Security Problems in the TCP/IP Protocol Suite

S.M. Bellovin

Presented by:
Machigar Ongtang
Nazneen Irani
Agenda

- Introduction
- TCP Sequence Number Prediction
- Routing
- Authentication Server
Contribution

- Serious security flaws inherent the TCP/IP protocol, regardless of its implementation

- Major causes of vulnerabilities
  - Rely on IP source address for authentication
  - Minimal/no authentication in network control mechanisms, e.g. routing protocol, congestion control, flow control, ICMP messages, etc.

- Defense techniques
TCP Sequence Number Prediction

Client C

Server S

Attacker X

Server S

Trusted Client T

SYN(ISN_C)

SYN(ISN_S), ACK(ISN_C)

ACK(ISN_S)

Data

SYN(ISN_X), SRC=T

ACK(ISN_S), SRC=T

Bad data, malicious command

SYN(ISN_S), ACK(ISN_X)
Defense against Sequence Number Prediction

- Increase the rate of change of ISN.
- Increase the granularity of the increase
  - More possible ISN’s in particular time period, low probability of successful prediction
- Randomizing the increment
- Cryptographic algorithm for ISN generation
- Good logging and alert mechanism
  - Excessive ping request
  - Short-lived TCP connections
  - Unusual Request to Send (RST) packets
Source Routing Vulnerabilities

Defense
- Reject external packets (prevent outside attackers)
- Reject pre-authorized connections via source routing
RIP Vulnerabilities

- Advertise bogus routing information
- Claim a route to a particular unused host (impersonation)
- Claim a route to an active host to draw traffic to itself for inspection/alteration
- Compromise address-based authentication protocol
Defense against RIP attack

- Paranoid gateway to filter packets based on source/destination address
- Check the routes before accepting them
- Authenticate RIP packet. Using public-key is expensive when broadcasting
- Good log generation, notice anomaly
ICMP Vulnerabilities

- ICMP Redirect message from gateways to advise better routes may be spoofed
- Denial of Service attack from spoofed Destination unreachable, Time-to-live Exceeded, Subnet Mask Reply message

Defense

- Check to ensure that the message belongs to particular connection
- Verify whether the replay message contains reasonable sequence number
- Restrict route changes to particular connections
- Honor reply packets only at the appropriate time
Authentication Server

- Alternative to address-based authentication

- Secure because of the second TCP connection

Various Risks:

- Client host not secure
- Authentication message compromised
- Variant of TCP sequence number attack
- DoS Attack

Defense: More secure means of validation like Needham-Shroeder algorithm
1] Finger Service

- Used to find out information about users on remote systems

- Eg.
  FINGER abc@xyz.com

- Loss of privacy and other issues on distributed systems

- Useful information for password crackers

(Windows 2000 and Windows XP do not provide the finger service)
**2] Electronic Mail**

The POP3 client performs the three way handshake to establish a TCP connection.

The POP3 server acknowledges the establishment of a POP3 TCP connection by sending the +OK response to the client.

**Solution:** SSL, SSH, Kerberos
3] Domain Name System (DNS)

- Maps host names to IP addresses eg. cse.psu.edu to 198.2.1.2

- Vulnerabilities:
  - Sequence number attack in resolver implementation
  - Combined attack
  - Spying- Zone transfer request (AXFR) ->includes error code for “refused”

- Hesiod Name server

Recent attacks on DNS servers: PHARMING

4] File Transfer Protocol (FTP)

- FTP Authentication

- Anonymous FTP
  - Some implementations require creation of partial replica of directory tree
  - Truly anonymous
5] Simple Network Management Protocol (SNMP)

- **Aids in network management**: used by network management systems to monitor network-attached devices for conditions that warrant administrative attention.

- **Caveats of SNMP**

6] Remote Booting:

Subvert boot process: A new kernel with altered protection mechanism can be substituted.

- **Two protocols used**:
  - RARP with TFTP: risky since relies on Ethernet
  - BOOTP with TFTP: additional layer of security including 4 byte random transaction ID
Trivial Attacks

- **Vulnerability of Local Network**
  - Eavesdropping
  - Host-spoofing
  - Denial of Service Attack- Broadcast storms

- **Trivial File Transfer protocol**
  - File transfers without authentication

- **Reserved Ports**
  - Berkeley derived TCPs and UDPs- Port number < 1024 => privileged process
  - Neither TCP nor UDP contain any such concept
Comprehensive Defenses (Broad Spectrum Defenses)

- **Authentication**
  - Uses IP source address - can be spoofed
  - Cryptographic authentication needed - Needham Shroeder Protocol
  - Pre-authenticated connections can be implemented safely
  - DNS provides ideal base for authentication systems

- **Trusted systems:**

  Questioning the extent to which Orange book and Red book criteria protect a host from attacks.
• Encryption (implies authentication)

<table>
<thead>
<tr>
<th>Link encryption</th>
<th>End-to-End Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security within hosts</td>
<td></td>
</tr>
<tr>
<td>Data exposed in sending host</td>
<td>Data encrypted in sending host</td>
</tr>
<tr>
<td>Data exposed in intermediate host</td>
<td>Data encrypted in intermediate nodes</td>
</tr>
<tr>
<td>Role of User</td>
<td></td>
</tr>
<tr>
<td>Applied by sending host</td>
<td>Applied by sending process</td>
</tr>
<tr>
<td>Invisible to user</td>
<td>User applies encryption</td>
</tr>
<tr>
<td>Host maintains encryption</td>
<td>User must find algorithm</td>
</tr>
<tr>
<td>One facility for all users</td>
<td>User selects encryption</td>
</tr>
<tr>
<td>Typically done in hardware</td>
<td>Either s/w or h/w implementation</td>
</tr>
<tr>
<td>All or no data encrypted</td>
<td>User chooses to encrypt or no for data item</td>
</tr>
<tr>
<td>Implementation concerns</td>
<td></td>
</tr>
<tr>
<td>Requires one key per host pair</td>
<td>Requires one key per user pair</td>
</tr>
<tr>
<td>Provides node authentication</td>
<td>Provides user authentication</td>
</tr>
</tbody>
</table>
Conclusion:

Security flaws and attacks on TCP/IP protocol suite has been discussed.

Protocol-specific as well as broad spectrum defenses have been suggested.

Take Away:

TCP/IP has a number of security flaws which must be addressed.

“Hosts in a network should not give out information gratuitously.”
THANK YOU