Texas A&M Network Security Tools

Presenter:

Dr. Dave Safford, Director
Computing and Informations Systems
Texas A&M University

Credits:

David K. Hess
Douglas Lee Schales

Abstract

- Problem
- Approaches
  - Overview
  - Monitor (netlog)
  - Host Check (tiger)
  - Filter (Drawbridge)
- Resources
- References
- Questions

- Postscript copy of this presentation available from net.tamu.edu:pub/security/TAMU/nasa_oh.ps, along with original USENIX article tamu-security-overview.ps

Problem:

- internet hacker underground
- typical unix workstation misconfigured.
- sniffing (weakest link)

- => unprotected sites are at grave risk
- If you don't protect yourself, you will be broken into.

- Examples:
  - TAMU breakins August 92
  - UT breakins
  - Rice breakins

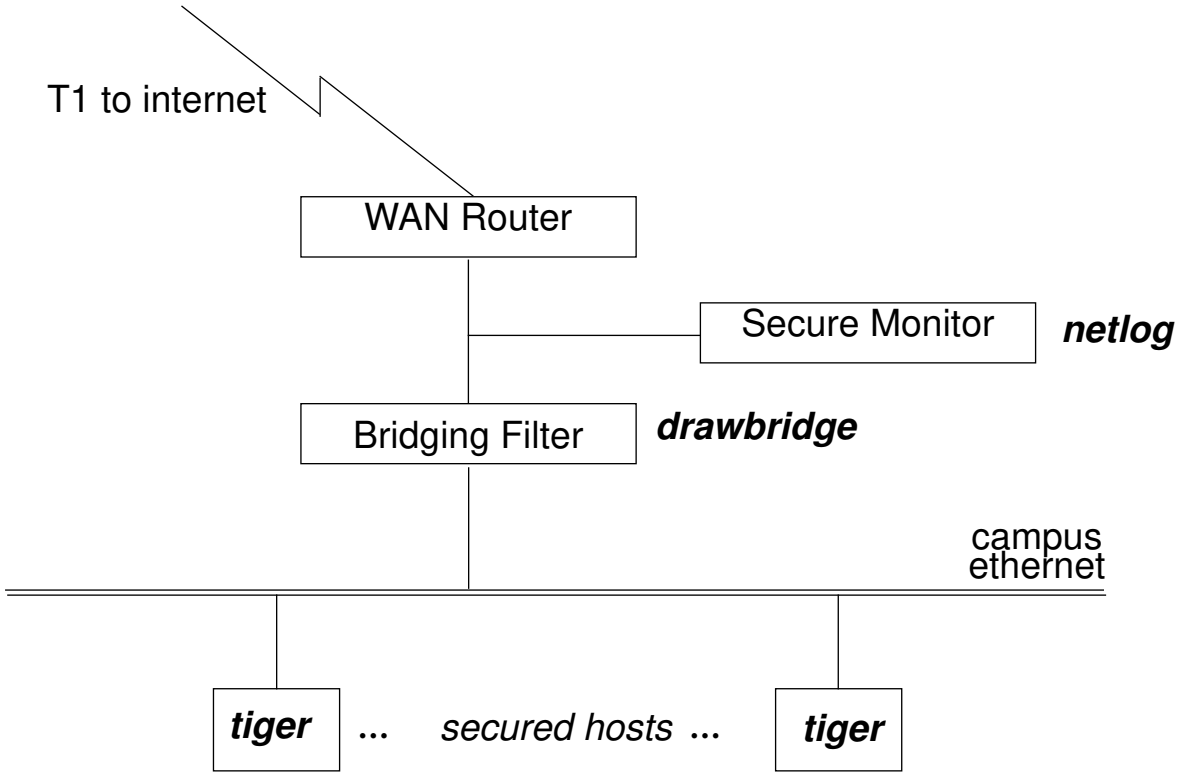
Texas A&M Network Security Tools

Approaches:

- Firewalls
- Network Monitors
- Host Checks

- Passworded Dial-ups
- “Secure” twisted pair ethernet hubs
  (we use 3-COM FMS-2 stackable)
- Backups

Overview of Components



Network Monitors:

- TAMU's netlog:
  - tcplog
  - udplog
  - netwatch - intrusion detection
    - telnet, ftp, rlogin, rshell, smtp, tftp, sunrpc, FSP

Netwatch Example Output

```
09/16/93 01:29:43.63 [rpc] x.y.4537 HOST.TAMU.EDU RPC
                lookup for: ypserv

09/16/93 01:36:23.80 [rpc] x.y.4565 SUN.TAMU.EDU RPC
                lookup for: ypserv

09/19/93 11:24:13.89 [ftp] a.b.1025 PLANET.TAMU.EDU
                'anonymous' (u@a.b) unknown cmd:
                cat ANNOUNCE

09/19/93 14:41:38.11 [rpc] SUN.TAMU.EDU.4552 r.m.com RPC
                lookup for: rexd

09/20/93 22:52:48.70 [telnet] d.e.1090 VMS.TAMU.EDU
                attempted login as 'field'

09/20/93 22:52:48.77 [telnet] d.e.1090 VMS.TAMU.EDU
                failed login as 'field'
```

Host Checks:

- TAMU's tiger scripts
  - easy to use, with detailed messages and explanations
  - security configuration auditing
  - security patch verification
  - intrusion detection

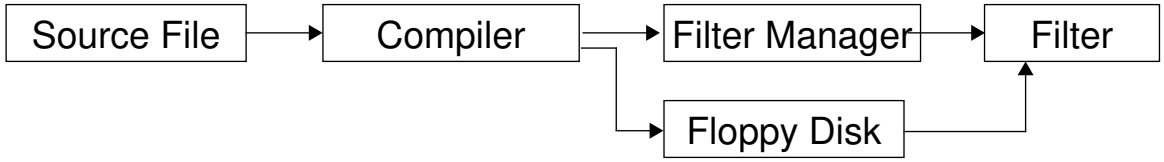
Overview of Checks

- login accounts
- anonymous FTP
- NFS exports
- inetd configuration
- .netrc files
- PATH setting
- file permissions
- digital signatures
- embedded pathnames
- e-mail aliases
- cron files
- group file(s)
- known break-in signs
- passwd file(s)
- printcap file(s)
- .rhosts files
- file system scan

Firewalls:

- None
  - easy, but you'll regret it
- Simple router filters (r'cmds, yp, nfs, tftp, X)
  - low cost, easy to implement, fairly invisible
  - only fair security improvement
- Powerful filters (Firewall-1, drawbridge)
  - medium cost, low visibility, medium security
- "true" proxy firewalls
  - high cost, high visibility, high security
- air-gap
  - total security, poor functionality

Drawbridge Compilation and Loading



Filter Language Constructs

```
host (<hostname>|<ip_address>) <list of service_entries>

network (<ip_address>|<ip_address> - <ip_address>)
        <netmask> <list of service_entries>

define <group_name> <list of service_entries>

allow <ip_address> <netmask> <list of service_entries>

reject <ip_address> <netmask>
```

Service Entry Grammar

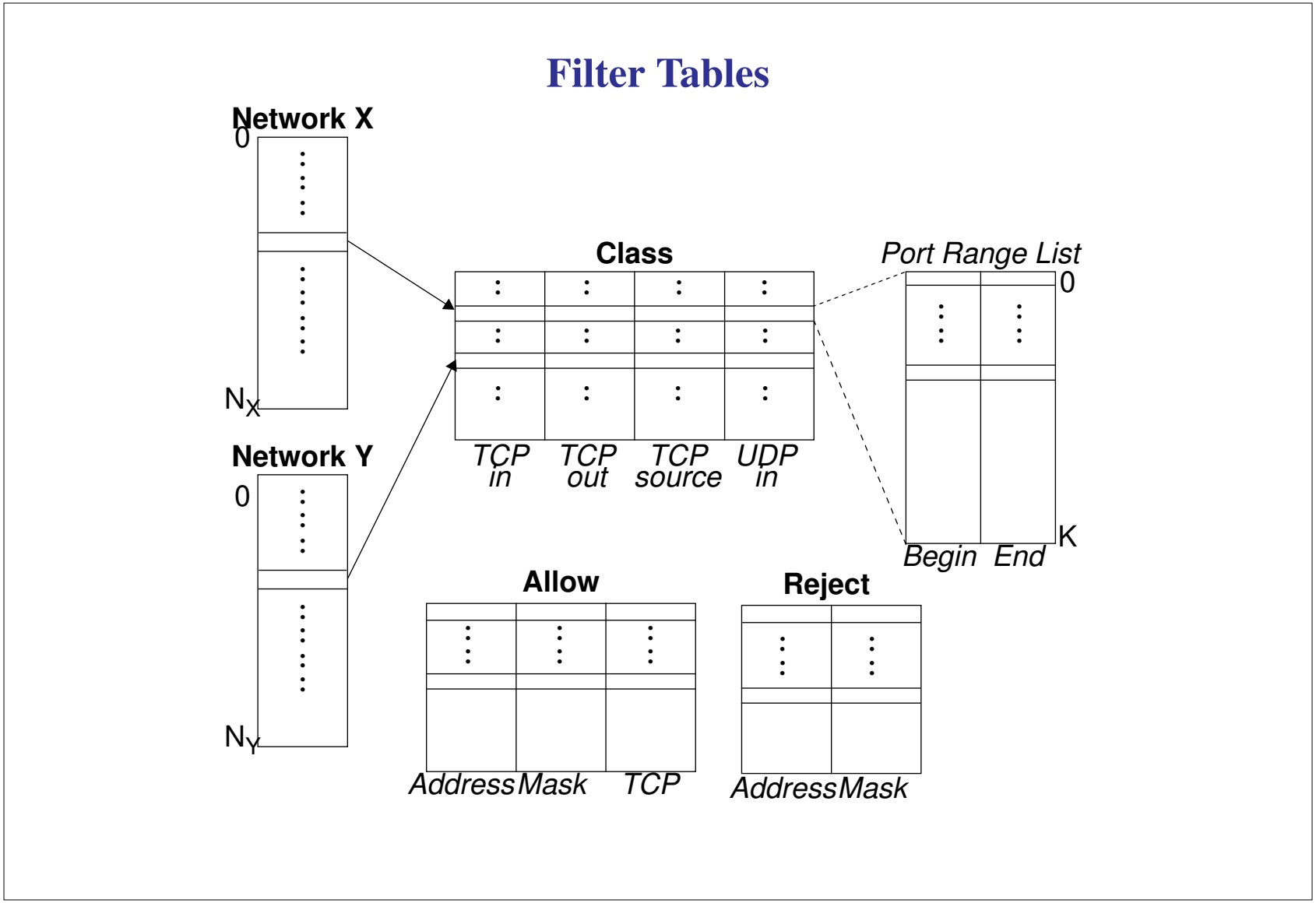
```
<service_entry>   ::=  < (src=|dst=) <service_desc>
                         (in|out|inout) > |
                       <!(src=|dst=) <service_desc>
                         (in|out|inout) > |
                       < group_name>

<service_desc>    ::= <service> | <service_range>

<service>         ::= <port_number>                  |
                      <port_number>  / <protocol>   |
                      <service_name>                |
                      <service_name> / <protocol>

<service_range>   ::=  <port_number> - <port_number> |
                       <port_number> - <port_number> /
                       <protocol>
<protocol>        ::= <protocol_number> |
<protocol_name>
```

Example Configuration File

```
# Defaults for any machine not listed in this file.
define default  <1-65535/udp in>, <!tftp/udp in>,
                <!sunrpc/udp in>, <!2049/udp in>,
                <1-65535 out>, <src=ftp-data in>,
                <smtp in>, <auth in>, <gopher in>;

# Admin requested no access in/out for this subnet
network 123.45.58.0 255.255.255.0 <!1-65535 in-out>;

# NNTP host and CSO phonebook server
host mailnews.tamu.edu    default, <nntp in>, <time in>,
                          <csnet-ns in>, <domain in>,
                          <finger in>;

# Machine (PC) which uses tftp to do document transfers
host sender.tamu.edu      <1-65535/udp in>;

# Has to have X
host arrow.tamu.edu       default, <ftp in>, <6000 in>;

# No TCP access in/out
host bee.tamu.edu         <!1-65535 in-out>;
```

Filter tables

- Network tables
- Class table
- Allow table
- Reject table


Filter Tables
Network X
0
N_X
Network Y
0
N_Y
Class
TCP in
TCP out
TCP source
UDP in
Port Range List
0
K
Begin
End
Allow
Address
Mask
TCP
Reject
Address
Mask

Drawbridge 2.0 Goals

- High speed support (T3 - 45 Mbit/sec)
- Hardware independence (wider card support)
- Media independence (ethernet, fddi, ...)
- Routable/portable management
- Better memory management

Drawbridge 2.0 Implementation

- Ethernet and FDDI support
- IP (UDP) stack for management
- Uses DOS NDIS 2.01 drivers
- Network tables in cached extended (XMS) memory
- Statistics reporting over IP
- Pseudo-one-time-pad encryption
- MIT style copyright (rather than GNU)

Drawbridge 2.0 Requirements

- >= 386 processor
- >= 2 MByte memory
- DOS 2.01 NDIS drivers
  - must support 2 NICs
  - must support promiscuous mode
  - must support native media frames

Drawbridge 2.0 Tested Configurations

- Ethernet
  - 33 Mhz 486
  - DOS 5.0
  - ISA bus SMC elite 16 ethernet card
- FDDI
  - 60 Mhz pentium
  - DOS 5.0
  - EISA bus Network Peripherals FDDI card
  - (3-COM Fddilink does NOT work)

Drawbridge 2.0 Results

- Sustained Ethernet (486 ISA) improved from 2 to 5 Mbit
- Sustained FDDI (60 Mhz pentium) greater than 18 Mbit
- Full media bandwidth should be possible with:
  - faster cards (SMC ultra, Etherlink 3)
  - faster buses (PCI)
  - faster cpu (90 Mhz pentium)

Resources:

- Organizations:
  - CERT
  - FBI
- Mailing Lists: (send "subscribe" in body to majordomo@)
  - Firewalls@greatcircle.com
  - Academic-firewalls@net.tamu.edu
- Newsgroups:
  - comp.security.announce (CERT)
  - comp.security.unix
  - alt.security

Resources:

- Major FTP sites:
  - ftp.cert.org
  - coast.cs.purdue.edu
  - net.tamu.edu

Vendors:

- Sun - igateway, firewall-1
- DEC - SEAL
- ANS - Interlock
- TIS - Gauntlet

- Checkpoint Technology - Firewall-1

Free Tools:
(available from coast.cs.purdue.edu:/pub/tools)

- tcpwrapper
- TIS-toolkit (coast.cs.purdue.edu:/pub/mirrors/ftp.tis.com)
- socks
- TAMU
  - drawbridge
  - tiger
  - netlog/netwatch
- cops
- tripwire
- crack

Publications:

- Rik Farrow, "Barbarians at the Walls", Open Computing, Oct, 1994 pp 62-65.
- Dan Farmer, "Improving the Security of your Site by Breaking into it", (coast.cs.purdue.edu:/pub/doc/firewalls admin_guide_to_cracking)
- Safford, Schales, Hess, "The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment", Proceedings Fourth USENIX Security Symposium, Oct 1993, pp. 91-118. (Also available via ftp from net.tamu.edu:pub/security/TAMU/tamu-security-overview.ps.gz)
- Cheswick, "The Design of a Secure Internet Gateway", coast.cs.purdue.edu:/pub/doc/firewalls/ Bill_Cheswick_secure_gateway

Reference Books

- Cheswick and Bellovin, Firewalls and Internet Security, Addison-Wesley, 1994 (ISBN 0-201-63357-4)
- Garfinkel and Spafford, Practical UNIX Security, O'Reilly & Associates, 1991 (ISBN 0-937175-72-2