Global Information Assurance Certification Paper

Securing UNIX GCUX Practical Assignment
Version 1.9 (revised April 8, 2002)

HP-UX 11.0 Installation and Security Verification Checklist for "Lawson" Application Server

Prepared by Theodore Ellis

1 Executive Summary

This paper provides a step-by-step recipe for building a HP-UX 11.00 server from the ground up, with the end state being a functional and secure platform. The checklist detail will focus on securing the HP-UX operating system to support an "off the shelf" application product. The software product used to create this checklist is the Lawson Insight Accounting software package, Version 7.3.3. Many "off the shelf" products have limitations that prevent making large changes designed at tightening security without violating the product's support contract. Lawson is no exception, so extreme caution is required when changing any part of the application. Lawson does have a complex security feature built into the application that addresses accounting user access and separation of roles and responsibilities. This paper will not go into any detail on the internal Lawson security features, but will instead address how the Lawson installation can be tuned to address key security gaps without violating any support agreements with Lawson. With the goal being a secure platform that supports "off the shelf" application installations, this checklist is designed for other third part software with similar environment requirements to Lawson.

2 System Description

2.1 Hardware

The system is a HP 9000 enterprise class server, model K570. The server is configured with three 200 MHz PA-RISC processors, 2 GB of physical memory, and two internal 18 GB hard drives. A SCSI dvd-rom and DDS-DAT2 tape drive are also installed. A peripheral 100Base-TX network adapter will provide network connection to the LAN backbone.

2.2 Operating System and Applications

The operating system to be installed and secured is HP-UX version 11.0 (64-bit), release December, 2001. Installation patch bundles and additional HP released applications are found on the HP-UX 11.0 Support Plus and Application Software media sets, release December, 2001. A Lawson Insight application will be installed, which is a third party application used for finance based corporate needs. The Lawson version to be installed is operating environment 7.3.3 for HP-UX with application version 7.2.3. A separate license has been supplied to allow for the installation of the disk mirroring tool HP-MirrorUX, release December, 2001.

2.3 System End State Description

This system will function as a Lawson Insight application server within a corporate firewall. The Lawson software is "off the shelf" and typically installed with the assistance of a Lawson technical resource. The client users will have access to the server via the Lawson Desktop Client with a very specific configuration. Users will not be able to compile any software directly on this machine, but they will require file transfer rights in order to perform normal accounting duties. Shell scripts, Perl scripts and binaries precompiled on another platform will be executable on the platform. Primary IP name resolution will be through DNS client, with all other network service verifications defaulting to local files. Electronic mail will be enabled for both send and receive, but with additional security settings enabled to secure this service. A dual boot disk configuration will be used with the boot disks mirrored, providing root volume group hardening. The following software will be installed in addition to the operating system:

- QPK1100.depot - Quality Pak patch bundle, December 2001
- HWE1100.depot – Hardware Enablement patch bundle, December 2001
- HP-PB 100Base-TX driver
- HP IgniteUX, release December 2001
- Perl
- Lawson Insight Financial suite (version 7.2.3) – installation steps not covered

3 Risk Assessment

The Lawson Insight Application installed on this server is a corporate financials software suite. Clients across the corporate network will use the application to execute all levels of corporate accounting, including, but not limited to, accounts payable, accounts receivable, payroll, benefits, asset management and purchase orders. The primary risk in failing to secure this server is nothing less than the compromise of critical corporate accounting information. The Lawson application environment runs on a Unix shell, with each individual user having a separate shell for each login. Lawson code is also notorious for having wide-open file system privileges that cannot be changed without damaging the basic software functionality. With users requiring a shell and direct access to the server, file transfers, shell access, user account information, file system control, and assorted services all take on high security priority. The Lawson software footprint on the server is very large, with a single instance of code requiring more than 1 GB of disk space, not including any database space.

The primary threat axis comes from unauthorized access to the system. Access could be from existing application users or from outside the organization. Significant damage to the Lawson application is possible from any user having access to a basic shell session. This is the result of Lawson's code set file permissions, which are not universally restricted based on normal UNIX security standards. It is, therefore, imperative that the security focus be on preventing unauthorized access to the system. Though the UNIX operating system can be tightened to limit damage from unauthorized access, the Lawson application files themselves could easily be tampered with or destroyed.

The Lawson application server is located within a corporate firewall, but the code sensitivity requires extreme vigilance with regard to security. The firewall cannot be the only line of defense. The Lawson server will need to have services and functionality limited to those required for Lawson operation and security monitoring. Automated monitors will have to be in place to constantly scan for attempts at breaching security. The UNIX system functioning as the Lawson application server must be secure enough for the entire corporate structure to place full faith in the security and integrity of their most sensitive information.

4 Installation Checklist

4.1 Operating System Installation and Configuration

This part of the guide will install the base operating system, key patches and software. Completing this section will result in a stand-alone system that is not connected to any network. The network connection will be established during the operating system security configuration.

4.1.1 Base Operating System

___ 1. Confirm hp-ux 11.0 install/update/recovery and support plus media versions. This install requires the December, 2001 install/update/recovery cdrom and the March, 2002 support plus cdrom.
___ 2. Verify that all peripheral devices are power on (dvd-rom, DDS, etc.)
___ 3. Turn the server on and insert the install media in the dvd-rom drive.
   a. NOTE: in this document, a cdrom is considered equivalent to a dvd-rom.
___ 4. Interrupt the boot sequence when prompted. The autoboot menu will be displayed.
___ 5. Locate the dvd-rom bootable device with the "sea" command
   a. The dvd-rom device will be reported as something similar to p3 below:

Path #	Device Path (dec)	Device Path (mnem)	Device Type
p0	10/0.6	fwscsi.6	Random access media
p1	10/0.7	fwscsi.7	Random access media
p3	**10/12/5.2**	**sescsi.2**	**Random access media**

   b. NOTE: hardware configurations will typically use a standard hardware path for peripherals such as DVD or DDS drives for each server class. The dvd-rom is a SE scsi device and will show as a se-scsi device path. A DDS drive may be on the same scsi chain as the dvd-rom, but will show as a Sequential access media instead of Random. Check the configuration of the server to determine which path is correct.
___ 6. Boot from the dvd-rom device with the following command:
   a. bo <hardware path from sea>
___ 7. Select "n" when asked to interact with IPL.
___ 8. At "Welcome to the HP-UX Installation/Recovery process!"
   a. select "Install HP-UX"
___ 9. Select the defaults on the "User Interface and Media Options"
   a. Source Location Options: Media Only Installation
   b. User Interface Options: Guided Installation
   c. NOTE: use the advanced option for customizing file systems with the install
___ 10. Select a configuration: 11.0 for commercial server
___ 11. Select a environment: 64-Bit CDE HP-UX Environment

   a. NOTE: the hardware must support 64-Bit to install the 64-Bit environment

___ 12. Select an appropriate root disk
___ 13. Specify desired swap space. Recommend matching primary swap space to physical memory, unless the system is a large memory configuration that makes this unpractical
___ 14. Select File system: Logical Volume Manager (LVM) with VxFS
___ 15. Keep one disk in the root volume group
___ 16. Select the language requirements
___ 17. Select appropriate use license
___ 18. Select the required additional software for:
   a. Installed card adapters (FDDI, HP-PB, etc)
   b. OnLineDiags
   c. QPK1100 patch bundle
   d. HWE1100 patch bundle
___ 19. Complete pre-install checks by verifying the root disk and acknowledging any warnings
___ 20. Select finish to start the installation, follow the install process and provide any required media changes when prompted.
___ 21. When install is complete, a large OK will be displayed and the system will reboot automatically
___ 22. Answer "no" when asked if you are ready to link this system to a network. The initial security configuration will be completed prior to establishing any network connections to prevent a compromise of the server during the installation when no security is yet in place.
___ 23. Answer "no" for DHCP use.
___ 24. Assign a host name, proper time zone, system clock and root password
___ 25. The system will now complete the boot process and return a login prompt on the local console.

4.1.2 Supplemental Software Installation

Additional software can now be installed from the HP-UX 11.0 application software set or from web based downloads. Some applications may require special codewords that are obtained through the purchase of a license. The only software described in this checklist is considered part of the environment necessary for properly securing the system. Log in as the root user in order to complete the following installations.

___ 1. Perl: The Perl language will be used to support script runs that can be used for a variety of information gathering and monitoring uses. The mount the correct application disk at /cdrom. For the December, 2001 release, disk 5 holds the perl software. Create the /cdrom directory with mkdir.
___ 2. run "swinstall –s /cdrom" and select perl programming language for installation
___ 3. HP Ignite-UX: For security purposes, the Ignite-UX tool set offers administers the ability to create bootable tape images of the root volume

group that can be used to recover a system. Download the Ignite-UX (ignite11_11.00) utility for HP-UX 11.00 from the following web-site: http://www.software.hp.com/products/IUX/download.html

___ 4. Move the downloaded file onto the new server and run "swinstall -s /tmp/ignite11_11.00" to install the tool set.

___ 5. Install other applications as required for server functionality. While the server is off the network, install C to allow for compiling operations. This will be removed before the server is placed on the network

4.2 Securing (Stripping Down) the Operating System

This portion of the checklist covers items that should be turned off, removed and/or replaced that are enabled as part of a standard operating system installation.

4.2.1 Login Banners

Change the login banners displayed to a login attempt to prevent the system from divulging information about your system configuration and to issue a warning to unauthorized users. This is a simple step that cannot only keep people from gaining information about your system, but also useful in a court of law if prosecution of intruders is required. The following steps replace login banners for terminal sessions, telnet and CDE.

___ 1. vi the file /etc/issue and replace the contents with:
WARNING! UNAUTHORIZED USE PROHIBITED!!

___ 2. vi /etc/inetd.conf and modify the telnet line with the banner option as follows:
telnet stream tcp nowait root /usr/lbin/telnetd telnetd **–b /etc/issue**

___ 3. Restart inetd to reread the new configuration: "inetd –c"

___ 4. Copy /usr/dt/config/C/Xresources to /etc/dt/config/C/Xresources

___ 5. vi /etc/dt/config/C/Xresources and modify the Dtlogin line with:
Dtlogin*greeting.labelString: "WARNING! UNAUTHORIZED USE PROHIBITED!"

___ 6. Make sure any line commenting is removed from the above line

___ 7. Reset dtlogin with /sbin/init.d/dtlogin.rc reset

4.2.2 Securing inet Services

Several services defined under the internet daemon, inetd, are considered both unsafe and unnecessary. The following steps address the /etc/inetd.conf file.

___ 1. vi the /etc/inetd.conf file and comment out with a leading "#" the following lines (note: several are commented out by default):

finger stream tcp nowait bin /usr/lbin/fingerd fingerd
tftp dgram udp wait root /usr/lbin/tftpd tftpd\ /opt/ignite\/var/opt/ignite
bootps dgram udp wait root /usr/lbin/bootpd bootpd

rpc stream tcp nowait root /usr/sbin/rpc.rexd 100017 1 rpc.rexd
rpc dgram udp wait root /usr/lib/netsvc/rstat/rpc.rstatd 100001 2-4 rpc.rstatd
rpc dgram udp wait root /usr/lib/netsvc/rusers/rpc.rusersd 100002 1-2 rpc.rusersd
rpc dgram udp wait root /usr/lib/netsvc/rwall/rpc.rwalld 100008 1 rpc.rwalld
rpc dgram udp wait root /usr/sbin/rpc.rquotad 100011 1 rpc.rquotad
rpc dgram udp wait root /usr/lib/netsvc/spray/rpc.sprayd 100012 1 rpc.sprayd
daytime stream tcp nowait root internal
daytime dgram udp nowait root internal
time stream tcp nowait root internal
time dgram udp nowait root internal
echo stream tcp nowait root internal
echo dgram udp nowait root internal
discard stream tcp nowait root internal
discard dgram udp nowait root internal
chargen stream tcp nowait root internal
chargen dgram udp nowait root internal

___ 2. enable inetd logging in /etc/rc.config.d/netdaemons using vi to update the INETD_ARGS variable:
   a. vi /etc/rc.config.d/netdaemons
   b. find and edit the INETD_ARGS entry with:
      export INETD_ARGS="-l"

___ 3. enable ftp logging:

ftp stream tcp nowait root /usr/lbin/ftpd **ftpd -oil**

___ 4. append "-l" to the following r-service entries to force the HP-UX server to ignore user .rhosts files completely. This step does not disable .rhosts files configured for the root user. Users will not be allowed to bypass passwords using these services:

login stream tcp nowait root /usr/lbin/rlogind rlogind **-l**
shell stream tcp nowait root /usr/lbin/remshd remshd **-l**
exec stream tcp nowait root /usr/lbin/rexecd rexecd **–l**

___ 5. If step 4 above is not practical, then scripts run by root cron will need to be in place to scan for improper entries in user .rhosts files (ie.+ +).

4.2.3 Access Control Lists (ACLs)

Access to the Software Distributor software suite (SD-UX) needs to be restricted to the local root user. The SD-UX software by default will allow arbitrary remote hosts the ability to list software and patches installed on the host. Having access to software and patching levels could provide enough information for an unauthorized individual to locate system vulnerabilities.

___ 1. Issue the following command to remove all but the root user from accessing the SD-UX software: "swacl –l root –D any_other"
___ 2. Verify the SD-UX ACLs with: "swacl –l root"
___ 3. Ensure that no entry with "any_other" is listed in the output.

4.2.4 Tcpwrapper

Tcpwrapper is a free program that "wraps" around and controls access to a second program. Tcpwrapper will be installed and configured to provide additional security to several inetd services. This tcpwrapper configuration will be configured for telnet, ftp and rlogin services with limitations based on network subnets and a "default deny" policy. The "default deny" implies that any tcpwrapper service not explicitly allowed will be denied by default if a user attempts to use them. Install TCPwrapper before OpenSSH in order to allow for the installation of OpenSSH using TCPwrapper. Since the TCPwrapper program does not require client based files, it can be used with Lawson.

___ 1. download the latest copy of the Tcpwrapper software from (version 7.6 for this checklist). Get the tar file and the license file. ftp://ftp.porcupine.org/pub/security/index.html
___ 2. copy this file onto server
___ 3. create /tmp/tcpwrapper directory on available server and move Tcpwrapper file there
___ 4. use "gunzip" to uncompress the tar file
___ 5. untar the tar file with "tar –xf"
___ 6. change directory to /tmp/tcpwrapper/tcp_wrappers_7.6
___ 7. Edit the Makefile:
    a. vi Makefile
    b. read the first 30 lines
    c. go to line 73 (note line numbers may change with different versions)
    d. uncomment line "REAL_DAEMON_DIR=/etc…" and change /etc… to /usr/old_bin
    e. go to line 152 and make the line read "LIBS=-lnsl RANLIB=echo ARFLAGS=rv AUX_OBJ=setenv.o\"
    f. make the Tcpwrapper executables with "make hpux"
    g. create directory /opt/tcpwrapper
    h. Move the /tmp/tcpwrapper contents to /opt/tcpwrapper
    i. Add /opt/tcpwrapper to the path environment variable
___ 8. create the /usr/old_bin directory and set ownership to bin with 555 permissions
___ 9. enable the man pages by copying the applicable files as follows:
    a. cp /opt/tcpwrapper/tcp_wrappers_7.6/*.3 to /usr/share/man/man3
    b. cp /opt/tcpwrapper/tcp_wrappers_7.6/*.5 to /usr/share/man/man5
    c. cp /opt/tcpwrapper/tcp_wrappers_7.6/*.8 to /usr/share/man/man8
___ 10. you can now view the man pages for tcpd, tcpdchk, tcpdmatch, hosts_access and hosts_options

___ 11. We will do things the easy way and not touch the configuration files for inet, but instead replace binaries with tcpd.
   a. Cp /usr/lbin/rlogind to /usr/old_bin/rlogind
   b. Cp /usr/lbin/telnetd to /usr/old_bin/telnetd
   c. Cp /usr/lbin/rlogind to /usr/old_bin/rlogind
   d. Now copy the recently created tcpd binary to each of the binaries just copied from /usr/lbin (ie. cp tcpd /usr/lbin/ftpd)

___ 12. test the tcpwrapper configuration for errors with ./tcpdchk

___ 13. Login banners are needed to preserve the banner convention established earlier. Create tcpwrapper banners as follows:
   a. make banner directory /opt/tcpwrapper/tcp_wrappers_7.6/banners
   b. change to the banners directory
   c. copy the banner makefile into the banner directory:
      cp /opt/tcpwrapper/tcp_wrappers_7.6/Banner.Makefile Makefile
   d. vi Makefile and read the top comments and then comment out line 32 (IN = in.)
   e. create a prototype banner file with "vi prototype" and enter the following text:
      WARNING! UNAUTHORIZED ACCESS PROHIBITED!
      Unauthorized users will be prosecuted to the full extent of the law!
   f. create the banner page with "make" command
   g. This will create a banner page for ftpd, telnetd and rlogind in the banners directory with the same name as the process. Note, if this does not happen, recopy the original Banners.Makefile to the banners directory and just change the IN variable to be equal to nothing (delete .in). Rerun the make command.

___ 14. Change directory back to /opt/tcpwrapper/tcp_wrappers_7.6

___ 15. Edit the Makefile and uncomment the following line:
   "#STYLE = -DPROCESS_OPTIONS # Enable language extensions."

___ 16. Re-execute "make hpux" to enable the banner page change

___ 17. Re-test tcpwrappers with ./tcpdchk

___ 18. create "default deny" policy with /etc/hosts.deny file. Tcpwrapper will first check the hosts.allow file and if access is not specifically allowed, the process will then consult hosts.deny and by default deny access.
   a. vi /etc/hosts.deny
   b. add "ALL : ALL" as the only entry and save the file

___ 19. create /etc/hosts.allow file for specific access.
   a. vi /etc/hosts.allow
   b. for access to the local subnet
      telnetd: LOCAL, .local.domain : banners /opt/tcpwrapper/banners
      ftpd: LOCAL, .local.domain : banners /opt/tcpwrapper/banners
      rlogind: LOCAL, .local.domain : banners /opt/tcpwrappers/banners
   c. Other formats can be used depending on the security desired. Check the man pages and documentation for other options.

4.2.5 Secure Shell (OpenSSH)… instructions provided, but n/a for Lawson

The Lawson application operates in a traditional client-server configuration. A thin-profile client on a workstation or PC establishes a connection to the server located on a different platform. With Lawson, version 7.2.3, the client is a proprietary terminal that connects to the server via telnet. The Lawson client will not function with OpenSSH, but administrators running remote sessions can take advantage of remore command protection. This checklist installs OpenSSH, version 3.4, which released June 26, 2002 and addresses some security issues in previous versions. OpenSSL and Zlib will also be required. OpenSSL is a toolkit implementing Secure Socket Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. Zlib is a compression library providing in-memory compression and decompression functions, including integrity checks of the uncompressed data. The OpenSSH will be configured to work with TCP Wrappers.

___ 1. download OpenSSH from ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/

___ 2. OpenSSH, v. 3.4 requires Zlib and OpenSSL in order to operate. Download from the following HP websites:
http://h21007.www2.hp.com/dspp/tech/tech_TechSoftwareDetailPage_IDX/1,1703,589,00.html - Zlib for HP-UX, v. 1.1.3 (this is the HPUX supplied version)
http://www.openssl.org/source - OpenSSL, v. 0.9.6d

___ 3. Install Zlib
   a. Copy zlib-1.1.4.tar.gz to /tmp
   b. Run gunzip to uncompress the file
   c. tar –xf /tmp/zlib-1.1.4.tar will extract the files from the tar ball
   d. move into the /tmp/zlib-1.1.4 directory and read the README file
   e. at command prompt: ./configure
   f. To compile and run test, enter at command prompt: make test
   g. should see message "*** zlib test ok ***" at end of make test
   h. To install, enter at command prompt: make install
   i. Cleanup /tmp by removing the zlib install files

___ 4. Install openssl
   a. Copy openssl-0.9.6d.tar.gz to /tmp
   b. Run gunzip to uncompress file
   c. Tar –xf /tmp/openssl-0.9.6d.tar will extract the files from the tar ball
   d. Move into the /tmp/openssl-0.9.6d directory and read the INSTALL file
   e. At command prompt: ./config
   f. To check that it guessed the correct OS, at command prompt: ./config –t
   g. Should get "Operating system: 9000/800-hp-hpux11" in first line
   h. At command prompt: make
   i. At command prompt: make test
   j. At command prompt: make install
   k. Cleanup /tmp by removing the openssl install files

___ 5. Install OpenSSH (configure for tcp_wrappers plus defaults)
   a. Copy openssh-3.4p1.tar.gz to /tmp
   b. Run gunzip to uncompress file

c. Tar –xf /tmp/openssh-3.4p1.tar will extract the files from the tar ball
d. Move into the /tmp/openssh-3.4p1 directory and read the INSTALL file
e. At command prompt:
./configure –tcp_wrappers=/opt/tcpwrapper –libwrap=/opt/tcpwrapper/libwrap.a
f. At command prompt: make
g. Create sshd user: useradd sshd
h. At command prompt: make install - this will install the binaries and man pages required for OpenSSH.

___ 6. Move appropriate binaries into place (client and host)
a. Create a directory /usr/rbin and copy rsh, rlogin, rcp and ftp there. This will give you a place to store the original binaries in base you have to recover them quickly.
b. Create symbolic links to the SSH binaries. The Lawson users will not require rcp, rlogin or rsh. The OpenSSH binaries will prevent unauthorized use of the programs.
ln –s /usr/local/bin/ssh /usr/bin/rsh
ln –s /usr/local/bin/ssh /usr/bin/rlogin
ln –s /usr/local/bin/ssh /usr/bin/rcp
c. This configuration will also use the secure FTP binary provided with OpenSSH.
ln –s /usr/local/bin/sftp /usr/bin/ftp

___ 7. Set the boot script to start the sshd daemon with reboots
cp /tmp/openssh-3.4p1/contrib/hpux/sshd.rc to /sbin/init.d/sshd.rc
ln –s /sbin/rc2.d/S505sshd /sbin/init.d/sshd.rc
ln –s /sbin/rc1.d/K505sshd /sbin/init.d/sshd.rc

___ 8. Generate keys for user authentication. This guide will use RSA key pairs for version 1 of the protocol. The secure shell can handle several different authentication methods, so feel free to analyze the pros and cons and choose the best one for your environment.
a. Each user (admin users for the Lawson server) run ssh-keygen to generate the key pairs. The host key can also be updated using ssh-keygen. An example of the key pair generation for user sshtest is shown for clarification.
/usr/local/bin/ssh-keygen –t rsa1
Generating public/private rsa1 key pair.
Enter file in which to save the key (/home/sshtest/.ssh/identity):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sshtest/.ssh/identity.
Your public key has been saved in /home/sshtest/.ssh/identity.pub.
The key fingerprint is:
7d:8a:85:fd:be:f1:2e:bb:52:aa:1f:4e:7d:13:f3:35 sshtest@sfohp2
b. Copy the public key, found in $HOME/.ssh/identity.pub, to all remote hosts to which the user will login. The file must be placed in $HOME/.ssh/authorized_keys.
c. Update the /etc/hosts.allow file for OpenSSH:
Add this line: sshd:ALL

4.2.6 File Transfer Protocol (FTP)

The server will support FTP, but not trivial FTP (TFTP) or anonymous FTP.

___ 1. verify that ftp logging was enabled during the inetd services security checks
___ 2. Deny ftp access to root, guest and all other accounts not specifically requiring the service by adding the user names to the /etc/ftpd/ftpusers file
___ 3. The anonymous FTP service requires configuration and will not be performed. Verify that there is no ftp user in /etc/passwd and the tftp service is commented out in inetd.conf
___ 4. ftp will have been replaced with sftp (secure ftp) from the previous steps to install OpenSSH

4.2.7 Sendmail (SMTP)

This server does not require the Sendmail to operate as a daemon/server. Sendmail configuration will allow outbound mail and run a root cron job to flush any queued mail. The HP delivered Sendmail will be retained. Modifications will be made to prevent the daemon from starting on a reboot and a cron entry will be made to process the mail queue on a timely basis. The version is 8.9.3, which has been heavily tested and security patched.

___ 1. Modify HP Sendmail that was installed with the operating system to prevent daemon launch with reboot.
   a. Shutdown the Sendmail daemon if running: /usr/sbin/sendmail stop
   b. Rename the run level script for Sendmail to prevent Daemon startup with a reboot:
   "mv /sbin/rc2.d/S540sendmail /sbin/rc2.d/NS540sendmail"
___ 2. Ensure that all security related sendmail patches are in place. Reference patching
___ 3. Modify the sendmail.cf lines file to close some potential security issues:
   a. Modify the received format line: it will be very similar to this
   HReceived: $?sfrom $s $.$?_($?s$|from $.$_) $.by $j **($v/$Z)**$?r with r. id i?u for $u; $|; $.$b

   $j is the host name
   $v is the version/patch
   $Z is the version number alone

   Removing the ($v/$Z) part will remove the patch and version information from embedding in mail
   b. Modify the smtp greeting message to remove the patch and version information:
   O SmtpGreetingMessage=$j Sendmail **$v/$Z**; $b

$j - fully qualified domain name (required)
$v - current version of sendmail
$Z - The version of the configuration file you're using
$b - current date time

Remove the $v/$Z

c. Disable the vrfy command of the Sendmail program. Add the following line to the Sendmail.cf file: "O PrivacyOptions=novrfy"

___ 4. Modify the Sendmail script in /sbin/init.d to reset the daemon function to not allow listening on port 25. Port 25 is the port that Sendmail will listen on for mail requests. Make the following change
/usr/sbin/sendmail -bd -q30m && echo "sendmail" - this is the original line the –bd option starts the Sendmail daemon and listens on port 25
/usr/sbin/sendmail -q30m && echo "sendmail" - this new line process the mail queue every 30 minutes, but no longer listens on port 25

___ 5. Make sure and make changes to /etc/mail/aliases to ensure mail sent to the root mailbox that may include system related alerts get forwarded to an active mailbox. Run the newaliases command to update the /etc/mail/aliases.db file.

4.3 Network Control

This guide will not provide guidance towards tuning routers and other network equipment not associated with the server. Several security measures related to network access have already been covered in earlier steps. One other key to network security is to keep all of the network devices in locked and secure locations. This should also include the cabling.

4.3.1 Network Time Protocol (NTP)

The outlined NTP configuration assumes that three secure and internet connected servers are configured as central time servers, that they synch with different internet time servers, and that they peer with each other. A list of publicly available stratum 2 servers, with administrative contact information, can be found at http://www.ntp.org/ . This configuration uses the latest release of NTP version 3 that is delivered as part of the general operating system for HP-UX 11.00. NTP is not configured by default with a fresh installation of the Installation. This server is assumed to function as an internal time server, which will peer off central time servers and other internal time servers as required. A psuedo clock will be configured. Security settings ignore all synch and administrative requests, witch exceptions for the class C subnet defined. An entry is also in place to protect against spoofed messages from the 127.0.0.1 ip address. It is assumed with this configuration that firewall protection will prevent external time sources from injecting NTP traffic into the LAN. The server will run the ntpdate command upon a reboot and will not broadcast NTP traffic. Clients of this server will need to pull NTP information. To configure NTP, complete the following steps:

___ 1. Create the NTP configuration file at /etc/ntp.conf

```
# NTP configuration file
driftfile       /var/adm/ntp.drift      # not using default in /etc

# psuedo clock
server  127.127.1.1
fudge   127.127.1.1 stratum 8

# central time servers
server  xxx.xxx.xxx.xxx             # comment point about server
server  xxx.xxx.xxx.xxx             # comment point about server
server  xxx.xxx.xxx.xxx             # comment point about server

# peer servers
peer    xxx.xxx.xxx.xxx             # comment
peer    xxx.xxx.xxx.xxx             # comment
peer    xxx.xxx.xxx.xxx             # comment

# security
restrict        default                                 ignore

restrict        xxx.xxx.xxx.0 mask 255.255.255.0    nomodify
restrict        127.0.0.1                           nomodify
```

___ 2. Edit the /etc/rc.config.d/netdaemons file, changing the xntp configuration portion as follows:

```
#####################################
# xntp configuration.  See xntpd(1m) #
#####################################
#
#  Time synchronization daemon
#
# NTPDATE_SERVER: name of trusted timeserver to synchronize with at
#boot
# (default is rootserver for diskess clients)
# XNTPD:        Set to 1 to start xntpd (0 to not run xntpd)
# XNTPD_ARGS:  command line arguments for xntpd
#
# Also, see the /etc/ntp.conf and /etc/ntp.keys file for additional
# configuration.
#
export NTPDATE_SERVER="<timeserver 1> <timeserver 2>"
export XNTPD=1
```

___ 3. The xntp process will run as a daemon after the next system reboot.

4.3.2 Network Parameters (nddconf)

The /etc/rc.config.d/nddconf file is a configuration file that set various settings to network parameters that can improve a systems hardness to attacks. The ndd binary allows settings to be examined or modified, but changes made with ndd are lost after a reboot unless the settings are placed within the nddconf file.

___ 1. "ndd –h sup" will generate a list of the HP supported parameters. Swap unsup for sup and you will get the unsupported parameters.
___ 2. "ndd –h <param>" will give you specific information for a parameter
___ 3. Stop ip forwarding, forwarding with source route options and forwarding of ip directed broadcast. Add the following lines to nddconf, which assumes no entry exists yet.

```
TRANSPORT_NAME[0]=ip
NDD_NAME[0]=ip_forwarding
NDD_VALUE[0]=0
TRANSPORT_NAME[1]=ip
NDD_NAME[1]=ip_forward_src_routed
NDD_VALUE[1]=0
TRANSPORT_NAME[2]=ip
NDD_NAME[2]=ip_forward_directed_broadcast
NDD_VALUE[2]=0
```

___ 4. run "ndd –c" to set parameters defined in nddconf
___ 5. At reboot the nddconf file will be re-read, so settings will remain intact

4.4 File System Access Control

4.4.1 NFS File System Sharing

NFS is not required on this server and will be secured. No file system will need to be shared across the network.

___ 1. edit the /etc/rc.config.d/nfsconf file and set the "NFS_CLIENT" and "NFS_SERVER" variables to 0
___ 2. in /sbin/rc2.d, move the link for starting nfs client to a link that does not start with "S": "mv S430nfs.client NS430nfs.client"
___ 3. in /sbin/rc3.d, move the link for starting nfs server to a link that does not start with "S": "mv S100nfs.server NS100nfs.server"

4.4.2 Umask

The umask sets the value of the file mode creation mask or. The mask affects the initial value of the file mode (permission) bits for subsequently created files. Configure the system so that the boot run levels and /etc/profile register a standard umask of 022. The 022 umask will also be the standard for any user accounts added to the server.

___ 1. add the 022 umask to the end of /etc/profile and with:

a. /usr/bin/echo "umask 022" >> /etc/profile
b. /usr/bin/echo "umask 022" >> /etc/skel/.profile

___ 2. create and run a script that sets the umask for each run level during boot process:
   c. /usr/bin/echo "umask 022" > /sbin/init.d/umask.sh
   d. chmod 744 /sbin/init.d/umask.sh
   e. create a link to /sbin/init.d/umask.sh in each run level directory (/sbin/rc#.d) by changing directory to the desired run level directory and executing: "/usr/bin/ln –s /sbin/init.d/umask.sh S000umask"
   f. Verify that no other link in each run level directory uses "000" for the start sequence to ensure that no other process is started ahead of the umask setting script.

4.4.3 SUID Executables

"Set User ID" (SUID) permission allows unprivileged users the ability to accomplish certain, privileged tasks. SUID enabled programs will execute with the access rights of the owner and not the executing user. One example of a SUID executable is /usr/bin/passwd, which is owned by root, but allows users on the host to change their passwords. With the initial installation, create a list of SUID programs for a baseline. Do not create or set SUID bit on any executable without verification that the code is safe. Follow the below steps to create the baseline list.

___ 1. find / -perm –4000 –type f > /tmp/SUID.inventory and then make a copy of this file in a place where it will not be removed.
___ 2. Rerun step 1 and redirect to a new file
___ 3. run diff command against the two files to check for new SUID programs.
___ 4. File systems can also be mounted with nosuid argument in the /etc/fstab file. Before setting this option, make sure there are no SUID programs that need to be run from that mount point. The nosuid setting will not prevent the creation of nosuid files, but it will disable SUID functionality.
___ 5. The Lawson application runs several SUID programs, so make sure and re-set the baseline SUID listing after installing the Lawson application. Changing or disabling these programs will result in Lawson errors.

4.5 User Access Control

4.5.1 Restricted Shell (rsh)

A restricted shell will be used to control what the Lawson users can access once they have established a telnet session with the Lawson client. This will allow administrators to limit access on the server to the Lawson program and required files only. This security feature is really designed to prevent the "curious" user from inadvertently damaging the server environment. This guide will use the rksh shell.

___ 1. create any user that will require the restrictive shell using /usr/bin/rksh for the shell: useradd –g Lawson –d /home/user –m **–s /usr/bin/rksh** user
___ 2. The user will be unable to cd out of their home directory, but to prevent escaping the restrictive shell, the .profile will need to be modified:
   a. Modify the PATH variable to include only those areas required
   b. Add a sub-directory below PATH that has all of the required binaries and commands for the user to work with Lawson
   c. Test the access with the Lawson client and a normal telnet session
   d. The user should be able to open a session with Lawson, but at the command line will be unable to change directory, unable to change environment variables (SHELL, PATH, etc.), redirect output or perform any command containing /.
___ 3. The rksh can be defeated by experienced hackers, but the normal Lawson user will be prevented from "surfing" the system and creating trouble.

4.5.2 Restricting Remote Access

Users will not be allowed to configure .rhosts or hosts.equiv files that would circumvent password authentication. The OpenSSH secure shell provides additional security related to this, but a cron job will also be put in place that will locate and remove any unauthorized user files of this type.

___ 1. Create a script that can be run from a root owned cron job that will find and remove any .rhost or hosts.equiv files located in /home. An example script is provided in Appendix D.
___ 2. Add the job to the crontab:
   00 02 * * * /script_location > /dev/null 2>&1

4.5.3 Securing Modem Dial-In Access

Users on this server will not be allowed to dial in via any configured modems. If a modem is configured as part of the support scheme on your server, ensure that it gets configured as a dial-out only modem. Make the following changes to ensure that no-one accesses the system across any modem devices.

___ 1. Check the /etc/inittab file and ensure that lines similar to the following are commented out:
   #ttp1:234:respawn:/usr/sbin/getty -h tty0p1 9600
___ 2. run "init q" to have init recheck the inittab without changing the run level.
___ 3. run "ioscan –funC tty" and look for devices with ttydxpx formats
___ 4. Edit /etc/dialups (create if necessary) and add entries for devices found with ioscan. Devices listed in this file require the additional security of both a user password and a dialup password. Typical entry would be: /dev/tty0p0
___ 5. Edit or create /etc/d_passwd file. Entries are required for all of the user shell binaries. Typical entries include the shell and an encrypted password. An example entry is /usr/bin/sh:dpscen80aKWa2:

___ 6. In order to get the dialup password encrypted, create and use the short program found in Appendix F
___ 7. Now a login attempt across that device should result in the following prompts:
Login:
Password:
Dialup password:

4.5.4 Limit Access via X / CDE

By default, X/CDE will send a dtlogin screen to any graphics display that has network connectivity with our host. Hackers can request a login screen with a simple query. As some administrators may want to run X/CDE, we will not remove it entirely, but we will limit access. The steps required to kill X/CDE permanently are also provided.

___ 1. vi or create /etc/dt/config/Xaccess
___ 2. add entries for specific trusted hosts that should be allowed X/CDR access
___ 3. If no one requires X/CDE, then permanently disable it by changing the configuration file that is read by /sbin/init.d/dtlogin.rc at system start.
a. Vi /etc/rc.config.d/desktop
b. Modify line with DESKTOP to be: "DESKTOP=""
c. Save changes
d. Run "/sbin/init.d/dtlogin.rc.stop" to stop the current process

4.6 Lawson Application Control

A Lawson engineer will handle the installation of the application. The standard installation results in a new set of file systems that start with the /lawson mount point. The steps below outline what can be addressed to minimize the possibility of Lawson, or other third party software, from creating unacceptable security holes in your environment. Before attempting any modifications to third party software, contact the vendor and discuss security concerns and request any documentation available. Contact software support, if available, and verify what can be changed without violating support agreements. Security is very important, but if you violate contract terms while chasing security issues you get yourself in trouble.

___ 1. Get a complete list of what is installed at the time of installation. In the case of Lawson, more than just the application is installed. It requires a Cobol based run time environment for version 7.3.3, which is installed under /usr/cobol
___ 2. Run the following to get a list of directories that are world writable at time of installation. DO NOT CHANGE ANYTHING YET! The amount of directories installed will depend on the amount of modules installed for Lawson, but our installation returned a list of over 700 directories.
a. find /lawson –type d –perm 777 > /tmp/lawson_world_dir_list

___ 3. There are also several critical files that have SUID set with root ownership and are also world writable. We must identify these files and ensure that they retain SUID. Run the following to find these executables.
   a. find /lawson –perm –4000 –type f > /tmp/lawson_suid_files
___ 4. Now that we have some details on security issues, call Lawson, or the third party vendor, and start asking questions. In the case of Lawson, they have a document that is internally available that addresses file system and file permissions titled "UNIX File Permissions and Lawson". You will not get this document unless you ask for it, so ask for it! Appendix F shows the document.
___ 5. The document addresses what can and cannot be changed to the file system structure. Almost all of the directories identified in step 2 can have permissions changed to 755 instead of 777. Some can be made even tighter. Change the directory permissions only and do this one directory at a time. Do not try and change permissions recursively, as you will likely break the application. Lawson installs a code set that is over 1 GB and covers hundreds of directories, so a recursive change that causes trouble could be hard to correct.
___ 6. Modify directory permissions and TEST to ensure the application still works
___ 7. Modify file permissions and TEST again.
___ 8. The paper also identifies the executables that must remain SUID root. It does authorize changing the permissions from 4777 to 4755 to close the issue of group and world writable SUID root executables.
___ 9. Modify SUID root executables and TEST one more time.
___ 10. Lawson provides application updates in the form of patches and service paks. Many other third part applications also function in this way. Individual patches will normally address a few files or executables, while the service pak will deal with hundreds of issues. When a service pak is installed, it is routinely installed using an automated script. After a service pak is installed, re-run the permission checks to ensure nothing has been inserted or changed.
___ 11. When lawson users are created on the server, they first require a Unix account. The account needs to be created with the restricted shell configured earlier. The restricted shell will prevent a user from moving through different file systems or accessing permissions unnecessary to Lawson.

4.7 Key File and Log Monitoring (Tripwire)

Tripwire will be installed to monitor key system and log files. The purpose is to notify administrators to unauthorized changes on the system that could indicate an unauthorized access. Tripwire works by creating an initial database of information about files on the system. The database is created prior to connection to a production network in order to ensure a non-compromised snapshot. Tripwire is then run from cron once a day, where it compares the current state of files with parameters in the Tripwire database. All differences found are then reported. We install Tripwire version 1.3.1, Academic Source Release. A commercial version is also available. Pay close attention to these steps, as

special modifications were required for compiling the source code on the HPUX platform.

___ 1. Download the "Academic Source Release" at http://www.tripwire.com/downloads/tripwire_asr/
___ 2. make the /secure/tripwire directory
___ 3. Copy tripwire-1.3.1.tar.gz to the /secure/tripwire directory and uncompress
___ 4. untar the file
___ 5. change to /secure/tripwire/tw_ASR_1.3.1_src directory and read the README file
___ 6. Change the Makefile as follows. The compile for HPUX will struggle otherwise
   a. Set DESTDIR = /secure/tripwire/tw
   b. Set DATADIR = /secure/tripwire/tw/databases
   c. Uncomment the following lines or edit to set them accordingly. Comment out the other lines for these variables

```
LEX = lex
YACC = yacc
SHELL = /bin/sh
CC = cc
CFLAGS = -g -Ae
CPP = $(CC) -E
LDFLAGS = -static
LIBS =
INSTALL = /bin/cp
HOSTNAME = hostname
```

___ 7. cd ./include and make the proper modifications to the config.h file
   a. change the line: #include "../configs/conf-svr4.h" to #include "../configs/conf-hpux.h"
   b. change two additional lines with the new paths:

```
#define CONFIG_PATH     "/usr/local/bin/tw"
#define DATABASE_PATH   "/var/tripwire"
        to
#define CONFIG_PATH     "/secure/tripwire/tw
#define DATABASE_PATH   "/secure/tripwire/tw/databases"
```

___ 8. make the following directories, which will hold the binaries and database after installation
   /secure/tripwire/tw
   /secure/tripwire/tw/databases
___ 9. update a source file siggen.c to reflect HPUX variation:
   a. vi ./src/siggen.c and type: :%s/sigvector/sigvector1/g
   (This is just a vi search & replace command that replaces all occurrences of sigvector with sigvector1)
   b. save changes
___ 10. move back to /secure/tripwire/tw_ASR_1.3.1_src and run make
___ 11. step 12 should error out with a complaint about config.lex.c. Make the following change:

   a. move to the ./src directory and vi config.lex.c
   b. find the line: static void __yy__unused() { main(); }
   c. change it to: static void __yy__unused() { main(0,0); }
   d. save changes and rerun make to generate the binaries

___ 12. test Tripwire: make test
___ 13. perform the installation: make install
___ 14. Copy ./src/tripwire to /secure/tripwire/tw/tripwire
___ 15. Copy ./src/siggen to /secure/tripwire/tw/siggen
___ 16. Copy the man pages to system man pages
   a. cp ./man/*.8 /usr/share/man/man8/
   b. cp ./man/*.5 /usr/share/man/man5/
___ 17. Modify the ../configs/tw.config.hpux to include all files that should be monitored. In addition to the system binaries and programs, you need to communicate with the third party vendor (Lawson) and obtain confirmation of any set-uid programs and key binaries that should be checked. For Lawson add the following:

/Lawson/law/system/profile	R
/Lawson/law/system/univ.cfg	R
/Lawson/law/system/ladb.cfg	R
/Lawson/law/system/lajs.cfg	R
/Lawson/law/system/latm.cfg	R
/Lawson/law/system.security.cfg	R
/etc/Lawson.env	R
/Lawson/gen/bin/*	R

___ 18. Copy the tw.conf.hpux file to the /secure/tripwire/tw directory and rename as tw.config
___ 19. Initialize tripwire with "/secure/tripwire/tripwire –initialize". This will create the tripwire database under a databases directory. Copy the file created (tw.db-testserver) to the /secure/tripwire/tw/databases directory. Ensure that this directory and file are accessible by root only.
___ 20. If this is the last item (as it is here) that requires compiling, completely remove the compiler from the server. Future installations that require compiling should have that operation completed on a separate and isolated server.
___ 21. Create cron job to run tripwire once an evening and send report of results
   a. 15 01 * * * /secure/tripwire/tw/tripwire > /dev/null 2>&1

5 Security Verification Checklist

This section will walk through steps that can be used to verify that the security configuration is operating correctly. Feel free to add additional steps to enhance the verification process.

5.1.1 Test Tcpwrappers

Tcpwrappers was installed to "wrap-around" the vulnerable telnet, ftp and rlogin processes. The inetd.conf file was modified to force any attempt at establishing one of these connections to pass through some filtering to verify authorization. The /etc/hosts.allow and/etc/hosts.deny files have to have been configured to a "default deny policy (which will include an entry for OpenSSH) and then specific allow identification. These steps will verify this configuration for all three services.

___ 1. Check that the /etc/hosts/deny file has the following entry as a minimum to establish default deny authentication:

```
ALL : ALL
```

___ 2. Check that the /etc/hosts.allow file has entries for the services controlled plus the sshd process. The format also ensures that banners are used. Our example assumes granting access to the LOCAL domain. Insert the proper IP information for the xxx.xxx.xxx.xxx.

```
sshd : ALL
telnetd : LOCAL, .domain.com : banners \
/opt/tcpwrapper/tcp_wrappers_7.6/banners
ftpd : LOCAL, .domain.com : banners \
/opt/tcpwrapper/tcp_wrappers_7.6/banners
rlogind : LOCAL, .domain.com : banners \
/opt/tcpwrapper/tcp_wrappers_7.6/banners
```

___ 3. From a host not configured in /etc/hosts.allow, attempt to use telnetd, ftpd, and rlogind. The results should be similar to:

a. For ftp:

```
Connected to testserver.
421 Service not available, remote server has closed connection
ftp>
```

b. For telnet:

```
Trying...
Connected to testserver.
Escape character is '^]'.
Local flow control off
Connection closed by foreign host.
```

c. For rlogin:

```
rcmd: Lost connection
```

___ 4. From a host configured in /etc/hosts.allow, repeat the same attempts for ftp and telnet. This will also confirm the banners configuration for ftp. Note that you will need to make this test from a user that is not part of the lawson group.

a. For ftp:

```
Connected to testserver.
220-WARNING! UNAUTHORIZED ACCESS PROHIBITED!
220-Violators will be prosecuted to the full extent of the law!
```

220 testserver.domain.com FTP server (Version 1.1.214.8 Fri Apr 20 07:27:42 GMT 2001) ready.
Name (testserver:ellist):

b. For rlogin: recall that the inetd.conf file has the "-l" argument for rlogind which will prevent the use of a .rhosts file. The rlogin process should result in a password prompt to gain access along with the tcpwrapper banner.

rlogin testserver
WARNING! UNAUTHORIZED ACCESS PROHIBITED!
Violators will be prosecuted to the full extent of the law!
Password:

c. For telnet: Recall that we have a login banner for telnet and a login banner for tcpwrapper. This shows the result of having both configured. With tcpwrapper, you could remove the telnet banner.

Trying...
Connected to sfohp2.triu.com.
Escape character is '^]'.
WARNING! UNAUTHORIZED ACCESS PROHIBITED!
Violators will be prosecuted to the full extent of the law!
Local flow control on
Telnet TERMINAL-SPEED option ON
WARNING! UNAUTHORIZED ACCESS PROHIBITED!

login:

5.1.2 User Access Security Verification

The following checks verify steps of our guide that were directed at limiting user access for the system.

___ 1. from another host on the network, attempt a telnet to verify the login banner "WARNING! UNAUTHORIZED USE PROHIBITED!" is displayed.

___ 2. Now log-in from a remote location using a Lawson user account. This will open a restricted shell session and we need to verify that the settings prevent movement through unauthorized file systems and opening a different shell.

a. At the command prompt, attempt to cd to /: cd /
The results should match:
"/usr/bin/rsh: cd: The operation is not allowed in a restricted shell."

b. At command prompt, attempt to open a normal ksh session.
The results should match:
/usr/bin/rsh: /usr/bin/ksh: The operation is not allowed in a restricted shell.

___ 3. enter "umask" at command line of user session and confirm that 022 is returned to show that the umask setting holds.

___ 4. Try and rlogin from another host using a lawson user account. The action should be rejected. This is also verified as part of Tcpwrappers.

5.1.3 Access Control Lists (ACLs) Verification

Check that patching information on the server can no longer be retrieved by anything other than a root session on the server itself. Requests from another server and requests from a non-root user on the server will be verified.

___ 1. As root from another host on the network, attempt to gather a list of patch information about CDE on our new server:
"swlist –l product CDE @testserver.domain.com"
if the changes are not working, you will receive information similar to:

```
# Initializing...
# Contacting target "testserver.domain.com"...
#
# Target:  testserver.domain.com:/
#

  CDE               B.11.00       HP-UX CDE User Interface
```

If the changes are working properly, the following is returned:

```
# Initializing...
# Contacting target " testserver.domain.com "...
ERROR:   "testserver.domain.com:/":  You do not have the required permissions
         to select this target.  Check permissions using the "swacl"
         command or see your system administrator for assistance.  Or,
         to manage applications designed and packaged for nonprivileged
         mode, see the "run_as_superuser" option in the "sd" man page.
ERROR:   More information may be found in the daemon logfile on this
         target (default location is
         testserver.domain.com:/var/adm/sw/swagentd.log).
```

___ 2. On the new server from a non-root user shell session, attempt to access patching information with the same commands from step 1. The success and fail criteria are identical, with the successful verification resulting in:

```
# Initializing...
# Contacting target "testserver"...
WARNING: Security access denied to file "//var/adm/sw/products/INDEX".
ERROR:   "testserver:/":  You do not have the required permissions to
         perform this operation.  Check permissions using the "swacl"
         command or see your system administrator for assistance.  Or,
         to manage applications designed and packaged for nonprivileged
         mode, see the "run_as_superuser" option in the "sd" man page.
```

___ 3. View the swagentd daemon log file to verify that the failed attempts are logged at the end of the file. The results should be similar to:

```
* Started list agent on "/" for root@sfohp5.triu.com, pid=6549,
      07/18/02 07:59:48 PDT
WARNING: Security access denied to file "//var/adm/sw/products/INDEX".
ERROR:   The target "/" could not be opened. pid=6549 07/18/02 07:59:48 PDT
* Agent pid=6549 completed.  07/18/02 07:59:48 PDT
```

5.1.4 Inet Services Verification

___ 1. from another host, attempt to finger the new server with "finger @new_server"
The response should be similar to "connect: Connection refused"

___ 2. For a non-root, non-lawson user, create a .rhosts file on our new server in the users home directory and add an entry for a singular remote host and user. No from that remote host, attempt to rlogin as a user would from a trusted system in order to avoid password authentication. This will test the "-l" option appended to the login service in the inetd.conf file. If improperly set, the log-in would be allowed (assuming that it also has the OpenSSH settings properly configured). If properly set, the results look like:
"rcmd: Lost connection"

5.1.5 FTP Verification

Recall that the ftp binary has been replaced with the OpenSSH sftp. Checking ftp will verify part of the OpenSSH installation along with the ftp security settings.

___ 1. Attempt to ftp a file onto the server as root on anther host. This will check the entries in the /etc/ftp/ftpusers file. Root was added to this file and should result in a rejection. This check should be done using settings that would pass the sftp requirements. The session should be rejected with an output to the screen similar to:

```
Connected to testserver.
220-WARNING! UNAUTHORIZED ACCESS PROHIBITED!
220-Violators will be prosecuted to the full extent of the law!
220 testserver.domain.com FTP server (Version 1.1.214.8 Fri Apr
20 07:27:42 GMT 2001) ready.
Name (testserver:ellist):
530 User root access denied...
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

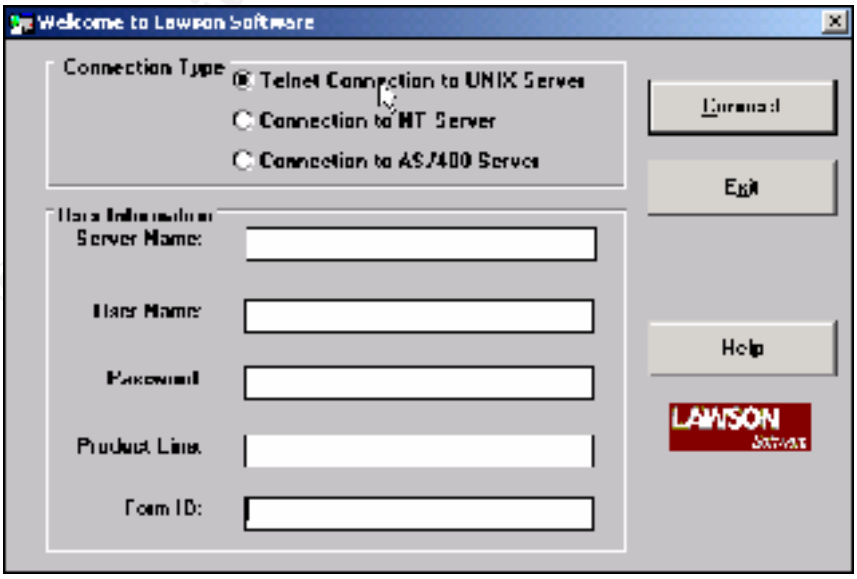
___ 2. Check that an entry is made into the /var/adm/syslog/syslog.log file for the ftp session attempt. The entry should be similar to:

Jul 18 08:46:04 testserver ftpd[7669]: FTP LOGIN REFUSED (bad shell) FROM remotehost [198.135.32.6], root

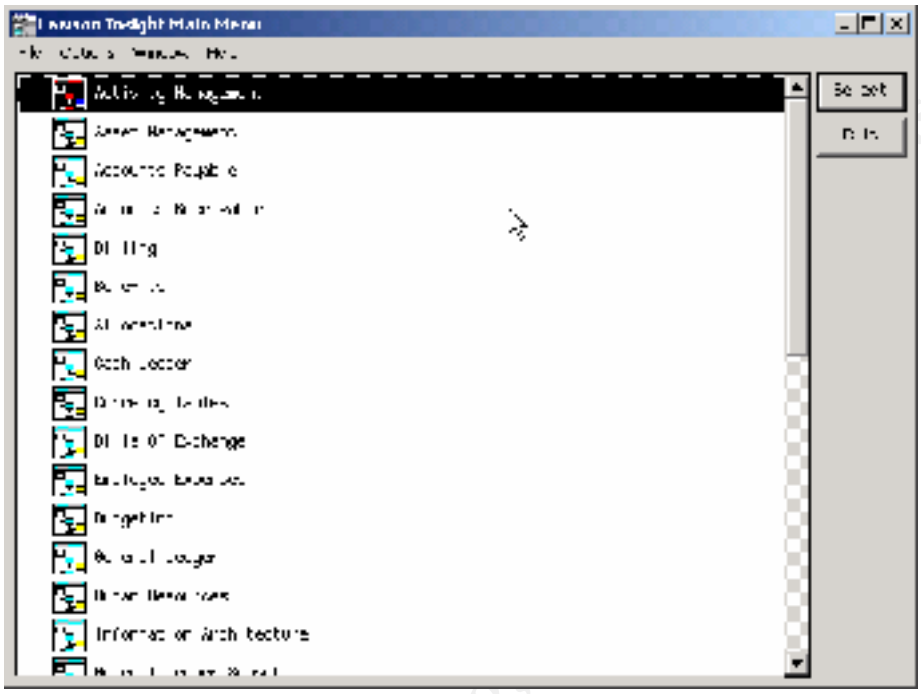
5.1.6 Lawson Alterations Security Verification

Check that the file system permissions for the Lawson based file systems (/lawson) prevent users that are not root or part of the Lawson group from creating, changing or deleting files. Also ensure that the application still functions after changes have been made.

___ 1. log-in as a user that belongs to the group "users" and move into the /lawson directory. Since Lawson requests permissions no more secure than 755, anyone will be able to change to this directory (cd).
___ 2. Attempt to create a file in that directory: touch filename
The resulting error message should read:
"touch: test cannot create"
___ 3. Run "find /lawson –perm –4000 –type f" and verify that no world writable or group writable SUID root executable exist on the server.
___ 4. Attempt to move a file out of a modified directory under /lawson.
   a. mv /lawson/law/prod/INFORMIX /tmp – this will try and move the INFORMIX database configuration file for the "prod" product line into /tmp.
   b. The command should return: "mv: INFORMIX: cannot unlink: Permission denied"
___ 5. attempt to delete the same file: "rm INFORMIX" – this should return a similar error: "rm: INFORMIX not removed. Permission denied"
___ 6. Start a client session and verify that the application establishes a session and that data can be retrieved. Screen shot examples are shown below:
   a. Screen shot of the client log-in screen



b. Screen shot of top-level menu from a successful log-in

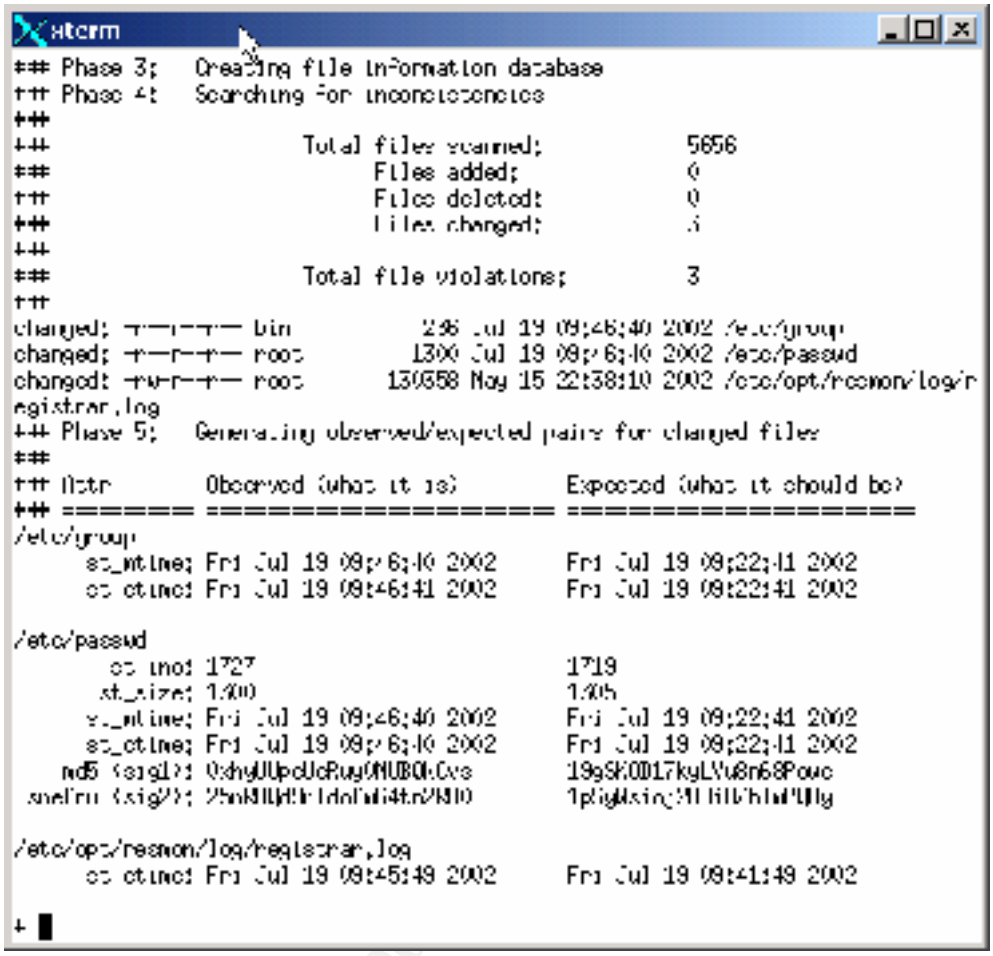


c. Screen shot of a failed session indicating a problem

5.1.7 System Monitoring Verification

When Tripwire is installed and configured with the files the need to be monitored for change, execute a test to confirm that a known change is detected and properly reported. This test will report a change to the /etc/passwd/file.

___ 1. Add the /etc/passwd file name to the Tripwire configuration file. It should be there by default. Change the scan setting to R, as I want to know when a new user is added, no matter how frequent that may be.
___ 2. Add the user "testuser" with the useradd command.
___ 3. Run tripwire. The resulting scan should show something like the following screen shot:



for the password file, Tripwire reports that the inode, size, modified time, change time, md5 and snefru values have all changed. The addition of a new user also touched the group file.

6 Preventative Maintenance, Backups and Monitoring

6.1 Patching

Patch management on the HP-UX server now running the Lawson Insight Financials application suite requires constant vigilance and organization. The system must be patched for both the operating system and Lawson. Operating system patches will take the form of both quarterly patch bundle releases and individual patches. Patches will address hardware changes, security issues, system stability and enhancements or changes to other software applications. One of the first steps to be taken in maintaining a well patched system is to be a member of as many notification groups as necessary to ensure complete coverage of patching updates. A word of caution regarding patches is to carefully read release notes and patch documentation to ensure the patch applies to the system. Irreparable harm can occur if the wrong patch is installed on a system. Here is a list of current groups that an administrator of this system should be signed up with:

- **HP Patch Notification** – to set this up, go to http://www.itrc.com and create a profile if you do not have one. Then follow the links for setting up custom patch notification to all relevant operating systems.
- **HP Security Bulletin Digest** – to receive this notification, use your new login with the IT Resource center and select "more…" from the menu on the left of the main page. Under notifications, select "support information digests". Select all digests that apply. You can also check pervious Security Bulletins from this site.
- **SANS Institute Security Digests** – go to http://www.sans.org/newlook/digests/SAC.htm and sign up for any appropriate notifications. These will often identify security holes ahead of any patch or fix release from HP.
- **Network Computing Security Alert Subscription** – go to http://server2.sans.org/nwcnews and sign up. This provides information released from SANS, CERT, the Global Incident Analysis Center, the National Infrastructure Protection Center, the Department of Defense, Security Portal, Ntbugtraq, Sun, and several other vendors
- **Lawson Security** – go to http://www.topica.com/ and sign up for applicable forums under a search for Lawson. This is a good back door for getting help on specific issues that Lawson may not address directly
- **Lawson support –** if you have support for Lawson, go to http://support.lawson.com and register for patch notifications under Interaction Center – Email Subscription Service menu.

6.1.1 HP-UX Quarterly Patching

HP typically releases a new support plus version every quarter during the year. The patch bundles follow a new format starting with September, 2001 release. Hardware enablement patches are found in the HWE1100 bundle and are required for new system installs and add-on hardware. All stable, defect correcting patches for core HP-UX, graphics and networking areas are on the QPK1100 bundle. The General Release (GR) bundle that used to be part of the quarterly release has been rolled into the QPK1100 bundle. The patch bundles and diagnostic tools contained on the cdrom can be downloaded off of the web or requested on cdrom for servers with current support contracts. The patch bundles tend to be very large, making the cdrom an attractive option. Follow the following steps to install the applicable patches:

___ 1. insert the support plus cd into the dvd-rom
___ 2. mount the cdrom with: /usr/sbin/mount <device file> /cdrom
___ 3. change directory to /cdrom
___ 4. read any applicable README files
___ 5. install the QPK and HWE patch bundles if applicable:

a. **swinstall –s ./QPK1100** – this will open an interactive software install session. Use the interactive option to have better control over the install
b. **swinstall –s ./HWE1100** – to start another interactive install session
c. NOTE: a reboot will most likely occur between each bundle install, requiring another cdrom mount to perform the next install
d. Swinstall –s ./DIAGNSOTICS/B.11.00 to install the latest OnLine diagnostic and EMS monitoring software.

6.1.2 Individual Patching

Patches addressing specific security issues can be installed one at a time or, if they are HP released patches, can be grouped into depots for installing in sets. Patches can also require manual editing of files or recompiling. Each patch will have to be closely analyzed before application, and should always be installed on a non-production machine to allow for system testing and verification. If the patch is an individual patch from HP:

___ 1. Copy the patch to a suitable holding point on the server
___ 2. unshar the patch with: sh <filename>
___ 3. Read the text document, paying special attention to the reboot required information.
___ 4. install the patch: swinstall –x autoreboot=true –x patch_match_target=true –s <filepath.depot>
___ 5. the "x" options in step 4 allow for unattended installations. They do not automatically reboot the server unless the patch requires it.

If the patch is not of HP design, the swinstall utility will most likely not apply. Follow patch guidance for installation, ensuring that proper testing and verification is completed prior to install on a production system.

6.2 Backups

Backups are a critical to system security. A solid backup program will allow administrators to not only recover from a destructive incident, but also assist in determining what was damaged and possibly help in any attacker prosecution. This guide will focus on two different areas. First is the recovery backup, which is an image of the root volume group and will allow a server to be quickly rebuilt. Second is file and data backups, which will backup all database files, raw and file system devices.

6.2.1 Recovery Backup (Ignite Tape)

HPUX provides a utility for creating recovery tapes, henceforth referred to as ignite tapes. The utility is delivered as part of the latest HP-UX operating system. If using older versions of HP-UX, the utility can be downloaded from the HP web-site http://www.software.hp.com/products/IUX/index.html. Ignite-UX provides the make_recovery binary, which can be used with a standard shell script to create ignite recovery tapes. Use a cron job run as root to run the script at a preset interval. The

minimum recommendation is weekly. With weekly execution, have 5 sets of recover tapes that get rotated. The result will be a minimum of one months worth of weekly ignite recovery tapes, all but one of which should be stored off-site.

___ 1. download the software and stage in /tmp on the server
___ 2. use swinstall to install: swinstall –s /tmp/ignite11-11.00 - change the source file for the appropriate version
___ 3. create a recovery script. Refer to Appendix C for an example currently used for some production system recovery tapes
___ 4. create a cron job to run the script once a week. You may also want to create a reminder to ensure tapes are loaded into the tape drive as required.

6.2.2 Files, Data, and Device Backups

The importance of critical data backups can not be under emphasized. This guide will not go into the details of backup design or operation. This guide recommends the use of some enterprise quality software for automating and scheduling backups. The detailed reporting, ease of use and ability to perform on-line backups for databases are just some of the features typically found in this type of third party software. Whatever method is chosen, it must not only back data up, but also be restorable. The only way to verify restorability is to perform a complete test.

6.3 Periodic System Audits

Audits should be performed on a quarterly basis and check for security problems across the entire enterprise. This guide will only list steps to be performed against the server we have created. Several tools will be used to help automate the process and make the checks as comprehensive as possible. John the Ripper, Nmap and TARA will form the nucleus of the quarterly audit. Ensure that audit results are stored securely and not retained permanently. Use the results to correct problems, make a high level report to the proper people, delete the results and get ready to retest next quarter. Please use a unique host for running audit applications and not the one we have just installed. Always ensure that necessary permission for the audit is obtained prior to start.

6.3.1 John the Ripper

John the Ripper (JTR) is a fast password cracker, currently available for many flavors of Unix, DOS, Win32, and BeOS. Its primary purpose is to detect weak Unix passwords, but a number of other hash types are supported as well. This guide installs version 1.6 on the remote host used to run audits.

___ 22. create a new file system in a non-root volume group of 500 MB and mount on a new directory /secure and change permissions to 700 with root ownership
___ 23. download the application: http://www.openwall.com/john/
___ 24. place the file in /secure

___ 25. uncompress with gunzip and untar with tar –x
___ 26. move into /secure/john-1.6 and read the README file
___ 27. move into ./src directory and run make. Select the proper file for the server OS
___ 28. enter: make SYSTEM_selected (make hpux-pa-risc-cc). This will place all necessary files to run JTR in /secure/john-1.6/run
___ 29. create directory /secure/JTR and copy all files from run here. Permissions for root only (600)
___ 30. Recursively remove /secure/john-1.6
___ 31. You can download different dictionaries from ftp://ftp.cerias.purdue.edu/pub/dict
___ 32. Modify john.ini to change how JTR runs
___ 33. IMPORTANT: Before running any scans with JTR, ensure proper permissions have been obtained for the scan, as some of the checks could result in some error generations.
___ 34. Copy password file from the system you want to scan
___ 35. Run a scan. Cracked passwords will be in the john.pot file
/secure/JTR/john –wordfile:password.1st –rules /secure/JTR/passwdfile
___ 36. Make sure and remove any files holding cracked passwords as soon as possible. DO NOT RETAIN THESE!

6.3.2 Nmap

Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap, version 2.54BETA37, is installed with this guide. Please note that it is recommended that a unique host be used to run Nmap and not the server we have created. Nmap will be run from the remote host and used to scan not only the new server, but also other hosts on the network.

___ 1. Download Nmap: http://www.insecure.org/nmap/nmap_download.html
___ 2. Copy the file to /secure on the host to be used for running security audits
___ 3. uncompress the file with gunzip and untar with tar –x
___ 4. move into /secure/nmap-2.54BETA37
___ 5. run ./configure
___ 6. run make
___ 7. run make install
___ 8. The nmap binary is installed by default in /usr/local/bin/nmap… read the man page for nmap for guidance and examples.
___ 9. run "/usr/local/bin/nmap –h" to get command summary
___ 10. IMPORTANT: Before running any scans with Nmap, ensure proper permissions have been obtained for the scan, as some of the checks could result in some error generations.

___ 11. A sample output of an nmap default scan is provided in Appendix E. The host scanned has a default installation of HP-UX 11i without any specific security adjustments. The command run was:
/usr/local/bin/nmap –sS –sU –sR –oN /tmp/host_nmap_scan host.domain.com

6.3.3 SARA (Security Auditors Research Assistant)

The Security Auditor's Research Assistant (SARA) is a third generation Unix-based security analysis tool that is based on the Security Administrator's Tool for Analyzing Networks (SATAN). The release to be installed is version 3.6.2, which has been released in 2002.

___ 1. Download SARA from http://www-arc.com/sara/index.shtml
___ 2. Copy SARA to the /secure directory to the host running security audits
___ 3. uncompress with gunzip and untar with tar –x
___ 4. move into the /secure/sara-3.6.2 directory and read the README file and INSTALL file
___ 5. run ./configure to create the makefile
___ 6. run make. During the install, the process will check for items such as Samba and web servers. If they are not found, that portions of the install will be skipped. This is normal. If these components are added at a later date, do not forget to re-install SARA.
___ 7. SARA needs to be run with a web browser enabled. Netscape should be installed on the host running Sara.
___ 8. SARA can operate with Nmap. To launch SARA with Nmap enabled, run "./sara –n"
___ 9. IMPORTANT: Before running any scans with SARA, ensure proper permissions have been obtained for the scan, as some of the checks could result in some error generations.
___ 10. Run scans based on audit requirements

7 Appendix A: References

1. Garfinkel, Simon & Spafford, Gene. Practical UNIX & Internet Security. Cambridge: O'Reilly and Associates, Inc, 1996.

2. Poniatowski, Marty. HP-UX 11.x System Administration "How To" Book. Upper Saddle River: Prentice Hall PTR, 1999.

3. Campione, Jeff. "Solaris 8 Installation Checklist." *SANS Institute:* http://www.sans.org/y2k/practical/Jeff_Campione_GCUX.htm

4. Schmidt, Della. "HP-UX 11.0 Installation Checklist." *SANS Institute:* http://www.giac.org/practical/Della_Schmidt_GCUX.doc

5. Evanoff, Michael. "Hardening the IRIX Operating System." *SANS Institute:* http://www.giac.org/practical/michael_evanoff_gcux.doc

6. Salas, Fernando Espinoza. "Securing HP-UX Services." SANS Institute: http://rr.sans.org/unix/sec_HPUX.php

7. Hewlett Packard Education Services. Practical Unix and Network Security, version C.00. Mountain View: Hewlett Packard Company, 2000.

8. The Sendmail Consortium. "Sendmail 8.12.5". http://www.sendmail.org

9. IT Resource Center Forums. Hewlett Packard Company: http://forums.itrc.hp.com/cm

10. The OpenBSD Project. "OpenSSH: Portable OpenSSH." http://www.openssh.com/portable.html

11. Tripwire Academic Source Release 1.3.1 for Unix. User Manual. Tripwire Security Systems, Inc., 1999.

12. Lawson Support Center. "UNIX File Permissions and Lawson". Lawson Software., 1997.

13. Advanced Research Corporation.. "SARA 3.6.2". http://www-arc.com/sara/index.shtml .

14. "Nmap 2.54 BETA". http://www.insecure.org/nmap/

15. Openwall Project. "John The Ripper password cracker." http://www.openwall.com/john/

8 Appendix B: HP-UX 11.00 Security Patch List

This patch list is taken from the following web-site and was current as of May 22, 2002. The list is a complete listing of all vulnerabilities with appropriate patch information and covers all HP operating systems. I have clipped the information relevant to HP-UX 11.00.

http://us-support3.external.hp.com/cki/bin/doc.pl/sid=b7c9d0f303e47d64aa/screen=ckiSecurityBulletin/?docId=PATCHMATRIX

```
s800 11.00:PHCO_21534 s700_800 11.00 patch for shutdown(1M)
           PHCO_22665 s700_800 11.00 kermit(1) patch
           PHCO_22766 s700_800 11.00 cu(1) cumulative patch
           PHCO_22957 s700_800 11.00 auto_parms/set_parms
           PHCO_23088 s700_800 11.00 man(1) patch
           PHCO_23117 s700_800 11.00 bdf(1M) cumulative patch
           PHCO_23118 s700_800 11.00 df(1M) cumulative patch
           PHCO_24702 s700_800 11.00 cumulative crontab/at/cron patch
           PHCO_25110 s700_800 11.00 lpspool subsystem cumulative patch
           PHCO_25342 s700_800 11.00 Kernel configuration commands patch
           PHCO_25527 s700_800 11.00 libpam and libpam_unix cumulative patch
           PHCO_25590 s700_800 11.00 login(1) cumulative patch
           PHCO_25707 s700_800 11.00 libc cumulative patch
           PHCO_25875 s700_800 11.00 Software Distributor (SD) Cumulative Patch
           PHCO_26020 s700_800 11.00 top(1) cumulative patch
           PHCO_26235 s700_800 11.00 cumulative newgrp(1) patch
           PHKL_22932 s700_800 11.00 ufs(hfs) deadlock causes the system hang
           PHKL_26059 s700_800 11.00 syscall, signal, umask cumulative patch
           PHKL_26800 s700_800 11.00 Probe,IDDS,PM,VM,PA-8700,asyncio,T600,Hang
           PHNE_16295 s700_800 11.00 vacation patch.
           PHNE_17949 s700_800 11.00 Domain Management (DESMS B.01.12)
           PHNE_18017 s700_800 11.00 Domain Management (DESMS-NS B.01.11)
           PHNE_21835 s700_800 11.00 inetd(1M) cumulative patch
           PHNE_23003 s700_800 11.00 r-commands cumulative patch
           PHNE_23274 s700_800 11.00 Bind 4.9.7 components
           PHNE_23697 s700_800 11.00 NTP timeservices upgrade plus utilities
           PHNE_23949 s700_800 11.00 ftpd(1M) and ftp(1) patch
           PHNE_24164 s700_800 11.X CIFS/9000 Server A.01.06 Cumulative Patch
           PHNE_24419 s700_800 11.00 sendmail(1m) 8.9.3 patch
           PHNE_25626 s700_800 11.00 ONC/NFS General Release/Performance Patch
           PHNE_26771 s700_800 11.00 cumulative ARPA Transport patch
           PHSS_16649 s700_800 11.00 Receiver Services October 1998 Patch
           PHSS_17483 s700_800 11.00 MC/LockManager A.11.05 (English) Patch
           PHSS_17484 s700_800 11.00 MC/LockManager A.11.05 (Japanese) Patch
           PHSS_17496 s700_800 11.00 Predictive C.11.0[0,a-m] cumulative patch
           PHSS_17581 s700_800 11.00 MC ServiceGuard 11.05 Cumulative Patch
           PHSS_21326 s700_800 11.00 OV OB2.55 patch - DA packet
           PHSS_21637 s700_800 11.00 OV OB2.55 patch - WindowsNT packet
           PHSS_22678 s700_800 11.X Continental Clusters A.02.00
           PHSS_23104 s700_800 11.00 OV OB3.00 patch - CORE packet
           PHSS_23266 s700_800 11.00 Support Tool Manager A.21.00 A.21.05
           PHSS_23269 s700_800 11.00 Support Tool Manager A.22.00 Patch
           PHSS_24424 s700_800 11.00 OV OB3.10 patch - CORE packet
           PHSS_24608 s700_800 11.00 AudioSubsystem July 2001 Periodic Patch
           PHSS_24798 s700_800 11.00 OV NNM6.1 Consolidated Patch 4
           PHSS_24864 s700_800 11.X PRM C.01.08.2 Cumulative Patch
           PHSS_25743 s700_800 11.X OV NNM6.2 Consolidated Patch 2
           PHSS_25820 s700_800 11.X OV OB3.50 patch - CORE packet
```

```
PHSS_25843 s700_800 11.00 Support Tool Manager Patch A.24.00
PHSS_26138 s700_800 11.X OV EMANATE14.2 Agent Consolidated Patch
PHSS_26338 s700_800 11.X MC/ServiceGuard and SG-OPS Edition A.11.09
PHSS_26490 s700_800 11.00 CDE Runtime Periodic Patch
PHSS_26909 s700_800 11.00 OV ECS3.00 Intermediate patch April 2002
PHSS_26919 s700_800 11.00 OV NNM6.1 pmd/ovtrapd fixes
PHSS_27069 s700_800 11.X OV NNM6.2 xnmloadmib loading faulty mib
```

9 Appendix C: Example Script for Creating Ignite Tape

```
#!/bin/ksh
#####################################################################
# Script: Script to Create Ignite Recovery Tapes
#####################################################################
# Variables
#
MSTRTIME=`date`                                  # Save date
TMSP=`date '+%m-%d-%y'`                          # Save date/time for log file
HOST=`hostname`                                  # Save hostname
HWPATH=`ioscan -funC tape | grep HP | awk '{print $3}'` # HP tape hardware path
HP_TAPE=`lssf /dev/rmt/*mn | grep "$HWPATH" | awk '{print $20}'`  # Tape device file
HP_MAKER="/opt/ignite/bin/make_recovery -A -v -d"      # HP make_recovery command
HP_LOGR="/usr/bin/logger"                        # HP logger command
HP_cpr="/usr/bin/cp -Rp "                        # HP cp command

# Begin Code
#
TAPED=${HP_TAPE}
#
# Check to see if a tape is in the drive
#
mt -t ${TAPED} rewind
tapecc=$?
if [[ ${tapecc} != 0 ]]; then
   $HP_LOGR "No DDS tape found in {$HOST}: Ignite failed"
fi
#
# Check the host and generate the ignite/ux tape
clear
echo "HP Ignite/UX Recovery Tape Creation started on host: ${HOST}"
echo "This process will take approximately 30-45 minutes."
echo "  Command issued: ${HP_MAKER} ${TAPED} -t "Recovery tape created from system:${HOST}
on ${TMSP}""
echo

${HP_LOGR} "Ignite/UX Recovery Tape Creation started on host: ${HOST}"

# generate the tape for the HP. The following command also adds header information that
# identifies the date of the ignite tape run and the host name.

${HP_MAKER} ${TAPED} -t "Recovery tape created from system:${HOST} on ${TMSP}"
MAKER_CC=$?
#
# Check for return code and send email message
#
if [[ ${MAKER_CC} = 0 ]]; then
  ${HP_LOGR} "Ignite UX Tape Creation completed on host: ${HOST}"
  mt -f ${TAPED} offl
elif [[ ${MAKER_CC} != 0 ]]; then
  ${HP_LOGR} "Ignite UX Tape Creation failed on host: ${HOST}"
fi
#
# End of script
```

10 Appendix D: Script for Removing Improper User files

```
#!/bin/ksh
# Script to search and destroy all .rhosts and hosts.equiv files

PATH=/usr/bin

# find all of the user accounts home directories by scanning the passwd file
# then perform a search loop to check for both .rhosts and hosts.equiv files.
# if any are found, place a log entry in the syslog and remove the file

for user in $(cat /etc/passwd | awk -F: 'length($6) > 0 {print $6}' | sort -u)
do
      [[ -f $user/.rhosts ]] && /usr/bin/logger "Deleting .rhosts file in $user"
      rm -f $user/.rhosts
      [[ -f $user/hosts.equiv ]] && /usr/bin/logger "Deleting hosts.equiv file in $user"
      rm -f $user/hosts.equiv
done

#end script
```

11 Appendix E: Nmap Scan Output

The following output represents the results of an Nmap scan set to check TCP, UDP and RPC service types. The remote host scanned was installed with the latest version of HP-UX 11i. No significant attempts were made to tighten security prior to running this scan. Due to the size of the report, only portions are shown here.

```
# nmap (V. 2.54BETA37) scan initiated Tue Jul 16 09:58:42 2002 as: /usr/local/bi
n/nmap -sS -sU -sR -oN /tmp/nmap_xxx.1 host.domain.com
Interesting ports on host.domain.com (xxx.xxx.xxx.xxx):
(The 1601 ports scanned but not shown below are in state: filtered)
Port       State       Service (RPC)
1/udp      closed      tcpmux
2/udp      closed      compressnet
3/udp      closed      compressnet
4/udp      closed      unknown
5/udp      closed      rje
6/udp      closed      unknown
7/udp      open        echo
8/udp      closed      unknown
9/udp      open        discard
10/udp     closed      unknown
11/udp     closed      systat
12/udp     closed      unknown
13/udp     open        daytime
14/udp     closed      unknown
15/udp     closed      unknown
16/udp     closed      unknown
17/udp     closed      qotd
18/udp     closed      msp
19/udp     open        chargen
20/udp     closed      ftp-data
21/udp     closed      ftp
22/udp     closed      ssh
.
.

32786/udp  closed      sometimes-rpc26
32787/udp  closed      sometimes-rpc28
39213/udp  closed      sygatefw
45000/udp  closed      ciscopop
47557/udp  closed      dbbrowse
54321/udp  closed      bo2k

# Nmap run completed at Tue Jul 16 10:06:50 2002 -- 1 IP address (1 host up) sca
nned in 488 seconds
```

12 Appendix F: Encryption Program for Dialup Passwords

```
/*The following should be compiled with a C compiler as something like dialupadd.c.
* so compile with: cc dialupadd.c –o dialupadd
*After compiling, the program can be run as: “ ./dialupadd >> /etc/d_passwd” */

#  include <stdio.h>
main()
{
char shell[25], password[25];
char *result;

/* prompt for both the shell and password and save them to appropriate variables */

fprintf(stderr, “Enter the shell you wish to protect: “) ;
scanf(“%s”, shell) ;
fprintf(stderr, “Enter the password to be encrypted: “) ;
scanf(“%s”, password) ;

/* encrypt the password and then send the shell and encrypted password to standard
* ouput where it can be redirected to the end of the /etc/d_passwd file */

result = crypt(password, “xx”) ;
fprintf(stdout, “%s:%s:\n”, shell, result) ;
}
```

13 Appendix G: UNIX File Permissions and Lawson

UNIX File Permissions and Lawson 05/09/97 10:32 AM

This is a working document that changes as new Lawson cyclicals and versions are installed. Beware ***The Lawson Insight Enivornment*** *install procedures will set the permissions back to what Lawson ships. THESE CHANGES NEED TO BE FOLLOWED ' TO THE LETTER' ON ALL DIRECTORIES AND FILES.*
WE suggest you write a Unix script that implements these changes.
If you have problems after implementing, and need to go back to the original permission use the instructions in the Installation and Upgrade manual for REINSTALLING Environment. (You do not need to copy the Environment CD-ROM again).

All Lawson end users will need to be assigned to unix group LAWSON in the /etc/group, this allows access via group permissions. This should be their primary group assign.

The minimum (most restrictive) file permissions in Lawson are as follows:
Please note that there are files in the $GENDIR/bin directory that need to be run as setuid root.

Perms	Directory	Owner	Group
755	$GENDIR	lawson	lawson
755	$GENDIR/bin	lawson	lawson
755	$GENDIR/bin/*	lawson	lawson
750	$GENDIR/lib/*	lawson	lawson
4755	$GENDIR/bin/execjob	root	lawson
4755	$GENDIR/bin/deljobhst	root	lawson
4755	$GENDIR/bin/getrptaccess	root	lawson
4755	$GENDIR/bin/jqcontrol	root	lawson
4755	$GENDIR/bin/ladb	root	lawson
4755	$GENDIR/bin/lajs	root	lawson
4755	$GENDIR/bin/latm	root	lawson
4755	$GENDIR/bin/ladeathlawson	root	
4755	$GENDIR/bin/lafile	root	lawson
4755	$GENDIR/bin/lawsec	lawson	root
4755	$GENDIR/bin/qcompile	root	lawson
4755	$GENDIR/bin/qcontrol	root	lawson
4755	$GENDIR/bin/qstatus	root	lawson
4755	$GENDIR/bin/queue	root	lawson
4755	$GENDIR/bin/stopqueue	root	lawson
4755	$GENDIR/bin/stopjobqueue	root	lawson
4755	$GENDIR/bin/stoplatm	root	lawson
4755	$GENDIR/bin/stopladb	root	lawson
700	$GENDIR/a	lawson	lawson
600	$GENDIR/a/*	lawson	lawson
700	$GENDIR/pdlib	lawson	lawson

600	$GENDIR/pdlib/*	lawson	lawson
700	$GENDIR/wslib	lawson	lawson
600	$GENDIR/wslib/*	lawson	lawson
700	$GENDIR/dict	lawson	lawson
700	$GENDIR/elm	lawson	lawson
750	$GENDIR/install	lawson	lawson
777	$GENDIR/template	lawson	lawson
644	$GENDIR/template/*	lawson	lawson
777	$GENDIR/menus	lawson	lawson
755	$GENDIR/menus/*	lawson	lawson
700	$GENDIR/gen/map	lawson	lawson
700	$GENDIR/gen/map/default	lawson	lawson
755	$GENDIR/sybase	lawson	lawson
755	$GENDIR/oracle	lawson	lawson
755	$GENDIR/informix	lawson	lawson
777	$GENDIR/cgi-bin	lawson	lawson

Replace the word PRODLINE with each of your actual product lines.(these are in UPPER CASE)

777	$LADBDIR	lawson	lawson
770	$LADBDIR/PRODLINE	lawson	lawson
660	$LADBDIR/PRODLINE/*	lawson	lawson
666	$LADBDIR/PRODLINE/reorg.hist	lawson	lawson
777	$LADBDIR/GEN	lawson	lawson
660	$LADBDIR/GEN/*	lawson	lawson
775	$LADBDIR/dict	lawson	lawson
644	$LADBDIR/dict/GEN	lawson	lawson
664	$LADBDIR/dict/PRODLINE	lawson	lawson
775	$LADBDIR/sec	lawson	lawson
666	$LADBDIR/sec/*	lawson	lawson
775	$LADBDIR/elm	lawson	lawson
664	$LADBDIR/elm/*	lawson	lawson

Replace the word prodline with each of your actual product lines.(these are in lower case)

777	$LAWDIR	lawson	lawson
750	$LAWDIR/pdlib	lawdev	lawson
740	$LAWDIR/pdlib/*	lawdev	lawson
750	$LAWDIR/wslib	lawdev	lawson
740	$LAWDIR/wslib/*	lawdev	lawson
777	$LAWDIR/print	lawdev	lawson
755	$LAWDIR/prodline	lawdev	lawson
600	$LAWDIR/prodline/ORACLE	lawson	lawson
600	$LAWDIR/prodline/INFORMIX	lawson	lawson
600	$LAWDIR/prodline/SYBASE	lawson	lawson

755	$LAWDIR/prodline/pdlib	lawdev	lawson
644	$LAWDIR/prodline/pdlib/*	lawdev	lawson
755	$LAWDIR/prodline/wslib	lawdev	lawson
644	$LAWDIR/prodline/wslib/*	lawdev	lawson
755	$LAWDIR/prodline/int	lawdev	lawson
755	$LAWDIR/prodline/int/*	lawdev	lawson
755	$LAWDIR/prodline/rdlib	lawdev	lawson
755	$LAWDIR/prodline/sdlib	lawdev	lawson
755	$LAWDIR/prodline/Admin	lawdev	lawson
775	$LAWDIR/prodline/obj	lawdev	lawson
644	$LAWDIR/prodline/obj/*	lawdev	lawson
775	$LAWDIR/prodline/map	lawdev	lawson
775	$LAWDIR/prodline/map/default	lawdev	lawson
644	$LAWDIR/prodline/map/default/*	lawdev	lawson

replace the word lang with each of your locales if using language translations

777	$LAWDIR/prodline/map/lang	lawdev	lawson
644	$LAWDIR/prodline/map/lang/*	lawdev	lawson
777	$LAWDIR/prodline/work	lawdev	lawson
755	$LAWDIR/prodline/??src	lawdev	lawson
600	$LAWDIR/prodline/??src/*	lawdev	lawson
644	$LAWDIR/prodline/??src/*.or	lawdev	lawson
644	$LAWDIR/prodline/??src/*.sr	lawdev	lawson
777	$LAWDIR/prodline/bsi750	lawdev	lawson
774	$LAWDIR/prodline/bsi750/*	lawdev	lawson

if you have the following products INVENTORY CONTROL , PURCHASE ORDER , MATCHING, REQUISTITIONS

777	$LAWDIR/prodline/hht	lawson	lawson
775	$LAWDIR/prodline/fax	lawson	lawson
777	$LAWDIR/prodline/edi	lawson	lawson
775	$LAWDIR/prodline/bid	lawson	lawson
777	$LAWDIR/prodline/interface	lawson	lawson
775	$LAWDIR/prodline/patient	lawson	lawson
777	$LAWDIR/prodline/vertex	lawson	lawson
777	$LAWDIR/system	lawson	lawson
644	$LAWDIR/system/*	lawson	lawson
644	$LAWDIR/system/license	lawson	lawson
664	$LAWDIR/system/*.cfg	lawson	lawson
664	$LAWDIR/system/*.log	lawson	lawson
755	$LAWDIR/system/termdef	lawson	lawson
644	$LAWDIR/system/termdef/*	lawson	lawson
777	$LAWDIR/system/joblog	lawson	lawson
664	$LAWDIR/system/joblog/*	lawson	lawson
777	$TMPDIR	root	

if you have installed the additional software packages needed for EDI .

777	$EDI_ROOT	lawson	lawson
777	$EDI_ROOT/mentor	lawson	lawson
777	$EDI_ROOT/cleoa	root	lawson

You may notice that the $LAWDIR/prodline directories are owned by a user **lawdev**, group lawson. You must add this user (lawdev) to your system as a valid login, with a UID greater than 200.

OR any user that has a UID greater than the LAUAMINUID in $LAWDIR/system/univ.cfg, and has been given Lawson security access, can be the owner of these directories and files. The purpose of doing this is to allow a user to compile lawson COBOL programs. If security is on, the user 'lawson' cannot compile COBOL programs. This is because the UID of the user 'lawson' is 80, which is less than 200. The user 'lawson' then does not have access in security to compile COBOL programs. Having one user other than lawson allows for tighter file access permissions and allows programs to be compiled while Lawson security is on. Only this user ID will have unix permissions to compile.

All end users accessing Lawson need to be assigned to unix group LAWSON in the /etc/group, this allows access via group permissions.

The following files in the $GENDIR/bin directory must be installed as setuid root i.e. (4755 for permissions).

execjob
deljobhst
getrptaccess (Universe 2.2.4 or greater)
jqcontrol
ladb
ladeath (Universe 2.2.4. or greater)
lafile (Universe 2.2.4. or greater)
lajs
latm
lawsec
qcompile
qcontrol
qstatus
queue
stopjobqueue
stopqueue
stopladb
stoplatm

execjob

When a user runs a batch job, for example GL200, an execjob is run which is used to start a lacobrts and changes the UID of the lacobrts to the person who submitted the job. If execjob were not setuid root, then execjob will inherit the UID of whoever started the job scheduler (lajs). This will create a problem in viewing print files since print files permissions are set by the person who submits the job. Execjob also needs to be able to have access to change permissions on a print directory so that it can write the print file. This comes into play if a user other than the original job owner runs a job.

lajs

lajs needs to be setuid root because within the job scheduler (jobschd), there is the ability to kill a running batch job. This kill option is really doing a kill of the pid and lajs needs the privilege to do so.

latm
If latm is turned on, in on line screens, for example GL00, the lacobrts is run as lawson being the owner. Latm needs the privilege of being able to kill the lacobrts if there is a problem, for example the program is looping. Latm , therefore has to be set as setuid root.

ladb, lafile, ladeath
ladb needs to be setuid root because, for example, in an Oracle database, when a user runs a job, an oradb is started. Ladb needs to be able to change oradb to the UID of the person who starts the job. lafile handles the data access for Lawson database and all users share the same open to a given file. ladeath notifies ladb when processes have completed to be killed.

qcompile, qstatus, qcontrol and stopqueue
These need to be setuid root. For the following reasons: qcontrol needs to be setuid root because a kill can be issued in qcontrol to kill any job that is currently compiling. Stopqueue needs to be setuid root because it needs the privilege of issuing a kill of the compile server which is run as root. Furthermore, these 4 programs are linked so that all of them need to have the same permissions.

queue
Queue needs to be setuid so that when users submit jobs to compile to the server, they will run as the UID of the person who submits them.

Stopqueue, Stopladb, Stopjobqueue and Stoplatm
These all need to be setuid root because they bring down servers and they need the privilege of issuing kill commands to the PIDs of the servers they control.

Startqueue is a script that has umask set to 0 in the script. That script may be changed to umask 022. This will ensure that the $LAWDIR/prodline/obj/* programs will be compiled with a permission of 644.