Network Attacks

Chapter 2

Network & Security

Gildas Avoine

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

IUF

SUMMARY OF CHAPTER 2

- Denial of Service
- Spoofing
- Hijacking
- Conclusion and References

DENIAL OF SERVICE

- Denial of Service
- Spoofing
- Hijacking
- Conclusion and References

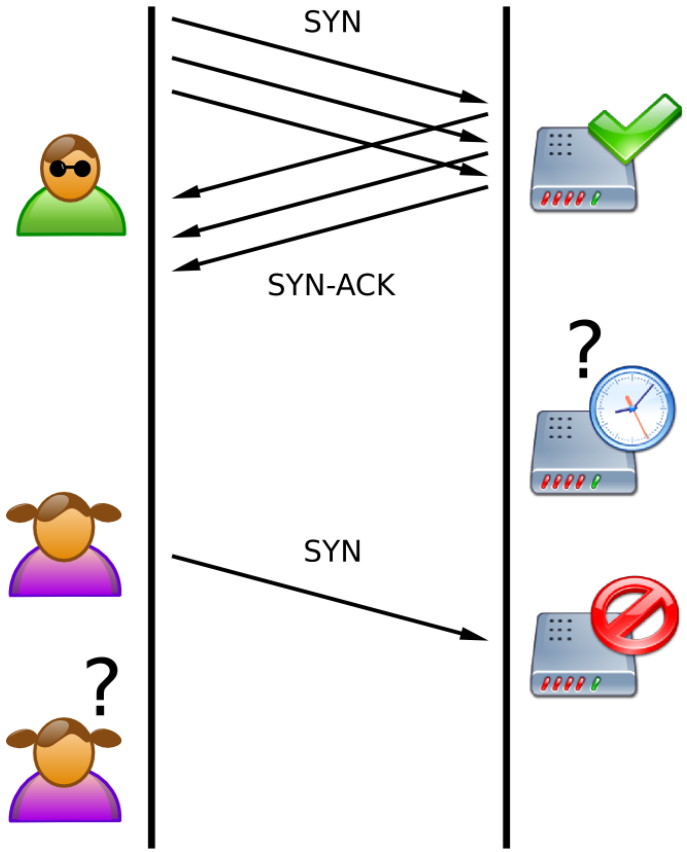
Ping of Death (for Historical Purposes)

- Ping size should be 64 bytes (84 with IP header).
- Send IP packets that exceed the maximum legal length (65535 bytes).
- One of the earliest denial of service attack.
- Unix, Linux, Mac, Windows, printers, and routers were vulnerable (< 1997).

SYN Flooding

- Upon reception of the SYN packet, the server allocates necessary memory for the connection and enters it in a queue of half open connections.
- This situation having not been foreseen, the server can no more accept new connections once the queue overflows.
- The attacker can forge the source address of his SYN packets to remain anonymous.
- Current versions of operating systems are protected against such attacks.

SYN Flooding



SYN Flooding: Protections

- Increase the size of the queue.
- Reduce timeout during which server is waiting for an ACK.
- Drop the oldest SYN in the queue.
- Filtering eg on IP addresses.
- SYN-Cache: cache the SYN and send a SYN/ACK. If the ACK arrives, a complete connection is created.

SYN Flooding: Protections

- SYN-Cookies: Once the connection queue is almost filled up, the server uses SYN cookies.
- Upon reception of a SYN:
  - The server sends a SYN/ACK containing a SYN cookie.
  - The server erases the SYN entry.
- Upon reception of a ACK:
  - The server checks whether it contains a valid cookie. If so this highly likely means that the client has already sent a SYN and is so a honest client.

SYN Flooding: SYN-Cookie Content

- SYN cookies are specific Initial Sequence Numbers.
  - t is a 5-bit counter incremented every 64 seconds modulo 32.
  - m is the Maximum Segment Size encoded on 3 bits.
  - s is the 24-bit result of a cryptographic function computed on t, the server IP address and port number, the client IP address and port number.

$$\text{ISN} = [t \mod 32] \,||\, m \,||\, s$$

SYN Flooding: SYN-Cookie Check

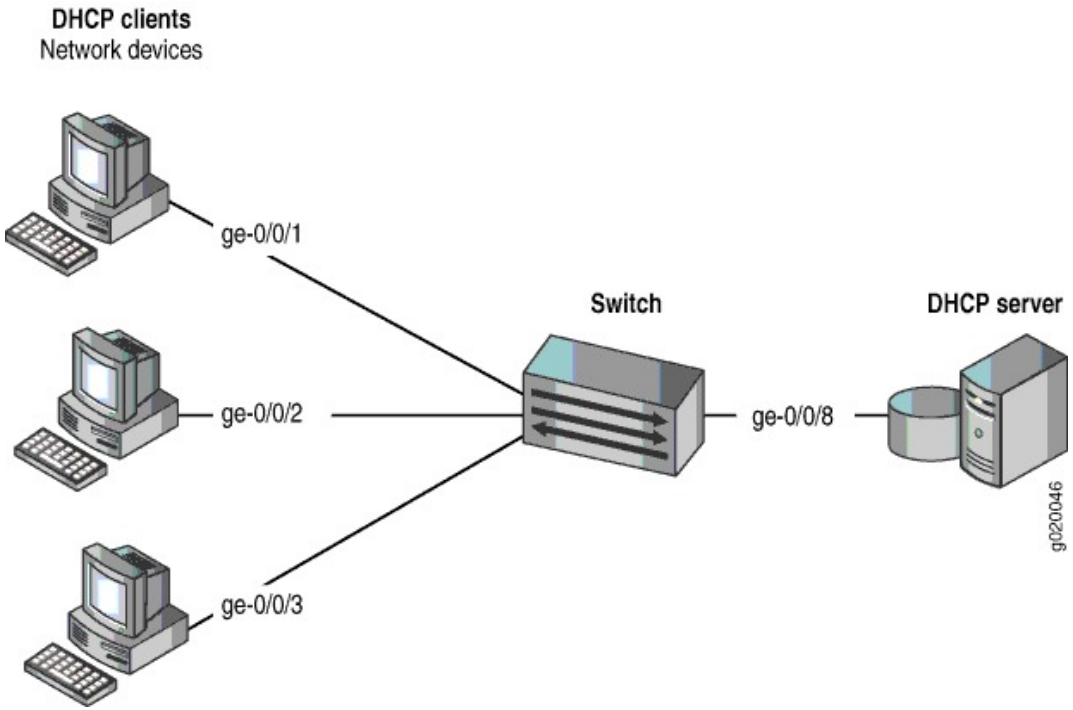
- Upon reception of an ACK, the server carries out the following operations.
  - Check that the received value t is valid with respect to the current time. Otherwise, this means the connection is expired.
  - Recompute s to check its validity.
  - Decodes the value m, which allows the server to reconstruct the SYN queue entry.

Kamikaze Packets (Xmas Tree Packets)

- TCP Packets with flags URG, PSH, and FIN.
- When many Kamizake packets are sent, an unexpected behavior of routers may occur.
- Certain routers may reboot.

DHCP Starvation

- The attacker floods a DHCP server with DHCP requests from spoofed (counterfeit) MAC addresses.
- The server's pool of IP addresses is exhausted.

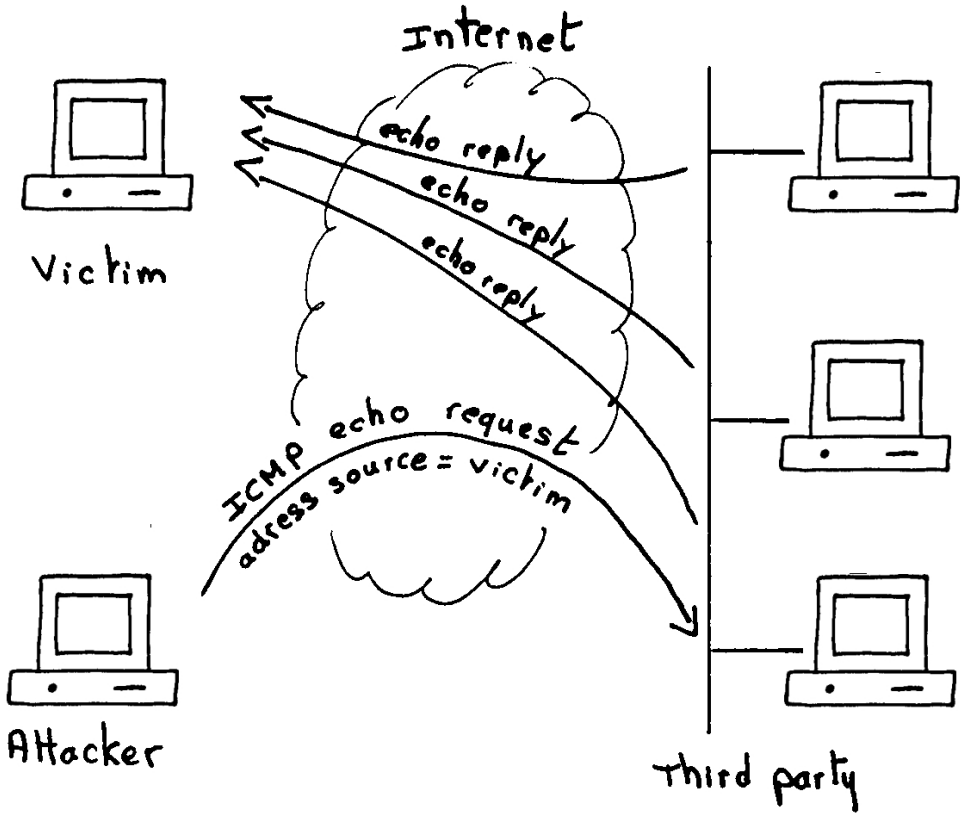


www.juniper.net

Smurf Attack

- Drown the target with the help of traffic amplifiers.
- Typical case: ICMP echo-request (ping).
- The hacker sends a ping packet with the target address as source address.
- The "pinged" machine sends its response to the target.
- If the hacker sends the packet to a broadcast address, all machines of the network will reply to the target.

Smurf Attack



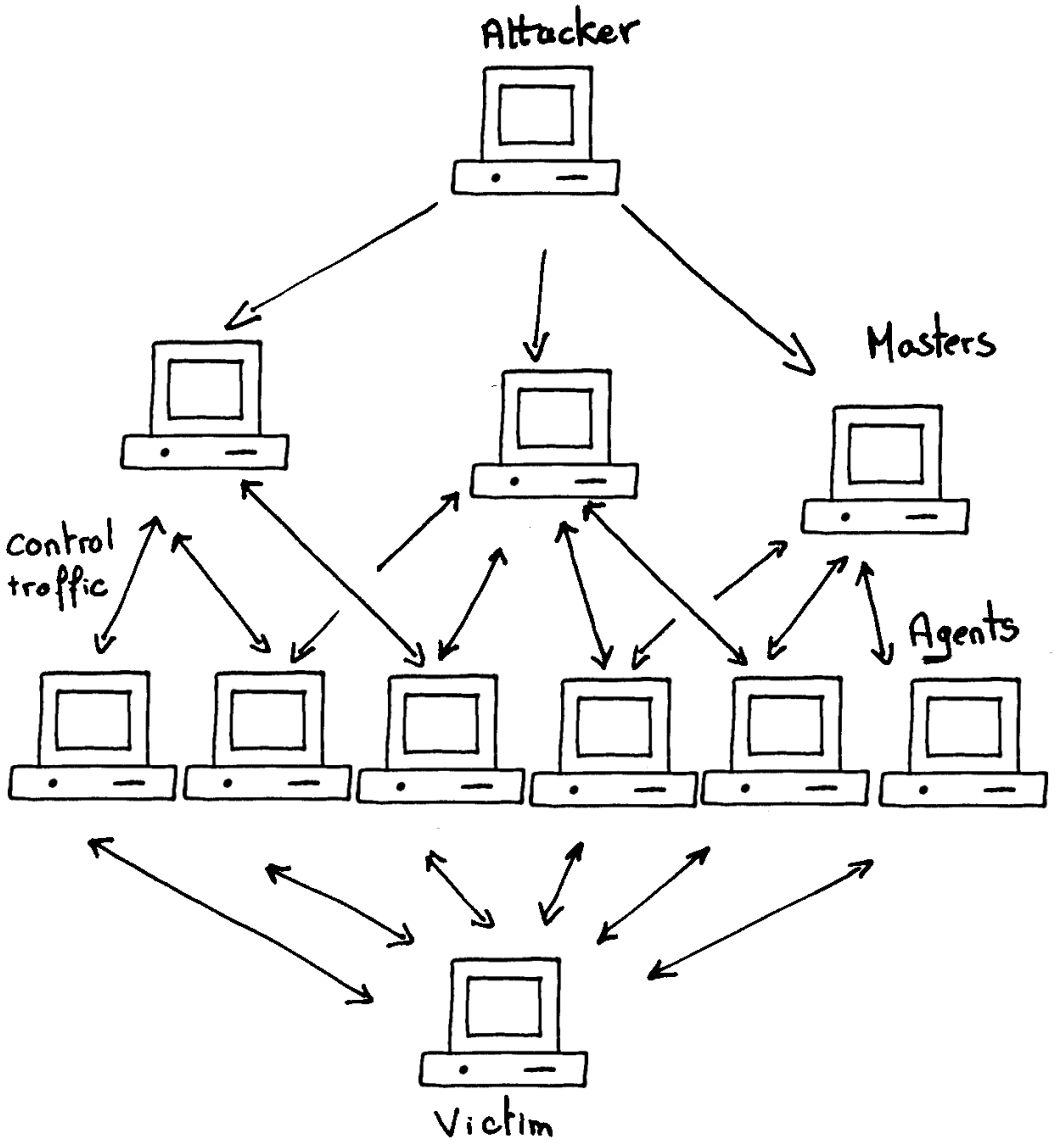
Smurf Attack: Protection

- Configure individual hosts and routers not to respond to ping requests to broadcast addresses.
- Configure routers not to forward packets directed to broadcast addresses.
- Magnifying the traffic can be done with applications where the replies are much bigger than the requests.

DDoS: Distributed Denial of Service

- To increase the efficiency of Denial of Service, hackers hack into several machines and install agents on them.
- Several master machines control the agents.
- The hacker sends commands to the masters which in turn execute the attack through the agents.

DDoS: Architecture



DDoS: Botnets

- Botnet: A network of hacked machines controlled by a hacker.
- The power (bandwidth) of the attack is multiplied by the agents/bots.
- Typically the bots connect to an Internet Relay Chat and wait for commands from their master.
- It is more difficult to trace the hackers (2 intermediate layers).
- Since attack comes from several sources, it is much more difficult to filter it.

DDoS: Renting Botnets

- Hackers rent botnets to spammers for as low as $350 per week for 5000 bots.
- In the press: 3 men arrested in the Netherlands in 2005; they managed a 1.5 million computer botnet.

DDoS: Historical Example

- February 7, 2000: The Internet portal of Yahoo was inaccessible for several hours.
- February 8, 2000: Amazon, Buy.com, eBay, and CNN were also victims of a DDoS attack, which significantly reduced their activities.
- February 9, 2000: E*Trade and ZDNet were both victim of a DDoS attack.

DDoS: Tools

- Trinoo.
- The Tribe Flood Network.
- Stacheldraht.
- Tribe Flood Network 2000 (tfn2k).
  - Agents (bots) do not answer to the masters.
  - Masters send 20 command packets.
  - Masters use ICMP, TCP, UDP.
  - Communication encrypted.
- Loic, eg used by Anonymous in Operation Chanology (against the scientology Church) in 2010. Particularity: People voluntarily install Loic on their computer to join the botnet.

SPOOFING

- Denial of Service
- Spoofing
- Hijacking
- Conclusion and References

IP Spoofing

- In certain cases, the IP source address is used to authorize a connection.
  - Routers and firewalls can filter packets according to their source.
  - Some programs (rlogin, rsh) can authorize certain sources to connect without authentication.
- It is easy to forge a packet's source address and to abuse the trust of that source.
- The reply to a forged message is sent to the forged address.
- Easy to use with protocols based on UDP.
- The applications to be hacked (typically rlogin, rsh, ...) use TCP.

DNS Spoofing (UDP)

- A user sends a DNS request to a local DNS server.
- An attacker sends a DNS response faster than the DNS server.
- DNS is mostly based on UDP.

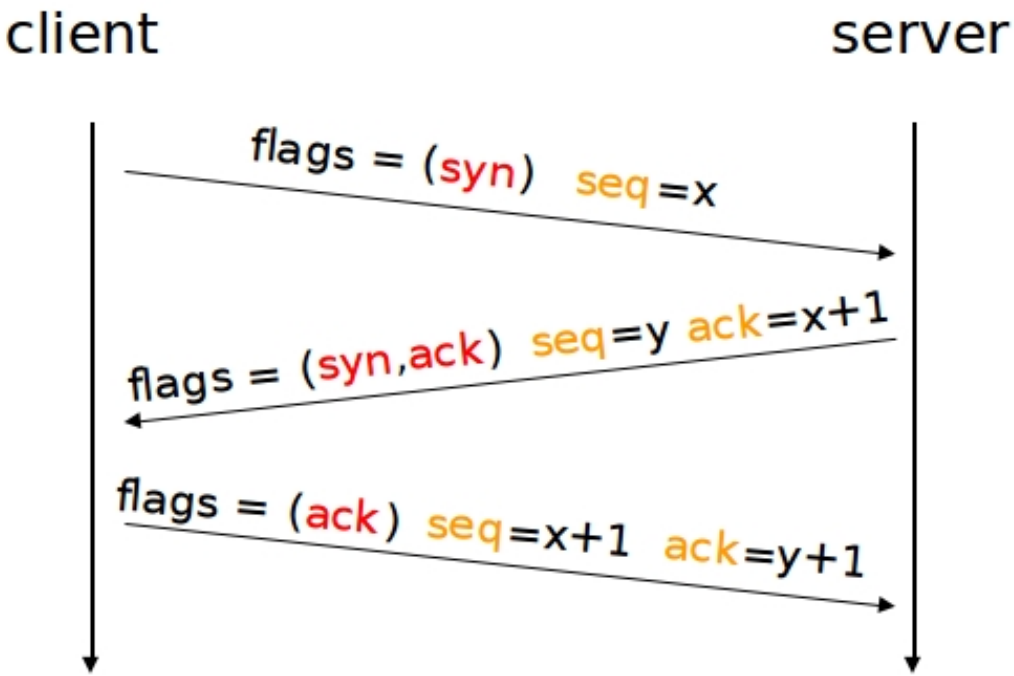
DNS Cache Poisoning (UDP)

- The attacker sends a DNS request to a local DNS server.
- The local DNS server queries a master DNS server.
- The attacker spoofs the master DNS server, providing the local DNS server with a fake DNS response.
- However: the local DNS server's query includes an identifier.
- The attacker must guest the identifier.
- The attacker floods the local DNS server with DNS responses.
- The attacker may send many DNS requests.

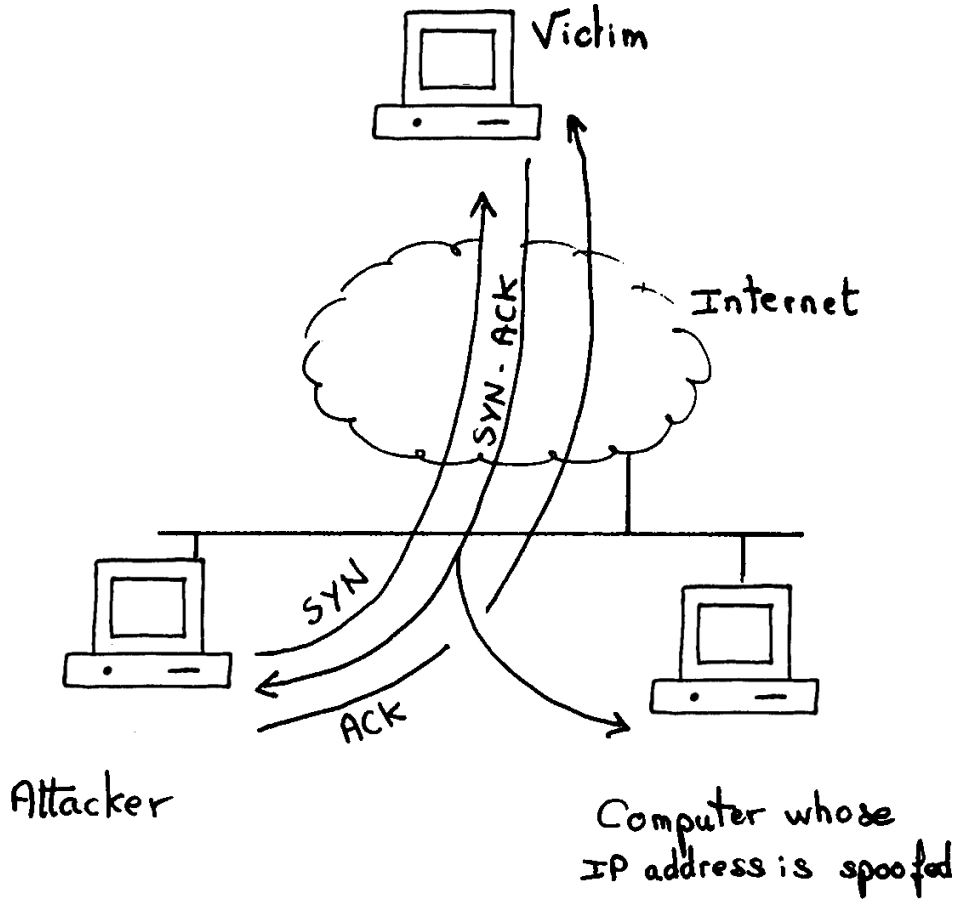
TCP/IP Spoofing

- TCP is a sliding window protocol, it uses sequence numbers to keep track of sent and received data.
- To avoid using the same sequence numbers, a random initial sequence number (ISN) is chosen for each new connection.

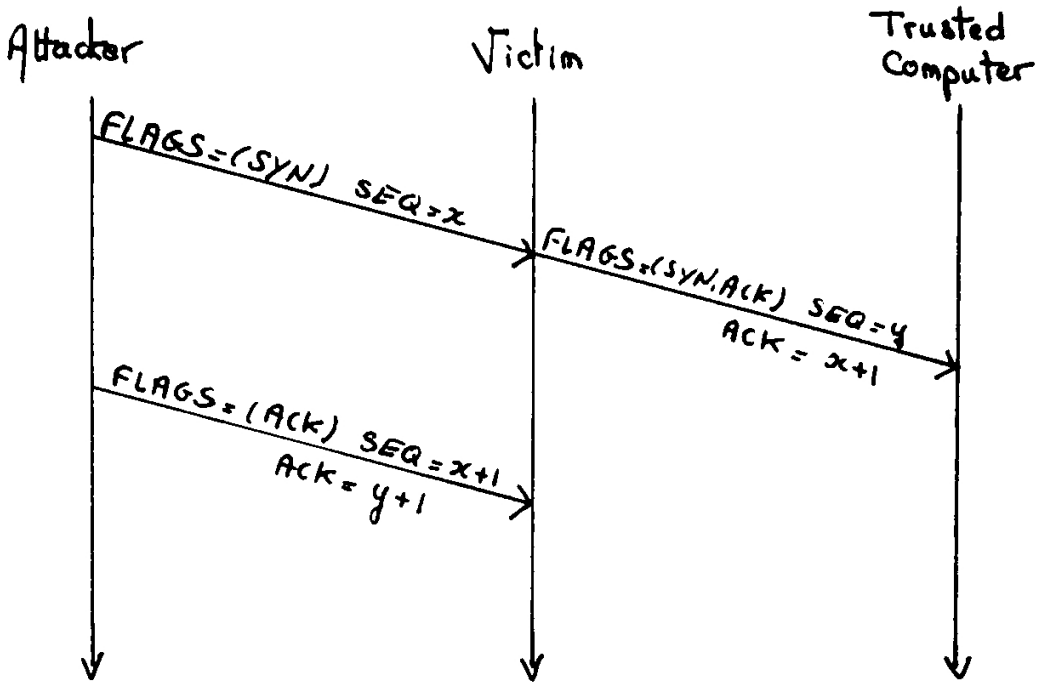
TCP/IP Spoofing: TCP Handshake



TCP/IP Spoofing Within a LAN



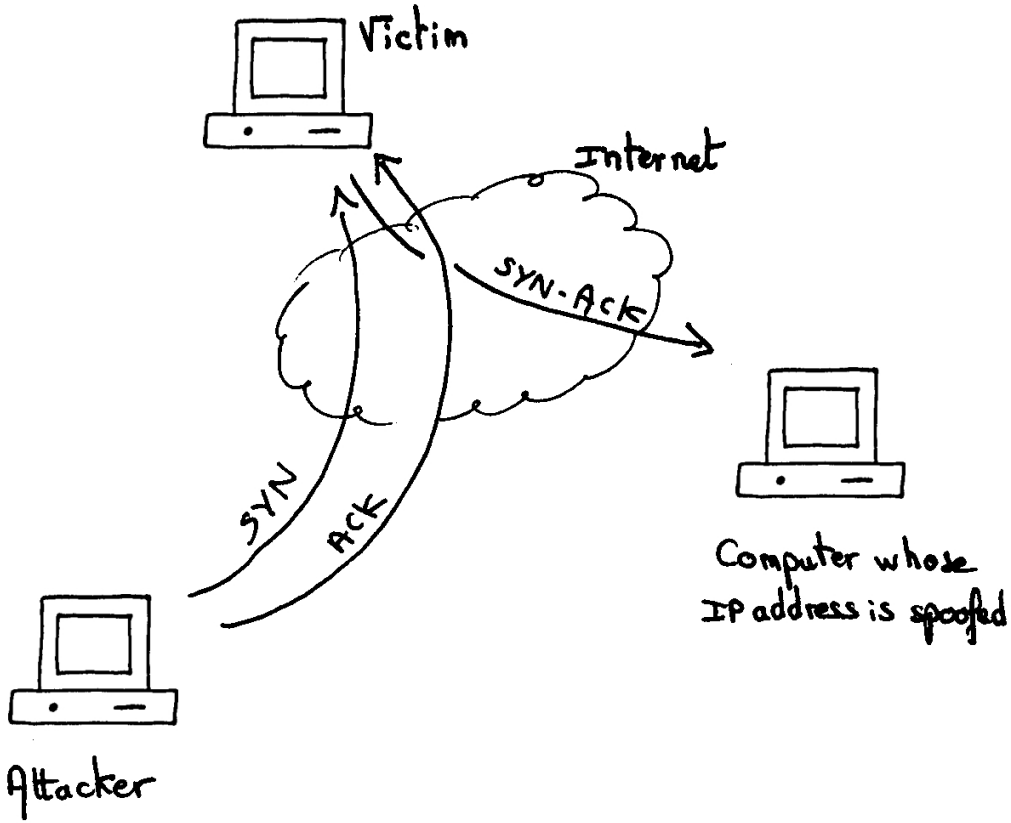
TCP/IP Spoofing Within a LAN



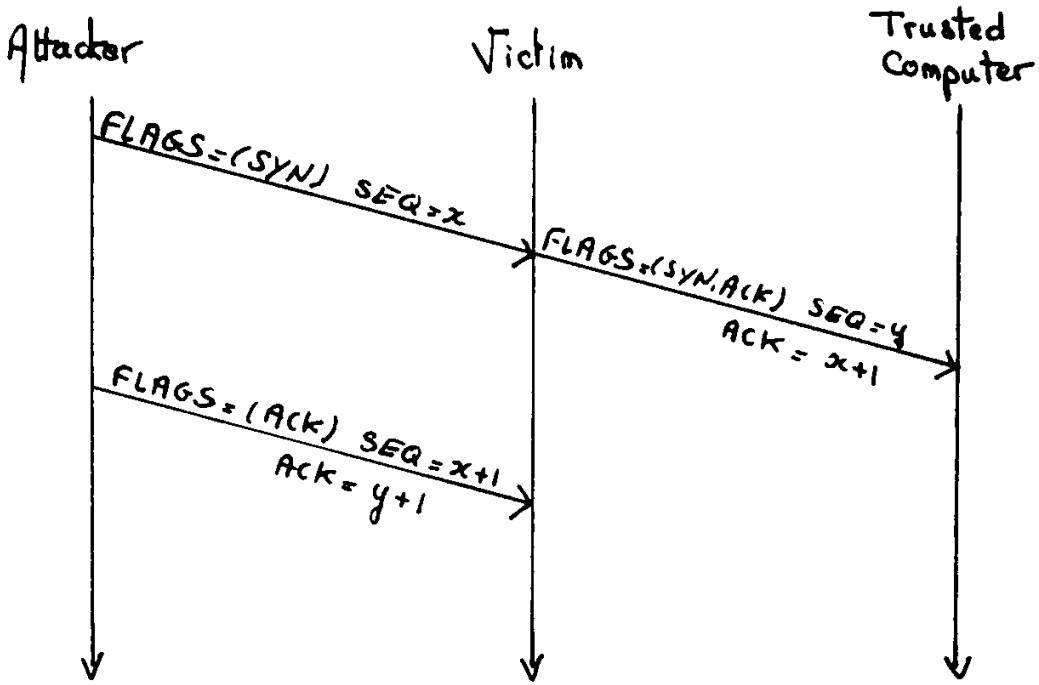
TCP/IP Spoofing Within a LAN

- The victim resets the handshake protocol.
- The hacker must prevent the victim from responding.

TCP/IP Spoofing From Outside



TCP/IP Spoofing From Outside

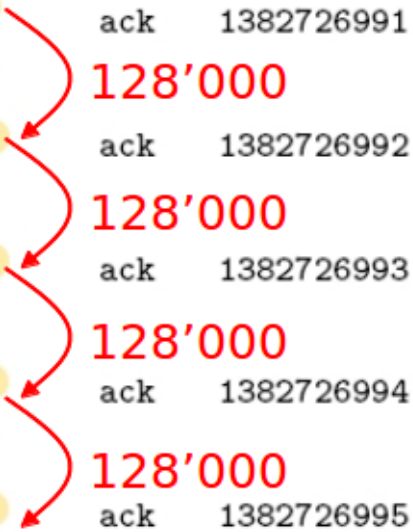


TCP/IP Spoofing From Outside: ISN Prediction

- The original standard (RFC 793) requires that the ISN be incremented once every four microseconds.
- In some simple TCP implementations the next ISN can be predicted.
- Hacker's procedure (ISN prediction):
  - He opens a few authentic connections (for example SMTP) to obtain the current ISN and increment samples.
  - He launches his forged connection using the last ISN plus an increment obtained from those samples.
  - He can launch multiple forged connections with different increments hoping that at least one is correct.

TCP/IP Spoofing From Outside: ISN Prediction

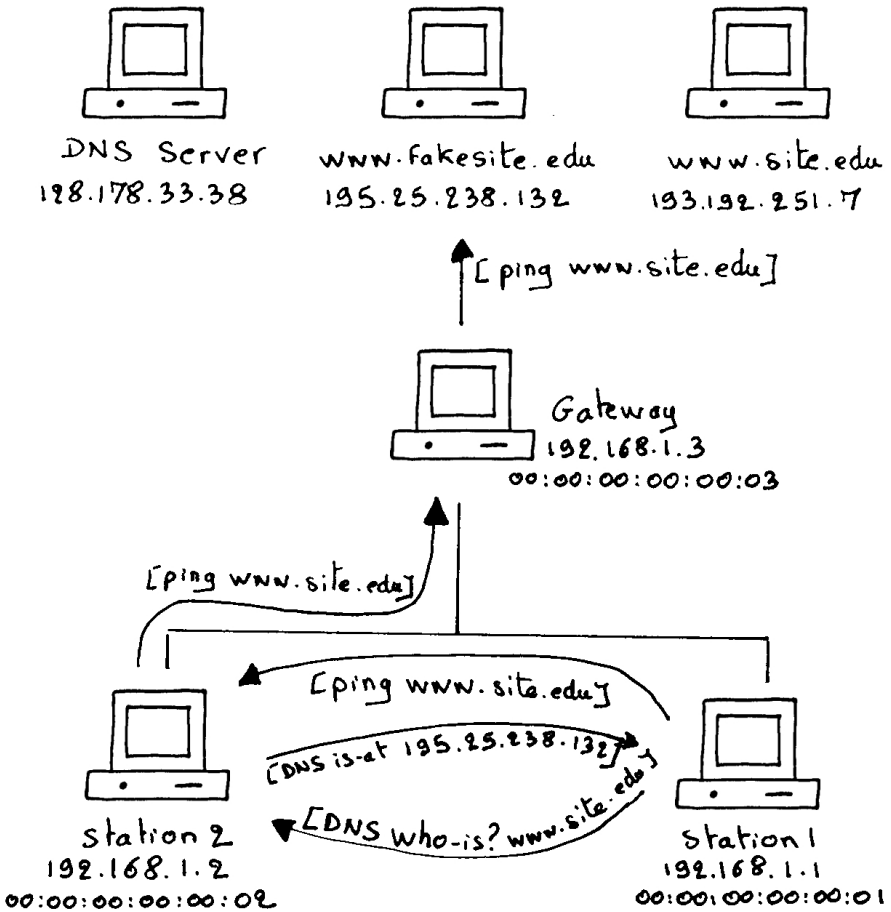
```
14:18:25.90   kevin.1000   >   bob.514:      S   1382726990
14:18:26.09   bob.514      >   kevin.1000:   S   2021824000   ack   1382726991
14:18:26.17   kevin.1000   >   bob.514:      R   1382726991
14:18:26.50   kevin.999    >   bob.514:      S   1382726991
14:18:26.69   bob.514      >   kevin.999:    S   2021952000   ack   1382726992
14:18:26.77   kevin.999    >   bob.514:      R   1382726992
14:18:27.01   kevin.998    >   bob.514:      S   1382726992
14:18:27.17   bob.514      >   kevin.998:    S   2022080000   ack   1382726993
14:18:27.25   kevin.998    >   bob.514:      R   1382726993
14:18:27.54   kevin.997    >   bob.514:      S   1382726993
14:18:27.71   bob.514      >   kevin.997:    S   2022208000   ack   1382726994
14:18:27.79   kevin.997    >   bob.514:      R   1382726994
14:18:28.05   kevin.996    >   bob.514:      S   1382726994
14:18:28.22   bob.514      >   kevin.996:    S   2022336000   ack   1382726995
14:18:28.30   kevin.996    >   bob.514:      R   1382726995
```



ARP Poisoning

- ARP: Address Resolution Protocol.
  - Protocol that helps finding a layer 2 (Ethernet) address from a layer 3 (IP) address.
- Very simple and insecure:
  - client: who knows the ethernet address of 10.1.2.3?
  - anybody: 10.1.2.3 has ethernet address 010203040506.
- It is easy to forge responses (even non-solicited) to redirect traffic.

ARP Poisoning



ARP Poisoning Countermeasures

- Dynamic ARP Inspection (analyze consistencies of ARP packets).
- DHCP Snooping (detect fake DHCP servers).

HIJACKING

- Denial of Service
- Spoofing
- Hijacking
- Conclusion and References

Session Hijacking

- Instead of stealing a password, the hacker can wait until a user authenticates himself and then steal his session.
- This technique can be applied to several layers, eg, modem, TCP, HTTP.

Session Hijacking: Modem Session

- The modem gives access to a serial line (for ex. remote access).
- A user may drop the line without quitting the online session.
- The terminal's session remains active for a while.
- The next user (or hacker) who connects to the modem finds the preceding user's session.

Session Hijacking: TCP Session

- If a hacker can spy on a TCP connection, he can insert a TCP packet with correct sequence numbers.
- Inserting an additional packet in a TCP connection creates a packet avalanche:
  - The source, who has never sent the packet, does not agree with the acknowledged sequence number and emits an acknowledgement.
  - The destination, who has seen the packet, insists on the sequence number and also sends an acknowledgement.

Session Hijacking: HTTP "Session"

- HTTP protocol is not session-oriented.
- It is made of independent requests/responses.
- E-commerce web-sites use artificial means to recognize requests belonging to a session: cookies or personalized URLs.
- If the hacker can spy on these data, he can create requests that would be part of the same session.

Session Hijacking

CONCLUSION AND REFERENCES

- Denial of Service
- Spoofing
- Hijacking
- Conclusion and References

Conclusion

- Most of the presented attacks are known for a long while.
- But they are still up to date.
- ARP Poisoning is an efficient attack.
- Countermeasures exist but they are (too) rarely deployed.

References

- SYN-cookies:
  http://cr.yp.to/syncookies.html
- Christmas Tree Attacks:
  https://www.youtube.com/watch?v=bVrxL2AL4yQ
- DNS spoofing:
  https://www.checkpoint.com/defense/advisories/public/dnsvideo/index.html
- TCP hijacking:
  http://www.cs.berkeley.edu/~daw/security/shimo-post.txt
- ARP poisoning:
  http://www.royabubakar.com/blog/2013/11/04/arp-poisoning-attack-and-mitigation-for-cisco-catalyst/