Case Study # 2

The FISH Network Audit

With Data Taken from Real Life

title.fig

Case study - the Fish network

- About the Fish network
- Audit tools and procedures
- Major risks
- Major problems

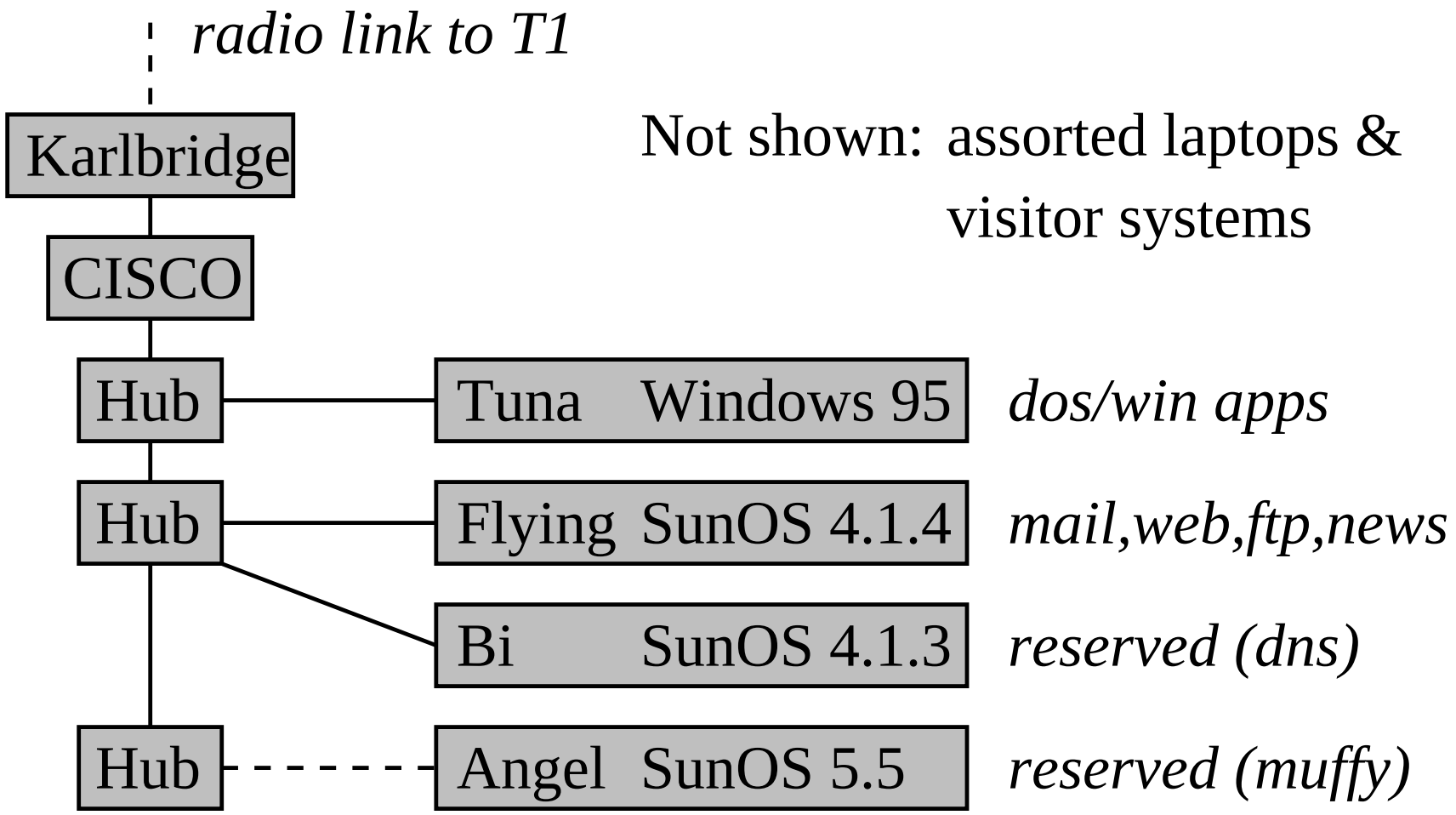
overview.fig

About the Fish network

- Home base of Dan and Muffy
- Dozens of mailing lists
- Web/FTP site
- Watering hole for friends of fish
- Why security

about.fig

Fish network topology



drawing.fig

General nature of Fish network

Use the network but don’t trust it

- No firewalling
- No packet filtering
- No secure hubs
- Encrypted radio link

network.fig

General nature of Fish systems

Focus on host/network security:

- No trusted hosts (NFS, rsh, rlogin)
- No unnecessary accounts (ingres, uucp, sync)
- No unnecessary network services (RPC, echo, chargen)
- No unnecessary network clients (tcp wrapper)
- No reusauble passwords over remote networks (S/Key)

systems.fig

Strong dependency on host/network security

Keeping an unfirewalled site secure:

- Competent system administration
- Consistent system configuration
- Active system monitoring
- Limited number of systems
- Limited number of users (is 35 limited?)

small.fig

Audit tools and procedures

- Remote access via 3-DES tunnel (STEL)
- Full access to configurations and other details
- Manual samples of processes, configs, etc.
- Automated scan with Tiger (security, checksums)
- PGP encryption for data transport

procedure.fig

Manual samples

- Processes (ps)
- Network services (lsof)
- Configuration/other files (motd!)
- Accounts
- System startup scripts

Automated scans

TIGER scan in all-out mode (40+ MB of output)

- File/directory protections/ownerships
- Configuration of common services/processes
- Pathnames embedded in commands, cron jobs, etc.
- Checksum comparison with distribution/patch media
- Non-standard set-uid programs

automated.fig

Accounts - system access and authentication

Source: /etc/{passwd,skeykeys,skey.access,hosts.allow,ttytab}

- Accounts removed or blocked (non-executable shell)
- Privileged (root) logins only on local terminals
- Remote logins only from specific sites (hosts.allow)
- S/Key password mandatory for remote access
- Pre-printed S/Key password sheets

accounts.fig

Fish small print...

```
SunOS Release 4.1.4 (FLYING-FISH+MC+4.1.4) #2: Wed Aug 2 21:06:10 PDT 1995
Attention!  User policy!  Look in /fish/policy for the full text...
-- dan & Muffy
```

- Conditions of use
- Availability of systems
- Feedback and contact information
- User’s rights and privacy
- Owner’s rights

Changes/additions to system software

Source: Tiger 2.2.3 using extended OS descriptions

- Kernel object modules (multicast)
- Network daemons/login (sendmail, S/Key)
- Privileged commands (majordomo, lsof, top)
- Security etc. patches (version!!)

checksum.fig

Embedded pathname analysis

Source: Tiger 2.2.3 embedded pathname scan

Problem in WWW statistics cron job:

- Executes with root privileges
- Writes to file in user-owned directory
- Impact: user can symlink to any file on the system

Fix: Run cron job at proper privilege level

Overview of network services

- Dangerous services limited (NIS)
- Dangerous services disabled (NFS, r-commands, RPC)
- Unnecessary services disabled (echo, chargen, rstatd)
- Unnecessary remote access disabled (tcp wrapper)
- Public services: DNS, SMTP, WWW, anon FTP
- SMTP listener enabled only on mailhost

services.fig

NIS - limited service

Source: ypwhich, ypwhich -m, rpcinfo -p

- One NIS domain per host
- NIS maps restricted to naming service (not users)
- Systems run KEYSERV (secure RPC), not used

Anonymous FTP

Preventing abuse of anonymous upload facility

- Incoming directory (drwx-wx-wx owner root)
  Anon users can’t see other anon user’s files
- Logdaemon FTPD switches umask to 0277
  Anon users can’t read other anon user’s files
- Logdaemon FTPD disables remote chmod

ftp.fig

World-wide web

Source: Netsite config files, cgi-bin directory

- Server runs as nobody; not chrooted
- Server executes CGI scripts

Problem:

- CGI scripts run /usr/ucb/mail (~! shell escapes)
- Exploit via newlines (%0A) in query arguments

Fix: Send message directly into ‘/usr/lib/sendmail -t’ (yuck)

Usenet news

Source: NEWSLIB/innshellvars, nnadmin C, tiger 2.2.3 suid

- INN 1.4 news server, runs as user news
- Unofficial patch for /usr/ucb/mail ~! shell escapes (official patch misses hole in parsecontrol script)
- NNTP client access restricted to specific sites
- NNMASTER daemon should not run as root
- NEWS2MAIL should not be set-uid at all

Majordomo

Source: majordomo scripts and lists database

- Over 20 mailing lists
- Not vulnerable to shell matacharacters in recipients (uses ‘/usr/lib/sendmail -t’ consistently)

Problem:

- World-writable mailing list include files
- Any user can break into the majordomo account, replace the set-uid majordomo wrapper program and trick sendmail to run command as ‘daemon’

majordomo.fig

Sendmail

Source: strings -a, tiger 2.2.3 checksums

- No known vulnerabilities in 8.7.4.1 SMTP listener
- SMTP listener only on mailhost

Problem:

- Old vulnerable sendmail binaries still have set-uid and execute permissions enabled
- Bugs can be exploited with ‘sendmail -bs’

The dangers of legacy systems

The name server host (no users) is falling behind

- Vulnerable sendmail client (8.7.1 Alpha)
- Logdaemon vulnerability (VB:95-04)
- World-writable utmp vulnerability (CA-94:06)
- Set-uid mount/umount commands

Fix: Upgrade software or take system out of operation

Major problem categories

Remote:

- Execute arbitrary commands as unprivileged user

Local:

- Execute arbitrary commands as semi-privileged user
- Execute arbitrary commands as fully-privileged user

Structural:

- Legacy system is falling behind with security patches

categories.fig

Major risks

- Vulnerable visitor systems can help intruders to work around security policy:
  - Remote access restrictions
  - One-time password requirement
- Hiding systems by bogus default route does not protect them against routing/spoofing attacks
- No firewalling means no redundancy.
  Every mistake can be fatal

risks.fig