Vulnerability Class: Address Masquerading

L. Todd Heberlein

24 Jan 1996

Overview

- History
- Implementation
- Consequences

History

- Morris, 85
- Bellovin, 89
- UC Davis, Feb. 94
- UC Davis, Mar 94
- Mitnick-Tsutomu, Dec 94

History (cont.)

- UCD paper, spring 95
- Mendax, Rbone, summer 95
- Wee (UCD), fall 95
- AF project, Jan. 96

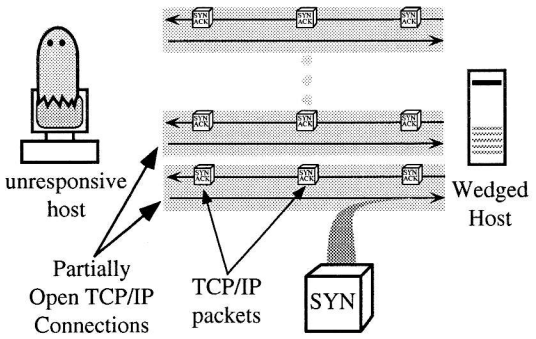
Implementation

- PP
- Replay
- Wedger
- Killer
- Injector

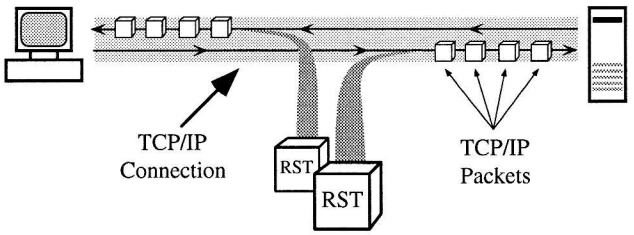
Packet Print (PP)

```
---------- TCP ----------
src port: 1018
dst port: 513
seq num:  956032001
ack num:  951104069
pkt_len:  20
ACK
window:   4096
checksum: 8127
p_urgent: 0
data len: 0
DATA:
---------- IP ----------
header_len: 5
version: 4
T.O.S.: 0
len: 40
ID: 5793
offset: 0
TTL: 60
protocol: 6
checksum: 62983
src: 128.120.56.222
dst: 128.120.56.89
---------- ETHERNET ----------
src: 8:0:20:1a:e3:9f
dst: 8:0:20:7:62:b3
type: IP
next proto len: 54
```

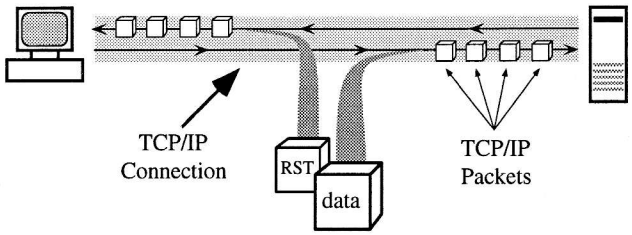
Wedger



Killer



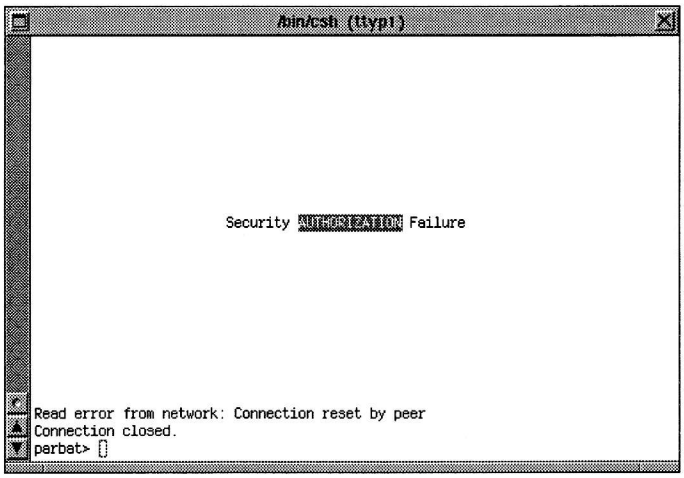
Injector



Injector: Intruder's View

```
/bin/csh (ttyp1)
root:PGLV5ourjlKIY:0:1:Operator:/:/bin/csh
nobody:*:65534:65534::/:
daemon:*:1:1::/:
sys:*:2:2::/:/bin/csh
bin:*:3:3::/bin:
uucp:*:4:8::/var/spool/uucppublic:
news:*:6:6::/var/spool/news:/bin/csh
ingres:*:7:7::/usr/ingres:/bin/csh
audit:Wshlc0274Qi5Y:9:9::/etc/security/audit:/bin/csh
allocate:*:20:0:allocate pseudo user::
AUftpd:*:21:10:AUftpd pseudo user::
AUrcmd:*:22:10:AUrcmd pseudo user::
AUrexecd:*:23:10:AUrexecd pseudo user::
AUrlogind:*:24:10:AUrlogind pseudo user::
AUtelnetd:*:25:10:AUtelnetd pseudo user::
AUsyslogd:*:26:10:AUsyslogd pseudo user::
AUpwdauthd:*:27:10:AUpwdauthd pseudo user::
AUyppasswdd:*:28:10:AUyppasswdd pseudo user::
sync::1:1::/:/bin/sync
sysdiag:*:0:1:Old System Diagnostic:/usr/diag/sysdiag:/usr/diag/sysdiag/sysdiag
sundiag:*:0:1:System Diagnostic:/usr/diag/sundiag:/usr/diag/sundiag/sundiag
+::0:0::
~
"/etc/passwd" [Read only] 22 lines, 849 characters
```

Injector: Intruder's View



Consequences

- Study network attacks
- Deny services
- Circumvent access control
- Obsoletes one-time authentication
- Forge replies

Study Network Attacks

- Capture traffic of new attack
- Run network server under debugger
- Replay attack in controlled fashion
- Study server's behavior

Deny Services

- Avoid active IDS
  - wedge security server
  - attack target system
  - leave before server awakens
- Kill intruder's session

Forge Replies

- NIS reply
  - What password do you want?
- DNS reply
  - What address/name do you need?
- NFS reply
  - Patch binaries on the fly.

Obsoletes One-Time Authentication

- One-time, up-front authentication
- Based on obsolete models
- One-time passwords obsolete