to encrypt a digitally signed message
  - supports confidentiality, sender authentication, and message integrity
  - PGP (pretty good privacy) for Internet email

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

- SSL/TLS: transport layer security service to any TCP-based applications
  - used for remote terminal access (SSH)
  - used between Web browsers, servers for e-commerce (https)
  - used between IMAP clients and servers

- Security services:
  - CA-certified public keys.
  - data confidentiality by encryption using a symmetric session key, key encrypted with server’s public key.
  - source authentication & data integrity by signed message digests.

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
  - IPsec packet is recognized as a supported protocol in IP
  - routers who don’t support it can ignore it \( \Phi \) allow incremental deployment with incremental benefits
More on IPsec

- **Transport mode:**
  - IP header
  - IPsec header
  - Payload is data (TCP/UDP)

- **Tunnel mode:**
  - IP header
  - IPsec header
  - Payload is a full IP packet

- Transport mode is more natural for a host-to-host secure conn; tunnel mode is better fit for intermediate segment of secure conn between two routers.

- (Virtual Private Network) VPN:
  - IBM US
  - Internet
  - IBM India

Tor Anonymity Network

- Standard encryption mechanisms protect the content of communication, but not the identities of the comm. parties

- Tor, The Onion Router, anonymity network
  - "Tor directs internet traffic through a free, worldwide, volunteer network consisting of more than four thousand relays to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis." --Wikipedia
  - "Edward Snowden used the Tor Network to send information about PRISM to the Washington Post and The Guardian in June 2013." --Wikipedia

Tor Anonymity Network

- NSA and GHCQ are curious
  - Compromise the source
  - **Quotes from Guardian:** But the documents [NSA leaks] suggest that the fundamental security of the Tor service remains intact. One top-secret presentation, titled 'Tor Stinks', states: "We will never be able to de-anonymize all Tor users all the time." It continues: "With manual analysis we can de-anonymize a very small fraction of Tor users," and says the agency has had "no success de-anonymizing a user in response" to a specific request.
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).