


invent

# Securing Tru64 UNIX®

## DECUS Symposium Bonn 2004

Speaker name: Reinhold Danner  
Title: Customer Support Consultant,  
HP



© 2004 Hewlett-Packard Development Company, L.P.  
The information contained herein is subject to change without notice



invent

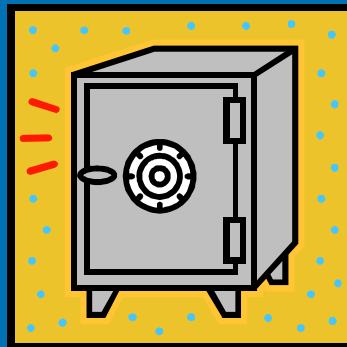
## Overview

- How Much Security is Enough?
- Secure Installation - Methodology and Practice
- Locking Down the Configuration
  - Daemons
  - Network Parameters
  - Files
- Vulnerability Testing
- Monitoring

Copyright © 2004 HP corporate presentation. All rights reserved.

2

## How Secure is Secure enough



## How Secure is Secure Enough?



- Always a tradeoff –
  - Security and Ease of Use
  - Security and Ease of Management
  - Security and Performance
- Need to consider the expected threat model
  - Random hackers? Industrial espionage? Disgruntled employees? Vendors? Partners?
- Need to consider the system function
  - Application server? Firewall? General Purpose?
- Need to consider the value of data stored on system
  - Which information assets are critical?
  - Cost of loss \* risk of loss
- Need to understand legal requirements
  - HIPAA, DOE or DOD sites
  - May specify database encryption, auditing, etc.



## Security Policies and Standards

- Corporate policies and standards are your best friend
  - Policies contain class-level security requirements
  - Standards are system-or-procedural specific
- Without security policies, you may have no legal recourse after a break-in
- Without security policies, you may be liable to prosecution
  - FTC vs Guess, Eli Lilly, Microsoft
- Without security policies, security decisions must be made by your system administrators without guidance or support
- Your organization may already have a standard defining a hardened configuration in its DMZ or Server security policy
- SANS Institute is excellent policy resource  
[www.sans.org/newlook/resources/policies/policies.htm](http://www.sans.org/newlook/resources/policies/policies.htm)

Copyright © 2004 HP corporate presentation. All rights reserved.

5




## Key Security Policies

- Acceptable Use policy
- Account and Password controls
- Configuration control
- Patch policy
- Vulnerability assessment policy
- Audit log and backup storage
- Incident response policies for a variety of scenarios
  - DoS attacks, root penetration, user account penetration
- Threat monitoring
  - Bugtraq, CERT, SANS, Tru64 UNIX Managers list

Copyright © 2004 HP corporate presentation. All rights reserved.

6

# Secure Installation



Copyright © 2004 HP corporate presentation. All rights reserved.

7

## Secure Installation Methodology

- Private net or removed from net completely
- Install OS
  - Custom installation to install minimal subsets required
- Install all patches
- Install applications and tools
- Lock down the system
- Repeat until satisfied:
  - Perform vulnerability analysis
  - Fix vulnerabilities
  - Be sure it reboots and didn't break anything

Copyright © 2004 HP corporate presentation. All rights reserved.

8



## Secure Installation

- Checksum software configuration
- Backup system
- Store checksums and backups in safe place(s)
- Secure the hardware
  - locked room
  - password for firmware
  - secure console mode
  - lock the panel, remove the key

Copyright © 2004 HP corporate presentation. All rights reserved.

9



## Tru64 UNIX® Secure Installation Specifics

- Include enhanced security subsets
- Include audit subset and build audit into the kernel
- Do not include kdebug in kernel
- Design a custom file system setup
  - world-writable directories like /tmp on private partitions
  - /usr readonly
- Install latest aggregate patch kit
- Install any additional SSRT patches

<http://h30097.www3.hp.com/unix/security-download.html>

Copyright © 2004 HP corporate presentation. All rights reserved.


10



# Lock Down the Configuration



Copyright © 2004 HP corporate presentation. All rights reserved. 11



## System Lockdown Overview

- Configure enhanced security
  - Establish user account defaults
- Install helpful tools
- Adjust network parameters
- Disable selected network services
- Prevent startup of unwanted daemons
- Examine configuration files
- Configure auditing

Copyright © 2004 HP corporate presentation. All rights reserved. 12



## Enhanced Security Configuration

- Establishes authentication defaults for all users
  - password expiration and lifetimes, triviality checks, better encryption, and more
- Sysman seconfig
  - Choose Enhanced Security, custom security profile
  - Take defaults for breakin detection
  - Choose Execute bit set only by root
  - Enable ACLs if needed
- Examine and adjust default account template
- Adjust root account – lower maxtries

Copyright © 2004 HP corporate presentation. All rights reserved.

13



## Free Helpful Tools

- From 5.1B Open Source Software Collection CD  
<http://h30097.www3.hp.com/demos/oss/html/0Wecome.htm>
- lsof
  - lsof -i displays open ports and associated commands/pids/accounts
- tcp\_wrappers - net services control
- tcpdump - network packet-level display
- ethereal - network protocol analyzer
  - 4.0D and 5.1 versions available at [www.ethereal.com](http://www.ethereal.com)

Copyright © 2004 HP corporate presentation. All rights reserved.

14



## Cheap Helpfull Tools

- From Internet Express CD
- <http://h30097.www3.hp.com/internet/osis.htm>
- Tripwire evaluation kit
  - Complete configuration process by running a Tripwire checksum of your system
- FireScreen (simple firewall based on screend)
- DoS prevention tool

Copyright © 2004 HP corporate presentation. All rights reserved.

15



## More Free Tools for 5.1A

From [www.tru64unix.compaq.com/unix/security-download.html](http://www.tru64unix.compaq.com/unix/security-download.html)

- SSH Webkit for 5.1A (Ships as part of 5.1B)
  - use instead of telnet, ftp, rlogin, rcmd, rexec, rsh
- IPSec (requires CDSA)

Copyright © 2004 HP corporate presentation. All rights reserved.

16





## Network Parameters

For denial of service attack prevention/reaction:

- `sysconfig -q socket`
  - increase `somaxconn`
  - set `sominconn` equal to `somaxconn`
- `sysconfig -q inet`
  - if under attack, set `tcp_keepinit` to 30 to drop connections fast
  - dynamic
- Randomized sequence numbers (RFC 1948) fully supported

Copyright © 2004 HP corporate presentation. All rights reserved.

17



## Network Services - `/etc/inetd.conf` `/etc/inetd.conf.local`

- Currently disabled by default
  - `uucpd`
  - `fingerd`
  - `tftpd`
  - `talkd`
  - `bootpd`
  - `inetd` internal services, `tcp` and `udp` versions
    - `daytime`, `echo`, `discard`, `chargen`
  - `RPC` `rstatd`, `rusersd`, `sprayd`, `walld`

Copyright © 2004 HP corporate presentation. All rights reserved.

18

## Network Services - /etc/inetd.conf /etc/inetd.conf.local



- Definitely also disable
  - comsat - biff email notification
  - ntalkd - talk server
  - time internal service
  - kdebugd - remote kernel debugger
  - rquotad - quotas for remote file systems

Copyright © 2004 HP corporate presentation. All rights reserved.

19

## Network Services - /etc/inetd.conf /etc/inetd.conf.local



- If you use SSH, you can also disable
  - rshd, rlogind
  - rexecd
  - ftpd
  - telnetd
- Ships with OS in Tru64 UNIX V5.1B
- Free SSH webkit for V5.1A at  
<http://tru64unix.compaq.com/unix/ssh/>

Copyright © 2004 HP corporate presentation. All rights reserved.

20

## Network Services - /etc/inetd.conf /etc/inetd.conf.local



- If not a mailserver, disable
  - pop3
  - imapd
- If not in a cluster, disable
  - cfgmgr
    - works with sysconfig -h
    - at least check /etc/cfgmgr.auth
- If you don't manage your system with Sysman browser or Sysman PC application, disable
  - suitjd - Sysman suitlet java daemon

Copyright © 2004 HP corporate presentation. All rights reserved.

21

## Network Services - /etc/inetd.conf /etc/inetd.conf.local



- If you don't manage LSM by gui, disable
  - initlmsad - LSM storage admin
- If you removed X or don't use CDE, disable
  - dtspc, CDE subprocess control
  - rpc.ttdbserverd, RPC-based tooltalk db server
  - rpc.cmsd, calendar manager

Copyright © 2004 HP corporate presentation. All rights reserved.

22



## Disabling Daemons

- Can disable some through rcmgr
  - insightd
    - rcmgr set INSIGHTD\_CONF NO
- For others, move unwanted scripts to /sbin/init.d/dont\_start\_these\_daemons/
  - snmpd (and all the MIBs)
  - smsd - Sysman Station
  - smauthd - Sysman authentication
  - lpd - line printer daemon
  - advfsd - AdvFS GUI
- Return scripts to original location when applying future patch kits

Copyright © 2004 HP corporate presentation. All rights reserved.

23



## Disabling Daemons (cont)

- Do NOT remove evmd (event monitor)
  - If not in cluster, prevent evm connections by setting “remote\_connection false” in /etc/evmdaemon.conf
- Do not remove esmd (essential services monitor)
- Do not remove caad (cluster application availability)
- Can disable inetd completely if:
  - you use SSH
  - you are not in a cluster
  - you don't need the other services

Copyright © 2004 HP corporate presentation. All rights reserved.

24



## Disabling Daemons (cont)

- Sendmail options:
  - Disable sendmail daemon startup (recommended)
    - Daemon mode only accepts inbound connects and manages stalled mail queue. Mailx can send outbound mail without the daemon.
    - Use cron hourly entry instead to process stalled outbound mail  
`0 * * * * /usr/sbin/sendmail -q`
  - Restrict to send-only
  - Set `/var/adm/sendmail/sendmail.conf` to reject mail connections from remote hosts

Copyright © 2004 HP corporate presentation. All rights reserved.

25



## Configuration Tightening

- Don't use NIS if you can possibly avoid it
- Grant sysadmin access to utilities through division of privilege (dop) or sudo
- If you don't disable snmp completely, at least disable default public community read access to your system in `/etc/snmpd.conf`
- Prevent remote access to syslog and binlog
- `touch /etc/syslog.auth` (owner root, 0600)
- `touch /etc/binlog.auth`

Copyright © 2004 HP corporate presentation. All rights reserved.

26



## Configuration Tightening (cont)

- Disable localhost source address on physical interfaces
  - in `/etc/ifaccess.conf`  
`ee0 127.0.0.1 255.255.255.255 deny`
  - enable filtering dynamically  
`ifconfig ee0 filter`
  - and add filtering to `/etc/rc.config`  
`rcmgr set IFCONFIG_0 nn.nnn.nn.nn netmask 255.255.255.0 filter`
- Limit crontab and at command use to root only
- `echo "root" > /usr/lib/cron/cron.allow`
- `echo "root" > /usr/lib/cron/at.allow`

Copyright © 2004 HP corporate presentation. All rights reserved.

27



## Configuration Tightening (cont)

- Require root password in single-user mode  
`#rcmgr set SECURE_CONSOLE YES`
- Set root's PATH and default umask
- Prevent network processes from creating core files
  - `ulimit -c 0` in `/sbin/init.d/inetd`
- Check protection of configuration files in `/etc`
  - does world really need read access?
- Verify `/etc/ftpusers` and `/etc/securettys`

Copyright © 2004 HP corporate presentation. All rights reserved.

28



## File System

- Use separate partitions for world-writable directories like /tmp
  - Hard links can't cross file systems
- Mount readonly wherever possible
- Mount `-o nosuid` wherever possible
  - only need suid where your legitimate setuid binaries reside
- Unless /, mount `-o nodev`
  - no access to block and character-special devices

Copyright © 2004 HP corporate presentation. All rights reserved.

29



## File Protections

- Periodically verify that all world-writable directories have sticky bit set
  - `find / -type d -perm -02`
  - If sticky bit (1000) not set on directory, any user can delete files regardless of file ownership and permissions
- Locate setuid and setgid programs
  - `find / \( -perm -4000 -o -perm -2000 \) -type f`
  - Periodically rerun and compare
  - If truly paranoid, remove set\_id bits and selectively add back
  - login and su may be all you really need

Copyright © 2004 HP corporate presentation. All rights reserved.

30



## Sysconfig Tunables

### Buffer overflow exploit protection NEW in 5.1B PK2

- **executable\_data** – Heap and Data area protection
  - prevents the execution of instructions that reside in heap or other data areas of process memory
    - recommended setting (5) affects privileged processes only
    - /usr/sbin/javaexecutedata before setting (exempts Java applications)
- **executable\_stack** - Stack protection
  - prevents the execution of instructions that reside in process stack
- **# sysconfig -q proc**  
executable\_stack = 0  
executable\_data = 5

© 2004 HP corporate presentation. All rights reserved.

31



## More Sysconfig Tunables

- **Core dump prevention**
  - For processes in general, dump\_cores
  - For only processes running setuid/setgid images, dump\_setuid\_cores
  - **# sysconfig -q proc**  
dump\_cores = 0 (0 = cannot dump core)  
dump\_setuid\_cores = 0 (0 = cannot dump core)

Copyright © 2004 HP corporate presentation. All rights reserved.

32





## More Sysconfig Tunables

- Safe symlink behavior
- Should mkdir follow final symlink?
  - # sysconfig -q vfs
  - follow\_mkdir\_symlinks = 0
- 0 is recommended, restores V4.x behavior

Copyright © 2004 HP corporate presentation. All rights reserved.

33



## More Sysconfig Tunables

- Safe symlink behavior
- Controls open(), link(), rename() actions
  - # sysconfig -q sec
    - restricted\_symlink\_follow = 1
    - restricted\_hardlink\_creat = 1
    - restricted\_fifo\_open = 1
- 1 is recommended for maximum protection against symlink attacks, see sys\_attrs\_sec for details

Copyright © 2004 HP corporate presentation. All rights reserved.

34



## NFS

- Use only if absolutely necessary
- mountd -a -i
- no anonymous access
- read-only, nosuid where possible
- Careful use of /etc/exports
- Fully qualified hostnames
- Don't run automount daemon

Copyright © 2004 HP corporate presentation. All rights reserved.

35



## Audit Configuration

- Sysman auditconfig
- Take the defaults except:
  - for strict “C2” - if log space exhausted, halt system
  - choose “networked\_system” event profile
  - Add “audit command name used by accounting” to style flags
- Don't forget to regularly back up your audit logs off the system
- Don't forget to regularly examine the audit logs!

Copyright © 2004 HP corporate presentation. All rights reserved.

36



## Using Auditing

- Can mark interesting directories to record file creation, deletion, etc
  - `auditmask -x directoryname`
- Can export audit data to excel spreadsheets
- Review audit logs for interesting events
  - `audit_tool -e auth_event `auditd -dq``
  - `audit_tool `auditd -dq` -l"/tmp"`

Copyright © 2004 HP corporate presentation. All rights reserved.

37



## “Welcome” Messages

- Eliminate CDE "Welcome" message
  - `copy /usr/dt/config/C/Xresources to /etc/dt/config/C/Xresources`
  - `uncomment`
    - `Dtlogin*greeting.labelString:`
    - `Dtlogin*greeting.persLabelString:`
  - change “Welcome” to warning of your choice

Copyright © 2004 HP corporate presentation. All rights reserved.

38



## “Welcome” Messages

- For a warning displayed before local and telnet logins, create /etc/issue
- # echo “Authorized Uses only!” > /etc/issue
  
- TCP Wrappers feature can be used to replace network "Welcome" messages

Copyright © 2004 HP corporate presentation. All rights reserved.

39



## Vulnerability Assessment

- Sys\_check locally
- Get permission FIRST before testing!
- Avoid peak usage times
- Repeat periodically, keep history
- Tools (Open Source Software Collection CD)
  - satan
  - tcpdump - network monitoring
  - libpcap - network packet capture
  - snort - intrusion detection

Copyright © 2004 HP corporate presentation. All rights reserved.

40



## Final Pass

- Remove compilers
- Remove X / CDE subsets and reset console
- Add firmware password

Copyright © 2004 HP corporate presentation. All rights reserved.

41

## Monitoring





## Monitoring

- Review syslog daily
  - evm
- Review audit logs daily
  - `audit_tool -e auth_event `auditd -dq``
- Use dxaudit to monitor events as they occur
- Periodically run Tripwire
- Use snort and ethereal to monitor your network

Copyright © 2004 HP corporate presentation. All rights reserved.

43



## Forensic Analysis

- Coroners Toolkit
  - [www.fish.com/tct/](http://www.fish.com/tct/)
- CERT - “Steps for Recovering from a UNIX or NT System Compromise”
  - [www.cert.org](http://www.cert.org)
- SANS Institute - “Incident Handling Step by Step”
  - [www.sans.org](http://www.sans.org)

Copyright © 2004 HP corporate presentation. All rights reserved.

44

