Network Security
Elements of Network Security Protocols

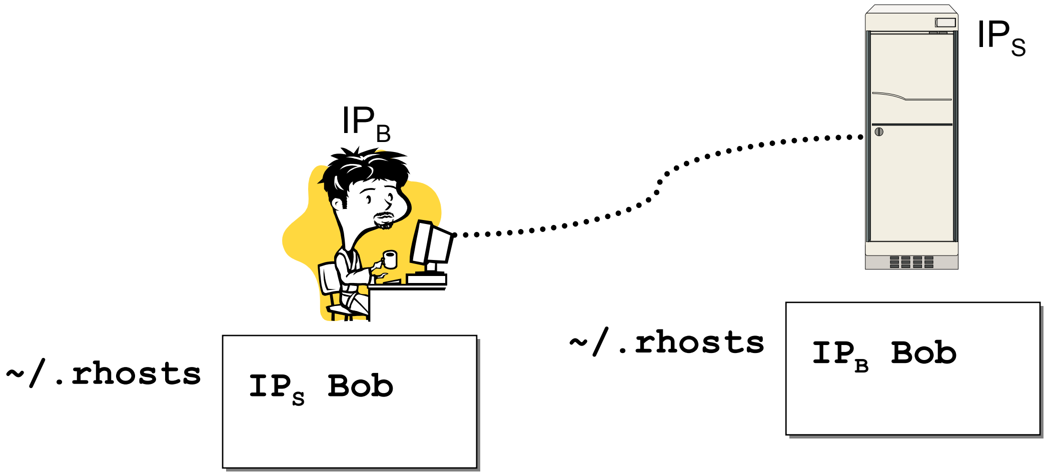
Spoofing of TCP

Overview

Problemi nella TCP/IP protocol suite:

- Autenticazione basata sull’indirizzo IP
- Meccanismi di controllo della rete (ad esempio, i protocolli di routing) fanno un uso molto limitato, o addirittura nessun uso, della autenticazione

Trust relationship in the Unix world



IP$_S$

IP$_B$

~/.rhosts

IP$_S$ Bob

~/.rhosts

IP$_B$ Bob

- Bob can use any of the r* commands without the annoying hassle of password authentication
- The r* commands allow address-based authentication

TCP 3-way handshake

Handshake for connection establishment

S: server (target host);
C: client (trusted host);
ISN: initial sequence number;

M1 C -> S: SYN(ISN$_C$)
M2 S -> C: SYN(ISN$_S$), ACK(ISN$_C$)
M3 C -> S: ACK(ISN$_S$)
trasmissione dati

☛sequence numbers allow TCP to implement data sequencing and acknowledging for communication reliability

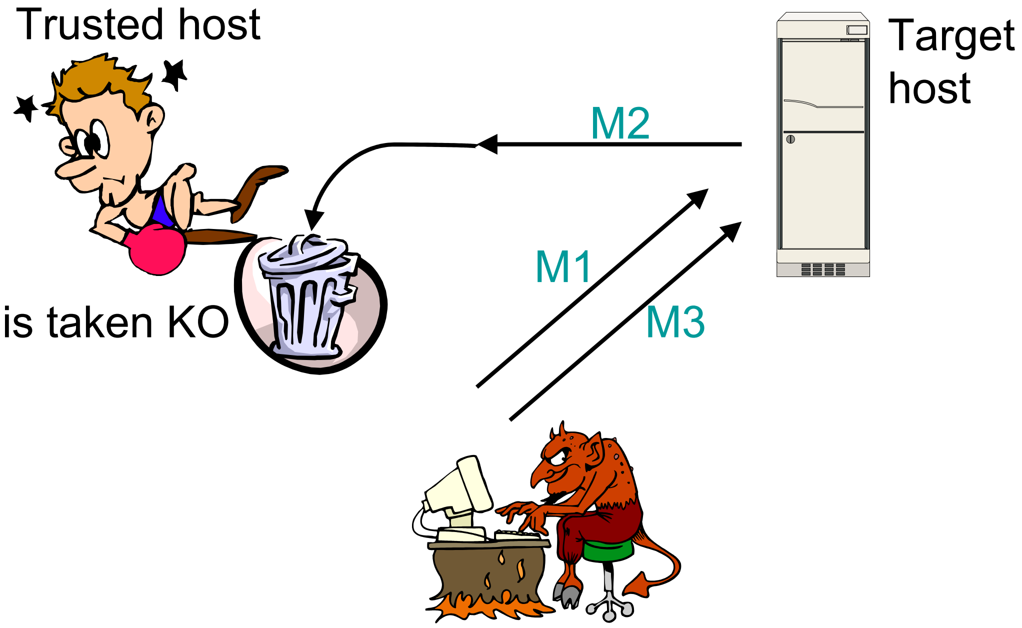
TCP spoofing: basic idea

If an adversary X is able to “guess” ISN$_S$, then he can impersonate the trusted host C

M1 X -> S: SYN(ISN$_X$), SRC = C
M2 S -> C: SYN(ISN$_S$), ACK(ISN$_X$)
M3 X -> S: ACK(ISN$_S$)
M4 X -> S: ACK(INS$_S$), *malicious payload*

X does not receive M2, but he is able to guess ISN$_S$ and thus generate M3

TCP spoofing: basic idea



Trusted host

is taken KO

M2

M1

M3

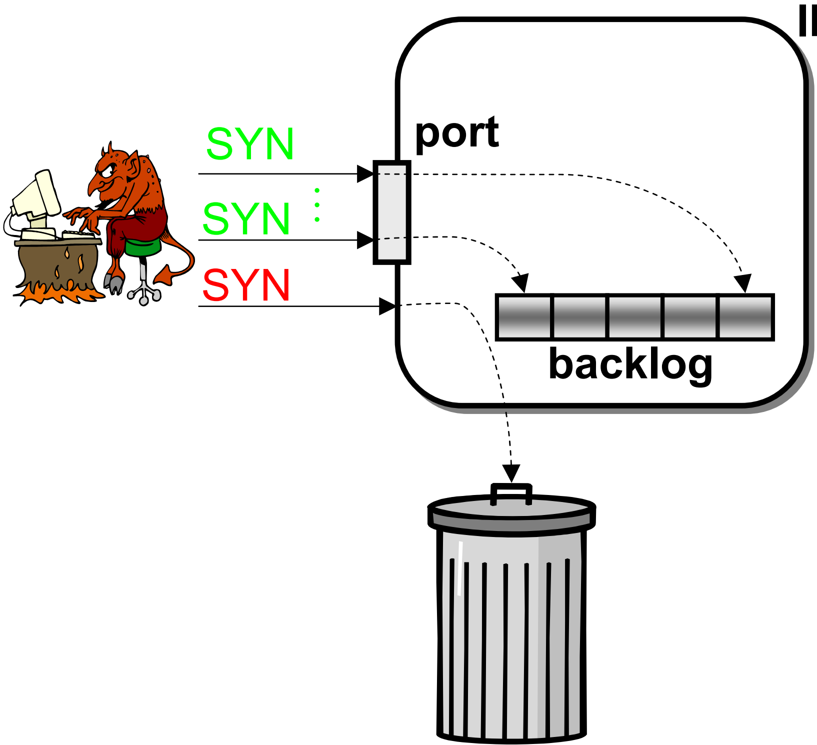
Target host

TCP spoofing: steps

The adversary does the following

- Choose the target host
- Discover a pattern of trust and a trusted host
- Disable the trusted host
- Impersonate the trusted host,
  sample sequence numbers,
  make connection attempt
- Leave a backdoor, if the attack succeeds

TCP SYN flooding

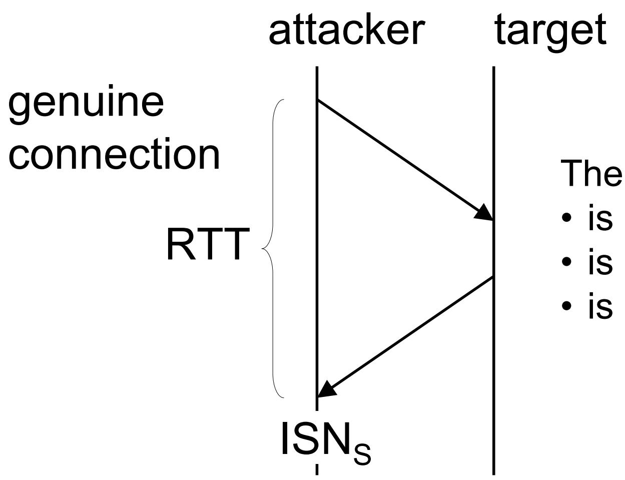


Backlog limits the number of concurrent SYN requests TCP can process for a given socket

	backlog
Unix	5
Linux	6

ISN sampling and prediction

RTT: Round Trip Time

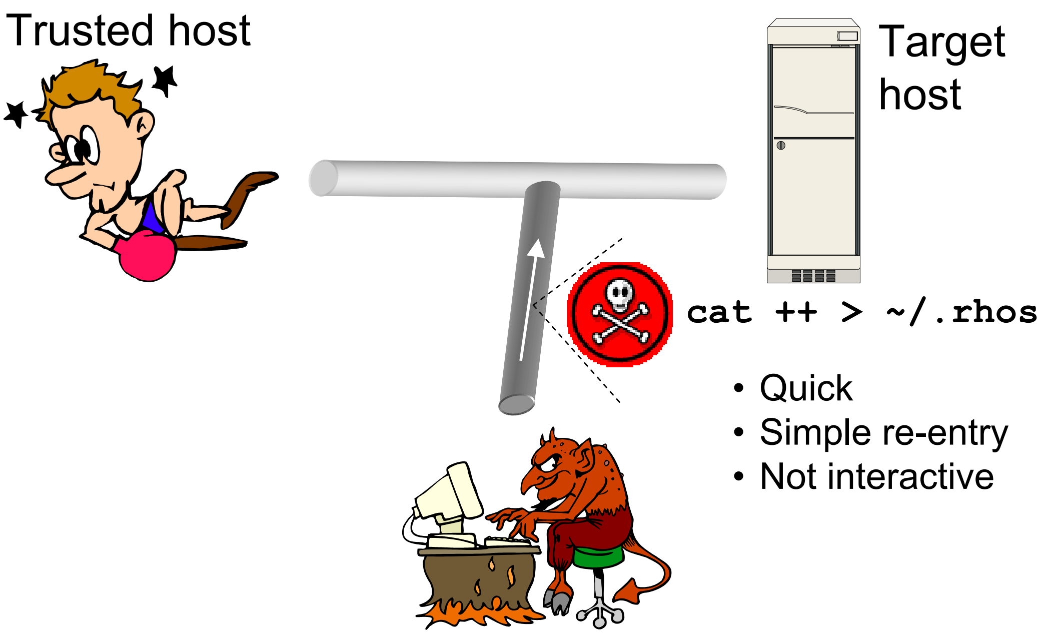


The ISN counter

- is initialized to 1
- is incremented by 128k every second
- is incremented by 64k at every connection

ISN_S and (an estimation of) RTT allow the attacker to estimate the next value for ISN_S to be used in the spoofing attack

How to insert a backdoor



```
cat ++ > ~/.rhosts
```

- Quick
- Simple re-entry
- Not interactive

Preventive measures (I)

- Be un-trusting and un-trustworthy
  - Disable all r* commands
  - Remove all .rhosts
  - Empty /etc/equiv (host wide trust relationships)
  - Force users to use other means of remote access, e.g. ssh
- Packet filtering
  - Impose trust relationships only among internal hosts: no internal host should trust and external host
  - Filter out all traffic from the outside that purports to come from the inside

Preventive measures (II)

- Cryptographic methods
  - Require all network traffic to be authenticated/encrypted
  - ISN Randomizing
    - Sequence numbers are chosen randomly and unpredictably
    - ISN = Clock + (upon every new connection)

      H(localhost,localport,remotehost,remoteport, s),

      where s is secret material