An Evening With Berferd

Bill Cheswick
AT&T Bell Laboratories

ches@research.att.com

Plan A - No connection

OUTSIDE INSIDE

Plan B - Dirty access machine

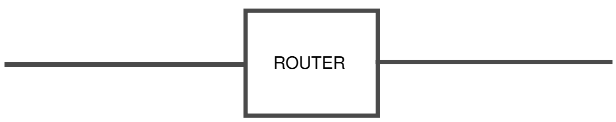
OUTSIDE INSIDE

Plan C - Application-level gateway

OUTSIDE INSIDE

Plan D - Packet filtering

OUTSIDE INSIDE



AT&T

Plan E - Wide open connection

OUTSIDE INSIDE

AT&T

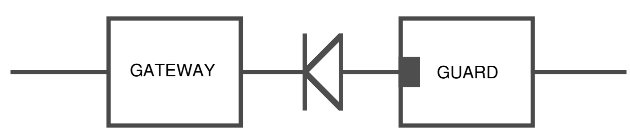
Our gateway goals

- Provide most services to insiders
- Provide necessary services to outsiders
- Secure even if gate is fully compromised
- Reasonable performance and maintainability

AT&T

Our Plan

OUTSIDE INSIDE



AT&T

The Gateway machine

(Hopefully) secure, but we limit trust:

- minimum network services
- no regular users
- few accounts
- fewer passwords
- backed up regularly
- off-machine logging (drop safe)
- instrumented, weakened daemons
- important files checksummed regularly
- regular scans for SUID ROOT programs
- extensive logging
- large, separate partitions for logs, public FTP, spool directories
- SMTP only - no uucp, no dialers, no Systems files
- unnecessary programs removed
- sources stored on a safe(r) machine

AT&T

Authentication

RISC/os (inet)

login: guard
RISC/os (UMIPS) 4.0 inet
Copyright 1986, MIPS Computer Systems
All Rights Reserved

Authentication Server.

Id? debra
Enter response code for 70202: 04432234

Destination? mercury/grumpy
OKYou have mail.
$

AT&T

Traps

- Guest/visitor accounts
- FTP passwd file with clues
- SMTP DEBUG command
- rlogin/rsh detection
- finger
- Many new ones - portmapper, tftp, bootp, nfs, etc.

AT&T

Attack rates

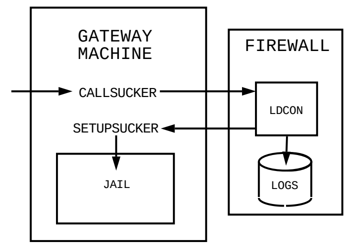
- 40 Guest logins/month
- 12 FTP passwd accesses/month
- 1 SMTP DEBUG per year

AT&T

Why bother?

- Shut down insecure machines and accounts.
- Learn their techniques.
- Trace them down, if lucky.
- Torturing a bad guy is fun.
- Provide a logging base?

The jail



Chronology

• 15 Jan	first DEBUG attempt
• 20 Jan	Evening with Berferd
• 4 Feb	"Jail" first installed
• mid Feb	first trace completed
• Feb - Apr	Occasional pokes
• 21 Apr	NY Times article
• late Apr	Hackers learn Stanford is bugged
• 1 May	Berferd adopts research.att.com
• 3 May	Management pulls the plug
• since	Occasional pokes?
• winter 92	Berferd is arrested

Legal/ethical questions

- Is a site liable for 'sponsoring' a hacker?
- Is a site liable for not preventing a hacker?
- Is a logged hacking base a good idea?

Conclusions

- Given any account on a machine, a hacker has a GOOD CHANCE of spreading to other machines and becoming root.
- Our gateway is probed daily.
- It is nearly impossible to locate a cautious, experienced cracker.
- Thorough logging is Good.

AT&T

Availability

- Either an AT&T product or
- General Release
- You can build the logging and many traps yourself

AT&T