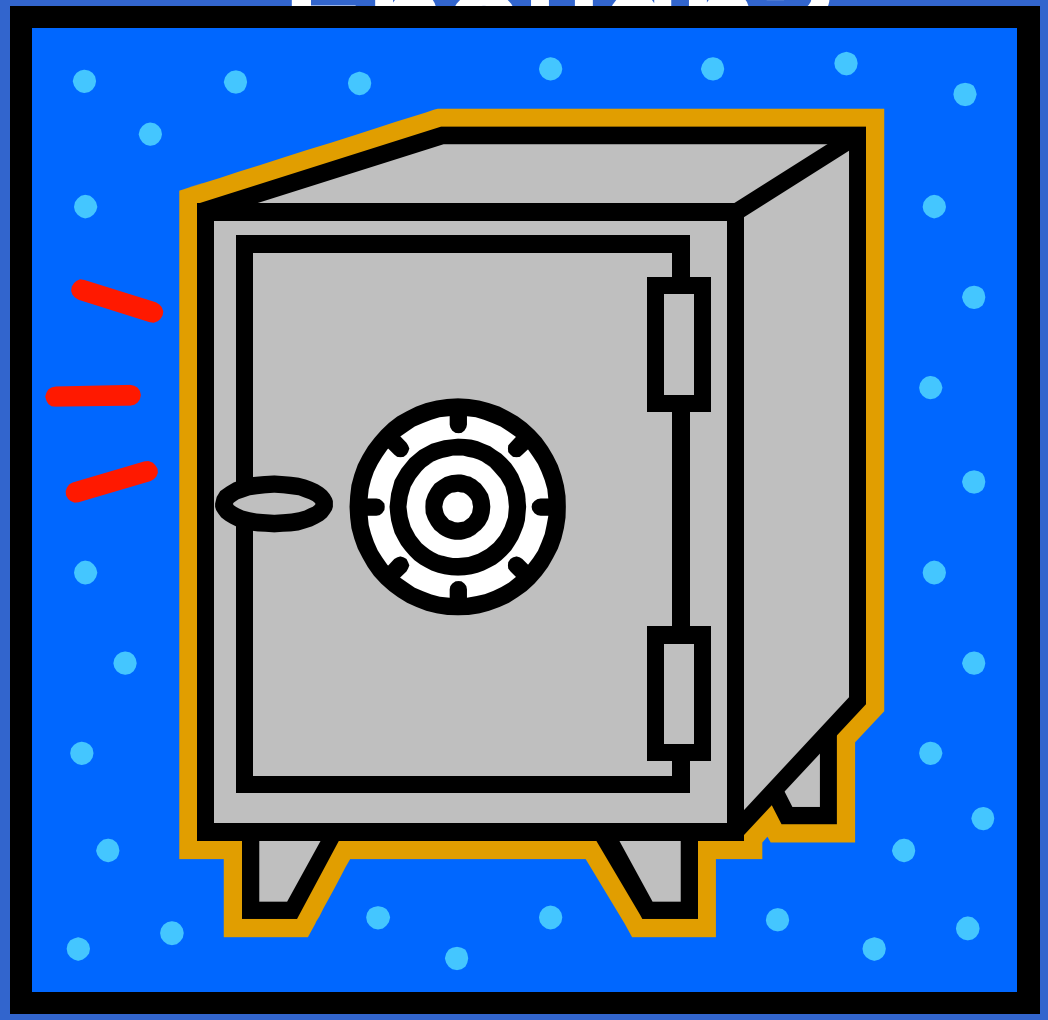

# Securing Tru64 UNIX®

Erin Chapyak
Tru64 Engineering Security Team
Hewlett Packard

# Overview


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

# How Much Security is Enough?



# How Secure is Secure Enough?

- Always a tradeoff – Security vs. Ease-of-Use
- Depends upon system type
  - workstation
  - internal ftp server
  - public web server
  - firewall
- Depends upon value of data stored on system
  - Which information assets are critical?
- Depends on legal requirements
  - HIPAA, DOE or DOD sites, etc.

# Security Policies and Standards

- Corporate policies and standards are absolutely required
- Policies contain class-level security requirements
- Standards are system or procedural specific
- 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

# Key Security Policies

- Incident response policies for a variety of scenarios
  - DoS attacks, root penetration, user account penetration
- Acceptable use policy
- Configuration control
- Vulnerability assessment policy
- Auditing, log and backup storage
- Response to vulnerability reports
  - Bugtraq, CERT, Tru64 UNIX Managers list

# Secure Installation

# Secure Installation Methodology


- Install OS
- Install all patches
- Install applications and tools
- Lock down the system
- Repeat until satisfied:
  - Perform vulnerability analysis
  - Fix vulnerabilities
- Checksum software configuration
- Backup system
- Store checksums & backups in safe place(s)

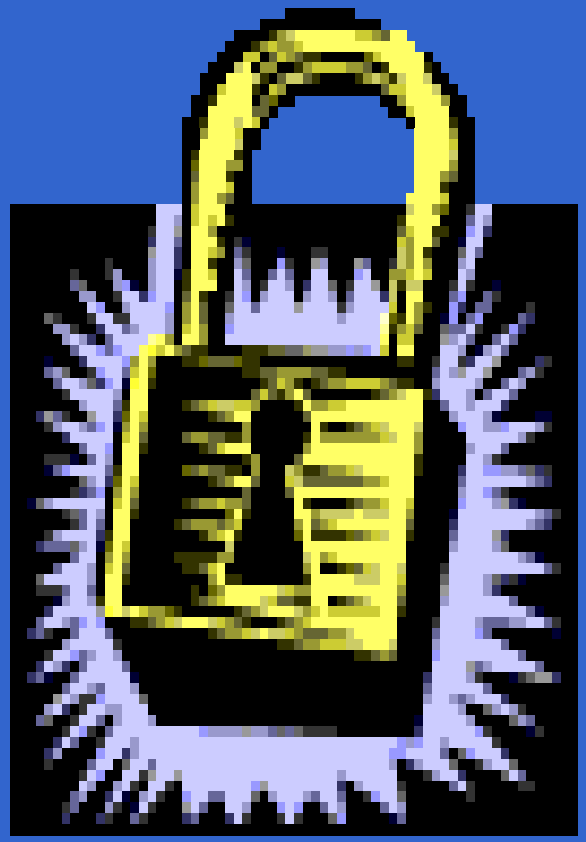
# Tru64 UNIX® Secure Installation Specifics

- Private net or removed from net completely
- Hardware secured
  - locked room
  - password for firmware
  - secure console mode
  - lock the panel, remove the key
- Custom installation to install minimal subsets required

# Tru64 UNIX® Secure Installation Specifics

- Include enhanced security subsets
- Include audit subset and build into the kernel
- Do not include kdebug
- Custom file system setup
  - world-writable directories like /tmp on private partitions
  - /usr read only
- Install latest patches especially SSRT patches
  - http://h30097.www3.hp.com/unix/security-download.html

# Lock Down the Configuration



# System Lockdown Overview

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

# Enhanced Security Configuration

- Sysman secconfig
  - Choose Enhanced Security, custom security profile
  - Take defaults for break-in detection
  - Choose Execute bit set only by root
  - Enable ACLs if needed
- Examine /adjust default account template
- Adjust root account - maxtries

# Install Helpful Tools

- From Open Source Software Collection CD

  http://h30097.www3.hp.com/demos/ossc/html/OSSCV51B.htm

  - lsof
    - lsof -i displays open ports and associated commands/pids/accounts
  - tcp_wrappers - net services control

# Install Helpful 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)

# Install Helpful Tools

- At http://h30097.www3.hp.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)

# 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

# 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

# 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

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

- If you use SSH, you can also disable
  - rshd, rlogind
  - rexecd
  - ftpd
  - telnetd
- Free SSH webkit for V5.1A at http://h30097.www3.hp.com/unix/ssh/
- Shipped with OS V5.1B

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

- If not a mailserver, disable
  - pop3d
  - 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

# Network Services – /etc/inetd.conf , /etc/inetd.conf.local

- If you don't manage LSM by gui, disable
  - initlsmsad - 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

# 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 to original location when applying future patch kits

# Disabling Daemons

- Do NOT remove evmd
  - If not in cluster, prevent evm connections by setting "remote_connection false" in /etc/evmdaemon.conf

  Do not remove esmd

  Do not remove caad (cluster)
- Can disable inetd if:
  - you use SSH
  - you are not in a cluster
  - you don't need the other services

# Disabling Daemons

- Sendmail options:
  - Disable sendmail daemon startup (recommended)
    - Use cron hourly entry instead to process mail

      0 * * * * /usr/sbin/sendmail -q
  - Restrict to send-only
  - Set /var/adm/sendmail/sendmail.conf to reject mail connections from remote hosts

# Configuration Tightening

- Don’t  use NIS if you can avoid it
- Grant 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  (owner root, 0600)

# Configuration Tightening

- Disable localhost source address on physical interfaces
  - in /etc/ifaccess.conf

    ee-0 127.0.0.1 255.255.255.255 deny
  - enable filtering dynamically

    ifconfig ee-0 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

# Configuration Tightening

- Require root password in single-user mode
  - rcmgr set SECURE_CONSOLE YES
- Change default umask to 077
- Prevent network processes from creating core files
  - ulimit -c 0  in /sbin/init.d/inetd
- Check protection of configuration files in /etc
- Set up /etc/ftpusers and /etc/securettys

# File System

- Use separate partitions for world-writable directories like /tmp
  - Hard links can't cross file systems
- Mount read only wherever possible

  Unless / or /usr, mount -o nosuid

  Unless /, mount –o nodev

# File Protections

- Periodically verify that all world-writable directories have sticky bit set
  - find / -type d -perm -02
- Locate setuid and setgid programs
  - find / \( -perm -4000 -o -perm -2000 \) -type f
  - Periodically rerun and compare
  - If truly paranoid, remove all set_id bits and selectively add back
  - login and su may be all you really need

# Sysconfig Tunables

- Buffer overflow exploit protection:
- In 5.1B PK2:
  - executable_data
    - prevents the execution of instructions that reside in heap or other data areas of process memory
    - recommended setting of 5 affects privileged processes only
    - run /usr/sbin/javaexecutedata before changing setting from 0
  - executable_stack
    - prevents the execution of instructions that reside in process stack
  - # sysconfig -q proc

    executable_stack = 0

    executable_data = 5

# Sysconfig Tunables

- Core dump prevention
  - For processes in general, dump_cores
  - For only processes running setuid/setgid images, dump_setugid_cores
  - # sysconfig -q proc

    dump_cores = 0 (0 = cannot dump core)

    dump_setugid_cores = 0 (0 = cannot dump core)

- See sys_attrs_proc man page for details

# 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

- **See sys_attrs_vfs man page for details**

# 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 man page for details

# 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

# Audit Configuration

- Sysman auditconfig

  Take the defaults except:
  - 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!

# 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` -/"/tmp"

# “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

# “Welcome” Messages

- For a warning displayed before local and telnet logins, create /etc/issue

  # echo “Authorized Uses only!” > /etc/issue

- For warning displayed when someone logs in remotely,  use /etc/motd
- TCP Wrappers feature can be used to replace network "Welcome" messages

# Department of Energy version: /etc/motd


WARNING: To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Automated Information System is prohibited and could be subject to criminal and civil penalties.

# Department of Justice version: /etc/motd


This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

# 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 - system admin tool for analyzing networks
  - tcpdump - network monitoring
  - libpcap - network packet capture
  - snort - intrusion detection

# Final Pass

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

# 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
- Snort - lightweight network-based intrusion detection system

# Forensic Analysis

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

# HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP

RECOMMENDED TRAINING VENUE FOR THE

**HP Certified Professional**