HP-UX 11iv2: Survey of Security Features

Stephanie Miller

Software Specialist
System Network and Security Lab
Enterprise Unix Division, HP

HP WORLD 2003
Solutions and Technology Conference & Expo

Agenda

- Basic Overview & Security Refresher
- System Security Criteria
- Standard Mode HP-UX
- Trusted Mode HP-UX
- Managing System Security
- Summary
- Q&A

A Few Simple Rules…

- I have a tendency to talk fast, so please ask me to slow down anytime!
- Let's save questions until the end of the talk so that, in fairness to everyone, we make it through all of the material.

Okay, Let's Get Started!

- A Warm-up Poll:
  - What is your general comfort level with security concepts?
  - Who among us are System Administrators? Managers? Developers? Operations?
  - What flavor of HP-UX do you use today?

- Introductions
  - So, who is Stephanie Miller and what qualifies her to be giving this talk?

Goals of this Session

- To cover core operating system security, and specifically focus on what's now available in HP-UX 11iv2
- To mirror the information available in our newly updated "HP-UX 11i Security Whitepaper"
- To remain true to the scope for this session:
  - System security, yes
  - Network security, no
  - Application security, no

Overview

- We're all here today because security is no longer an after-thought for organizations, it's a prime-time concern!
- HP-UX has some amazing functionality (most of it bundled and free!) to help you in protecting the platform
- The roadways toward stronger system security are paved and ready to be explored!

Facing Reality

The number of security incidents is increasing exponentially

Sources: www.cert.org
CSI – FBI Computer Crime Survey, 2002

Strangers Among Us…

- The Internet is no longer the benign playing grounds for researchers – we passed that stage long ago
- Easy-to-use exploit scripts are available everywhere, for every platform, for any skill level to use
- Information security is no longer just keeping the bad guys out, it's about letting the right ones in – at the right time, to the right service.

Defining the Security Puzzle

- Okay, so I'm preaching to the choir – we all understand there are weaknesses in the infrastructure and the bad guys are standing by to take advantage of them.
- The question now becomes, what does this all mean? What are the day-to-day solutions we as security practitioners must tackle? How do we translate this overall threat to armoring the individual systems we manage?
- Let's first define the critical issues that information systems need to address before we jump into what features are offered in HP-UX today.

System Security

- Fundamental Principles
  - Identification and authentication
  - Authorization
  - Access control
  - Audit/Accountability
  - Object reuse
  - Intrusion resistance
  - Intrusion detection
  - System hardening
  - Assurance

Identification and Authentication

- Uniquely identify each user on a system
- In Unix, this is accomplished with a user_name and a numeric user_id
- Authentication refers to the proof that the user is who he/she says he/she is:
  - Something you are (i.e. your user_id)
  - Something you have (i.e. a fingerprint)
  - Something you know (i.e. a password)
- Methods must become more complex as degree of trust rises

Authorization

- The authorization mechanism in a system grants privileges to individual users – usually grouped by class (i.e. root users, regular users)
- Fine-grained authorization separates an all-powerful root user's power into separate authorizations (administer systems, perform backups, etc)

Authorization Mechanisms

- **RBAC (Role-Based Access Control):** Associate users with roles, which are then assigned capabilities.
- **Command Authorizations:** An extension of the role concept into the implementation of existing commands such that they may behave differently depending on the role of the invoking user.
- **MAC (Mandatory Access Control):** Access restrictions placed on file access and inter-process communications to prevent rogue processes in one compartment from affecting other compartments.
- **Fine-grained Privileges:** Within the kernel of traditional Unix systems access checks are limited to all-or-nothing root or not root.
- **Privilege Bracketing:** Extending existing commands to limit the duration for which necessary privileges are active, therefore limiting the window of exposure.

Access Control

- A system's access control mechanism mediates user access of system resources (files, printers, programs, etc.).
- Traditional UNIX access controls consist of two mechanisms: standard UNIX file permissions (read, write, execute granted on a user, group, other basis) and Access Control Lists
- Access Control Lists are file-specific and mediate access to that file, regulated by a finer granularity than standard UNIX permission bits

Audit & Accountability

- The audit system can be configured to log system call events that root and ordinary users do on the system
- Capture pertinent information to assist in attack analysis and forensics

Object Reuse

- For a system to be secure, it must guarantee that a newly created object (memory buffer, file, etc.) does not contain information “left over” from the last time it was used.
- The ‘object reuse’ requirement of a secure system simply states that all user accessible resources are initially cleared or otherwise initialized so that no lingering information can be extracted from them

Intrusion Resistance

- Sound Design and Implementation principles used
- Common vulnerabilities over the years have included:
  - Poor programming practices in privileged application code that results in buffer overflow and/or race condition vulnerabilities
  - Password cracking or weak password encryption
  - Poor or insecure system configuration

Intrusion Detection

- Intrusion detection is the art and science of detecting illegal and improper use of computing resources by unauthorized outsiders and authorized employees, before such misuse results in excessive damage
- It does this by providing continuous monitoring of critical systems and data

System Hardening

- System hardening is the act of disabling unnecessary services and configuring the Operating System with the minimum set of features, users, and applications required for it's core functionality
- Actions to be taken manually or scripted include:
  - disabling of ports for specified network services
  - installation of all system critical and security related patches
  - configuration of daemons with the limited set of services
  - enablement of a system firewall for further lock-outs and monitoring.
- There are many published guides and benchmarks today to reference

Assurance

- Functionality alone is not enough to determine the security of a system.
- Assurance that the system's security features work as advertised is required for some applications, particularly deployments within military and government domains.
- Two basic classes of assurance exist:
  - vendor self-assurance (through their own design, development, and testing process)
  - independent third party evaluations (such as the common criteria certification)

Modes of Operation

- Standard Mode
  - Default operating system functionality
  - Good for every day operations
  - Enhancements being made each release to bolster standard mode robustness
- Trusted Mode
  - Historically, meant to address the C2 requirements
  - Enhancements to base security
  - Simply enabled/disabled; it's already built into system

The boundary is blurring…

- More and more of the features once available only with Trusted mode are becoming mainstream in standard mode HP-UX 11iv2
- An a la carte menu of options to allow the system owner to define the degree of protection necessary
- We are exploring the continuum of balance between protection, performance, and manageability

Standard Mode

- Addressing the fundamentals:
  - Identification and authentication
  - Authorization
  - Access control
  - Audit/Accountability
  - Object reuse
  - Intrusion resistance
  - Intrusion detection
  - System hardening
  - Assurance
- And then some…
  - Strong random number generator

The Default State

- This section will address features of HP-UX available today – in the default configuration
- Most features we'll cover are built-in components of the system
  - and we'll also discuss a couple of customer-selectable options in the OE (operating environment)
- Standard Mode HP-UX represents legacy, industry-standards based Unix

Identification and Authentication

- Users are identified with an eight character maximum username.
- Each username is mapped in the /etc/passwd file (or other backend repository) to a numeric user_id

Shadow password functionality, once only available in Trusted Mode, is now available in Standard Mode HP-UX 11iv1.6 and HP-UX 11iv2

Shadow Password

- Shadow passwords simplify the administration of multi-vendor configurations, since shadow passwords are a defacto standard (Solaris, Linux, etc.)..
- These hidden passwords are not seen in clear text.
- Passwords will be moved from the public readable /etc/passwd file to the /etc/shadow file, which is accessible only by a privileged user
- Co-existence with LDAP supported in HP-UX 11iv2

PAM

Pluggable Authentication Module

- Allows for multiple, replaceable authentication methods in the system – and the modules are “stackable”
- PAM supports authentication from files (/etc/passwd), Network Information Service (NIS), and NIS+.
- In addition HP offers three separate products that provide alternate authentication mechanisms installable on HP-UX 11.x
  - PAM NTLM providing authentication from a Microsoft Windows NT 4.0 domain controller (included in the CIFS Client B8724AA)
  - PAM Kerberos supporting authentication via Microsoft Windows 2000 or MIT Kerberos v.5 KDC (J5849AA)
  - PAM LDAP supporting authentication of POSIX accounts stored on an LDAP v3 directory (included in LDAP/UX Integration product J4269AA)

Authorization

- Root users have full authorization to administer the system
- Some HP-UX commands have the privilege to change their effective user id to root in order to do specific privileged functions on behalf of an unprivileged user (setuid, setgid)
- HP offers additional administrative authorization tools such as Restricted SAM, ServiceControl Manager, and the freeware tool sudo, which can delegate portions of root power for role-based system administration

Access Control

- Standard UNIX file access control is provided
  - Each file has a single user and group owner. File access control is accomplished through UNIX permission bits
- Access Control Lists (ACLs) offers Discretionary Access Control (DAC) at a level of granularity finer than standard permission bits
- HP-UX High Performance File Systems (HFS) ACLs that can assign the above read, write, and execute permissions to an arbitrary number of users
- Beginning with HP-UX 11iv1, ACLs are available with The Journaled File System (JFS)

Audit & Accountability

- Industry compatible UNIX provides several system logs to record system activity.
- The primary security logs are *syslog*, *sulog*, process accounting logs, and user accounting logs.
  - *Syslog* records basic system operations. Any application program can write logging messages to *syslog*.
  - *Sulog* records the usage of the *su* command
  - Wtmp, utmp, btmp records user and accounting information for such commands as last, who, write, and login

Object Reuse

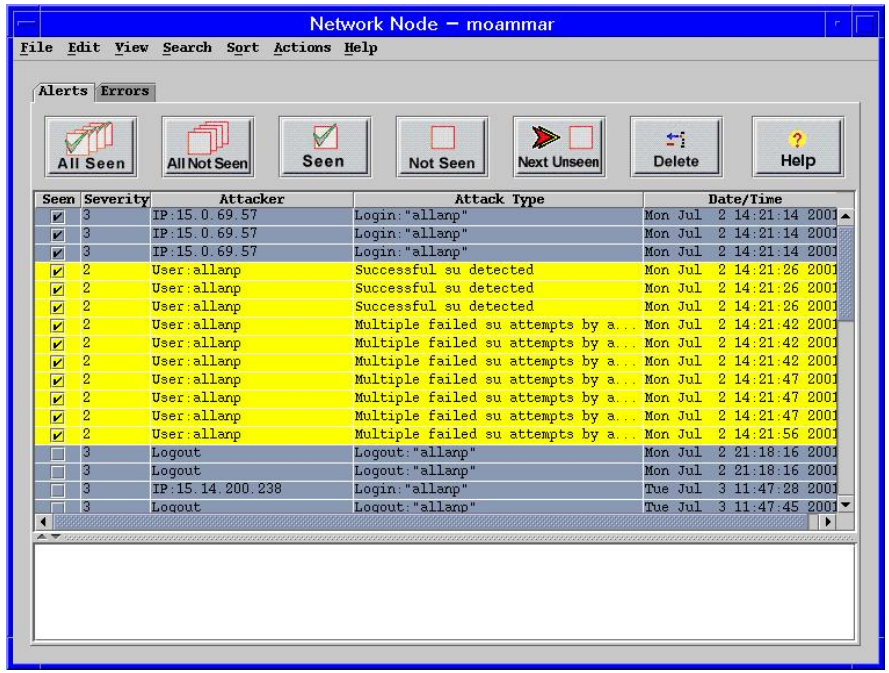
- HP-UX satisfies the object reuse requirement of a secure system in the Standard mode as well as in Trusted Mode.
- Memory buffers and files are initialized to known values before allocation to a user to prevent a previous user's data from being disclosed

Intrusion Resistance

- With HP-UX 11i, buffer overflow vulnerabilities are substantially reduced with the *Execute Protected Stack* feature
- This feature prevents the widely used attack against privileged programs of overflowing input buffers and placing executable code onto the system stack, which can under certain circumstances be executed
- The HP-UX stack overflow protection offers for the advantage of a per-binary override to enable legitimate applications to operate without problem
- See the *chatr* manpage for more information

Real-time host intrusion detection

- Detection Template
  - kernel audit data
  - high quality detection
  - not just audit log detection
  - five patents on technology
- Real-time alerts
  - agents on hosts
  - alerts to management console … or to…
  - OpenView VPO management
- The intrusion detection kernel data collector, known as idds, is independent of the Trusted Mode audit functionality



Added Goodies: /dev/random

- The strong random number generator is available as an additional core operating system feature beginning in HP-UX 11iv2 for IPF-based systems
- The strong random number generator is available as /dev/[u]random once configured as a dynamic loadable kernel module (DLKM).
- The Strong Random Number Generator provides a secure, non-reproducible source of true random numbers for applications with strong security requirements, such as for generating encryption keys
- The /dev/random functionality is also available for HP-UX 11iv1 as a web release for PA-based systems.

Assurance

- HP thoroughly tests HP-UX to HP's high internal standards for product quality, reliability, and standards conformance requirements before releasing the product for customer shipment
- HP monitors security advisories from major computer security centers, such as CERT and FIRST and responds as needed
- Standard HP-UX does not meet either the US or the European C2 security requirements. To meet these, the system must be in Trusted Mode

Summary Table

Standard Mode HP-UX Feature Availability

	10.20	11.00	11iv1	11iv2
Industry Standard UNIX Security	X	X	X	X
Object Reuse	X	X	X	X
HFS Access Control Lists	X	X	X	X
Restricted SAM	X	X	X	X
ServiceControl Manager Roles		X	X	X
Large (>60000) User IDs	X	X	X	X
Keberos V5 Authentication	X	X	X	X
LDAP v3 Authentication		X	X	X
Windows 2000 Authentication		X	X	X
NIS Manageability	X	X	X	X
Pluggable Authentication Module		X	X	X
NIS+ Manageability		X	X	X
JFS Access Control Lists			X	X
Encrypted Password Protection			X	X
Boot Authentication				X
Long Passwords				X
Password Complexity Checking			X	X
Password Reuse Checking				X
Password Life Cycle Management				X
Login Controls				X
Auditing			X[2]	X[2]
Strong Random Number Generator			X[3]	X
Boot Authentication				X
Execute Protected Stack			X	X

Trusted Mode

- Expanding on the fundamentals:
  - System boot authentication
  - Stronger password policies
  - C2 audit enablement
  - Improved user accounting (automatic expiration, login restrictions, disabling after failed login attempts)

Trusted Mode

- Trusted Mode gives the administrator or security officer additional features and options not available with standard UNIX security.
- When the system administrator invokes trusted mode conversion through SAM, the system creates the “Trusted Computing Base” (TCB), which provides the mechanisms and architecture to extend HP-UX security to be fully C2 Security compliant.
- Conversion to the TCB includes protected password database, system default files, terminal default files, device assignment files, and modified crontab entries.

System Boot Authentication

- Boot authentication provides that only authenticated and authorized users can access the system in its maintenance ‘single-user’ mode
- Configuration of boot authentication is controlled by the SAM utility while the system is in trusted mode.

While this feature was only available in Trusted Mode prior to 11iv2, it has been ported to Standard Mode with the 11iv2 release….AND is also available for 11v1 via the web (as of last week)

- This feature is configured differently in Standard Mode and Trusted Mode; check the documentation

Password Management

- Encrypted password protection (aka Shadow Password)
  - Encrypted passwords are not stored in the publicly readable /etc/passwd file but are stored in the root-only readable protected password database
- Long Password
  - A longer password, containing an increased amount of complexity – also known as entropy, is harder to crack than a short password
- Password Complexity checking
  - Password screening can detect and reject passwords based on policies for dictionary words, contain repeated characters. Enforce letter, number, punctuation usage vs. policies

More Password Management

- Password Reuse Checking (Password history)
  - Denies a user reuse of his/her old passwords
- Password Lifecycle management
  - minimum time that the password must be used
  - expiration time
  - warning time

Login Controls

- The system administrator can establish per user controls on when that user can access the system
  - Time-Based Controls: The user's access is regulated by the time of day and day of week.
  - Device based access controls: The system administrator can dedicate specific mux or DTC ports for a user. If a user tries to login via an unauthorized port, he/she is denied access to the system.
  - Account locking after consecutive failed login attempts.

Audit/Logging

- Using the Audit ID extension of Trusted Mode to uniquely identify users, the audit system can be configured to audit any of over 100 security relevant system calls on a per-user basis
- System call auditing is the most secure form of accountability. It is also the most resource intensive!
- HP provides a tool through the System Administrator (SAM), to view the audit records. This tool can be configured to filter out audit records that are of no interest to the system administrator
- The introductory man page for audit functionality is available in audit (5).

Certification and Compliance

- Trusted-mode HP-UX 11iv1 has achieved Common Criteria EAL4-CAPP certification – the certificate of compliance was presented in March, 2003.
- TCSEC CT, ITSEC E3/F-C2
  - Certified – 10.20
  - Compliant – 11.0, 11iv1, 11iv1.5, 11iv2

Summary Table

Trusted Mode HP-UX Feature Availability

	10.20	11.00	11iv1	11iv2
Encrypted Password Protection	X	X	X	X
Boot Authentication	X	X	X	X
Long Passwords	X	X	X	X
Password Complexity Checking	X	X	X	X
Password Reuse Checking		X[1]	X	X
Password Life Cycle Management	X	X	X	X
Login Controls	X	X	X	X
Auditing	X	X	X	X
C2 Security Compliance	X	X	X	X
JFS Support in Trusted Mode	X	X	X	X
NIS+ Manageability		X	X	X

HP-UX Security Manageability

- Peeking into the Management Toolbox:
  - SAM
  - Servicecontrol Manager
  - System Hardening / Scripts
  - OpenView integration
  - NIS, NIS+

Our Friend: SAM ☺

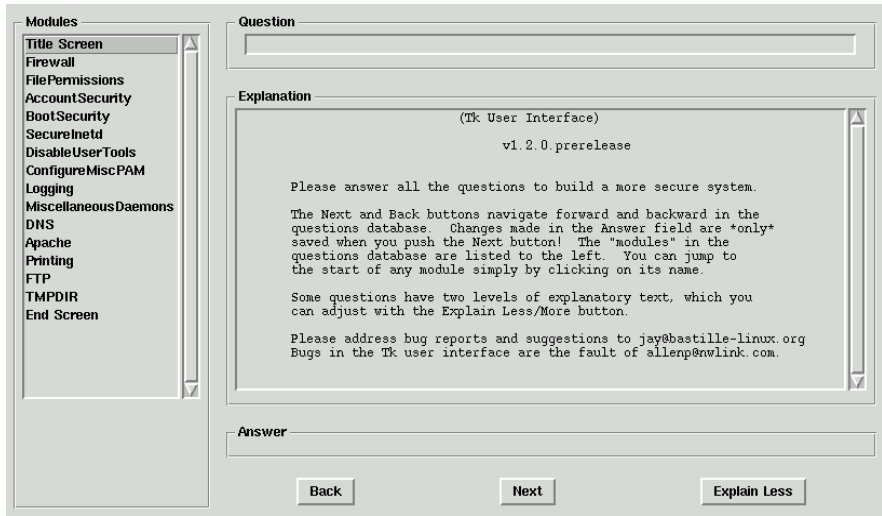
- SAM is the basic administration tool for configuring a single HP-UX system.
- Through SAM, the administrator converts the system to Trusted Mode and from there administers all the user configuration and audit configuration for the system.
- SAM can be configured to restrict what its authorized users can do. Called Restricted SAM, this feature allows the root administrator to delegate limited authority to others without giving the entire power of root away.

SCM: Service Control Manager

- Service Control Manager is the central point of control that proactively orchestrates the administration of many servers at one time.
- With ServiceControl Manager, system administrators are able to execute systems management tasks simultaneously on multiple HP servers
- ServiceControl Manager's Role-based Authorization allows certain users to operate only on certain nodes

System Hardening: HP-UX Bastille

- Security lockdown tool
- Various hardening required of servers used for web-servers, applications, and databases.
- 70 configurations presented as security/usability tradeoff questions
- Configures or disables: daemons, system settings, and IPFilter, password shadowing, inetd audit
- Turns off unauthenticated services such as pwgrd and printing, rcp, and rlogin
- HP-UX Bastille is part of the open-source community



System Hardening: Security Patch Check

- Security Patch Check is a tool that analyzes the currency of a system with respect to security patches.
- It recommends patches for security vulnerabilities that have not been fixed by other patches currently on the system
- Security Patch Check is compatible with Service Control Manager and is integrated into the Bastille utility.
- All HP-UX 11.X flavors are all supported by Security Patch Check

System Hardening: IP Filter

- The HP-UX IPFilter (B9901AA) is a stateful system firewall that filters IP packets to control packet flow in or out of a machine
- It can be run either as Dynamic Loadable Kernel Module (DLKM) or as statically linked modules on HP-UX 11.0, 11iv1, 11i v1.6 and 11i v2
- Another public domain software component

OpenView Integration

- The Host IDS product has been integrated with the OpenView Operations product.
- A Smart-Plugin (SPI) is available for free download from the OpenView gallery
- This SPI offers basic functionality for the management of intrusion detection related alerts

NIS / NIS+

- Provides a method to centrally configure and manage groups of UNIX systems.
- One NIS Master server can manage all the user accounts and standard security configuration of an entire domain of NIS Clients in a network.
- The standard mode of HP-UX security can be managed with NIS. Trusted Mode security (extended passwords, auditing, etc.) cannot be supported in a NIS domain.
- NIS+ is the second generation of NIS and supports extended security attributes
- NIS+ does offer support for Trusted Mode security

Summary

- HP-UX is well grounded in the fundamentals of system security – in fact we're a leader in the industry!
- We focused this talk on core OS features – be sure to consider the full range of network and application services also available for protecting your enterprise
- We've covered a lot of features in a short amount of time!

D.H. Brown Ranks HP-UX #1

- #1 scalability
- #1 reliabilitiy, availability, and serviceability
- #1 systems management
- #1 internet and web application services
- #1 directory and security services

Call to Action

- We've built a lot of security functionality into HP-UX 11i. Help us help you by using the features we've just discussed and by sharing your successes, feedback and recommendations!

"If you build it, they will come"

- *Kevin Costner in Field of dreams (1989)*

References: The Perennial Favorites

- http://docs.hp.com
- http://software.hp.com
- http://www.hp.com/go/security
- http://www.hp.com/go/unix
- And there are many more in Section 6 of the HP-UX 11i Core Security Whitepaper

Thank You!

Questions?

Interex, Encompass and HP bring you a powerful new HP World.

Don’t Forget…

- NIS/LDAP gateway
- PAM Unix
- /etc/default/security – 11i
- Open SSL (v9.9 with Apache)
- NFS enhancements
- FTPD- secure FTP and virtual servers
- X11 Xwindows security extensions
- Fast Crypto from RSA
- SSH
- IPSec

- … And the many other security tools/features offered for HP-UX