PRESENTATION 030

New Security Features of HP-UX 11i

Donald L. Pipkin
Information Security Architect
Internet Security Division
Hewlett-Packard
6655 S. Lewis
Suite 105
Tulsa, OK 74136
(918) 481-6700
(918) 481-2200 fax
don_pipkin@hp.com

INTRODUCTION

Recent headlines illustrate the importance of security for e-business. HP is making it clear that it intends to position HP-UX 11i as the operating environment for the Internet. HP-UX 11i provides industry leading capabilities and security for Internet companies. It includes IP filtering software to protect the systems from network attacks and buffer overflow protection to protect it from faulty software. To facilitate more secure Internet computing, HP-UX 11i includes IPsec software that enables secure end-to-end communication over the Internet for ISP customers, e-commerce and remote corporate access. HP-UX 11i is the first major operating system to feature host-based Intrusion Detection software providing protection from external attacks.

These features makes HPUX 11i the one of the most secure commercial operating system. This is illustrated by the fact that HPUX 11i protects against all of the Unix-applicable intrusions in the "SANS Top Ten Most Exploited Internet Security Flaws," listed at www.sans.org/topten.htm. HP-UX 11.i provided the highest quality real-time protection and detection against intruders of any commercial Unix system.

This paper will highlight these features and others which are available on HP-UX 11i. It will examine the 3 A's of securing an information systems

- Authentication and identification,
- Authorization or access control,
- Administration.

It will also explore network privacy, as well as software security, including:

- Security-enhanced applications,
- Secure application environment, and
- Developing secure applications.

Security is critical for the future of business, and you need to understand how to utilize the security tools provided to you by Hewlett-Packard in this newest release of HP-UX.

IDENTIFICATION

Identity management is core to being able to implement a secure enterprise. One must be able to accurately identify all information resources, including users, systems, information, etc. Originally, UNIX account and configuration information was stored in a series of text files. As the use of Unix systems in the enterprise increased so did the need to share this information.

Network Information Service (NIS), developed by Sun Microsystems, provides this network-wide management of many UNIX configuration files (e.g., /etc/passwd, /etc/group, /etc/services). While providing a high degree of backward compatibility with file-based configuration, NIS has limitations in scale and security that prevent it from being easily deployed in enterprise environments. NIS does not support delta-based updates, and can support only a limited number of entries per NIS domain; the information is transferred across the network unencrypted. Despite these shortcomings, NIS is widely used today.

The Name Service Switch (/etc/nsswitch.conf) architecture allows commands and applications to retrieve name service information (users, groups, services, etc.) without having knowledge of where or how it is stored. Commands and applications call standard C library functions, which in turn use the Name Service Switch to determine which name service routines to call.

NIS+

NIS+ was introduced as a successor to NIS to provide greater scalability and security. While succeeding to some extent, NIS+ has not achieved the level of acceptance of NIS. Administrators have reported that the level of complexity in administering NIS+ often outweighs the benefits. NIS+ was introduced in HP-UX Release 10.30 and is supported in both standard and trusted HP-UX systems. NIS+ is not an enhancement to NIS; it is a whole new service. Like NIS, it is a distributed database system that allows you to maintain commonly used configuration information on a master server and propagate the information to all the hosts in your network.

As an HP-UX extension to NIS+ for Trusted Systems, an HP-UX NIS+ server runs the ttsyncd daemon to synchronize the NIS+ password table with the NIS+ trusted table. Without ttsyncd, the trusted table will not be created and Trusted Systems cannot be centrally administered. In a Trusted System, the NIS+ user password length is limited to 8 characters for interoperability reasons.

LDAP-UX Integration (J4269AA)

The lightweight directory protocol can be used for storing both user identification and system identification. Specifically, this product allows HP-UX client systems to use an LDAP directory as its repository for user and group information. Client systems get user and group information from an LDAP directory as well as from /etc/passwd and etc/group files and other name services.

The information transmitted between the LDAP server and the clients is in clear text. To prevent sniffing of this information, an encrypted connection should be used. Future releases of the LDAP services are expected to utilize SSL to secure this communications.

Name Switch Services (NSS_LDAP)

NSS_LDAP is a new back-end that searches an LDAP directory for name service information. The first release will support user, group and shadow password entries. It has the ability to connect to the directory as an anonymous user, a configured proxy user, or as the user id of the calling process when used in conjunction with PAM_LDAP.

A rich set of configuration options allow each HP-UX system to specify up to three search filters into the directory. Search filters specify where in the directory tree to start the search, how deep to search, and what rules to apply to determine a match. Attribute mappings may also be configured to allow NSS_LDAP to integrate with directories that do not store name service data in the format specified by the RFC 2307 schema.

NIS/LDAP gateway (a.k.a. YPLDAP)

The NIS/LDAP Gateway is a Network Information Service (NIS) server that uses an LDAP directory as its information source instead of NIS map files. The Gateway accepts NIS client requests for information, gets the information from an LDAP directory, and returns the information to the NIS clients. Unix information such as user accounts, groups, and services are stored in an LDAP Directory in the format defined by the RFC 2307 schema. Unix clients configured to use NIS will be able to transparently use an LDAP directory to resolve user, group, host and other information. YPLDAP replaces the NIS slave server. NIS master servers are not needed; this functionality is now being provided by an LDAP directory. The NIS/LDAP Gateway allows your organization to leverage the scalability and distributed nature of LDAP directory services while maintaining an existing NIS infrastructure. This allows a greater number of entries to be stored than in a traditional NIS master. Communications between YPLDAP and the LDAP directory can be protected with a Secure Socket Layer (SSL) connection using X.509 certificates for authentication and encryption.

It supports the commonly used NIS maps, including passwd, group, hosts, networks, aliases, netgroup, and services. YPLDAP is available on HP-UX 10.20 and 11.0 platforms and will support any NIS version 2-compatible client, including HP-UX 10.20.

Domain Name System

Domain name services, the standard method of mapping Internet domain names to IP addresses, are supplied on HP-UX by the Berkeley Internet Name Domain (BIND).

Berkeley Internet Name Domain 8.1.2

HP-UX 11i supports a new release of BIND, v8.1.2, which is much more configurable than previous releases. The new security features enable entirely new areas of configuration (/etc/bind.conf) with many options that previously applied to all zones can now be used selectively. These mainly apply to such areas as, access control lists and categorized logging.

BIND v8.1.2 protects all DNS client/server transactions with IP address-base ACLs. On a name server, ACLs control who can query the name server, initiate zone transfers from the name server and request dynamic updates, as well as restricting the name servers to which queries can be sent. IP-address-based access control for queries, zone transfers, and updates may be specified on a zone-by-zone basis. These access controls rely on the source IP address stated in IP packets to determine the identity of the transaction initiator. If no precautions are taken, IP address spoofing can subvert this control mechanism. This is one manifestation of the well-known security limitations of the existing Internet DNS version 8.1.2.

This release of BIND supports a flexible, categorized logging system.

BIND 9

BIND v9 is a major rewrite of nearly all aspects of the underlying BIND architecture. It includes protocol enhancements necessary to securely query and update zones. The IETF is addressing the security limitations of the Internet DNS through the introduction of DNS security protocols, including DNSSec, TSIG, and TKEY. These protocols are implemented in BIND version 9. HP-UX will provide this next version of BIND, and it is available for download from HP Software Depot (http://www.software.hp.com/).

DNSSec is specified in the Proposed Standard RFC 2535. It provides data integrity and authentication to security-aware resolvers and applications using cryptographic digital signature. It prevents non-authorized access to DNS, and prevents name-to-address mapping tampering over the wire. These are the type of active network-level attacks to which DNS has been susceptible. DNSSec can also be used to safeguard DHCP dynamic updates. It restricts DHCP updates to those authorized to perform them. It guarantees the integrity of zone data, using digital signatures produced off-line by the owner of the data and stored in SIG Resource Records.

DNS Security Operational Considerations is covered by RFC2541, which covers the operational aspects for keys and signatures used in connection with the KEY and SIG DNS resource records.

- ***TSIG,*** Transaction SIGnature, can be used to cryptographically authenticate transactions. A key is shared by the resolvers and the name servers and use it to sign communi-

cations between them. Specifically, the integrity and origin of the data exchanged in a transaction is protected by HMAC-MD5, using a key shared by the servers involved. This key must be securely distributed to the participants by a manual configuration process.

- ***TKEY*** is a protocol which addresses the problem of distributing shared keys for TSIG by allowing participants in DNS transactions to establish shared secret material. Note that TSIG requires time synchronization between the name servers involved, and the name of the key (not just the key itself) must match on the servers. In addition, TSIG does not provide zone data integrity or secure binding of public keys.
- ***Split DNS*** is the process of dividing public and private names by separating them onto different servers for inside and outside as mentioned in RFC 1918. Resolvers would receive different answers depending on whether they are on the inside or outside. BIND v9 implements another method (based on the IETF draft) to achieve the effect of local names that is more in tune with the concept of a single global DNS tree or at least the appearance of a single tree. Use of this approach is not required, and older techniques will continue to work.

BIND v9 also has extensive logging capabilities that can be used for auditing.

AUTHENTICATION

Authentication is required to prove identity. An authenticated identity is needed to assign authorization and determine accountability.

Pluggable Authentication Module (PAM)

The Pluggable Authentication Module (PAM) is an industry-standard authentication framework. PAM gives system administrators the flexibility of choosing any authentication service available on the system to perform authentication. The PAM framework also allows new authentication service modules to be plugged in and made available without modifying the applications. It provides for assigning global authentication methods (/etc/pam.conf) and user-specific authentication methods (/etc/pam_user.conf). Therefore, users with different privileges can have different authentication requirements.

- The *Authentication Module* verifies the identity of a user and sets the user-specific credentials.
- The *account management module* retrieves the user's expiration information and verifies that the user's account and password have not expired.
- The *session management module* provides functions to initiate and terminate sessions.
- The *password management module* provides a function to change passwords.

PAM gives the system administrators the flexibility of choosing any authentication service available on the system to perform authentication. The PAM framework also allows new authentication service modules to be plugged in and made available without modifying the applications or rebooting the system.

The PAM framework provides easy integration of additional security technologies into HP-UX system entry commands. The Unix login (login), X-windows login (dtlogin) and remote X-windows actions (dtaction) , file transfer (FTP), switch user (su) all support PAM. Now on HP-UX 11i, the rexecd and remsh services use PAM for authentication.

Kerberos (J5849AA)

Kerberos is an authentication service for authenticating users or services across an open network. It works by assigning a unique shared secret key and issues a token called a ticket to each client that logs on to the network. The ticket is then embedded in messages to identify the sender of the message.

Under Kerberos, a client (generally either a user or a service) sends a request for a ticket to the Key Distribution Center (KDC). The KDC creates a ticket-granting ticket (TGT) for the client, encrypts it using the KDC key, and sends the encrypted TGT back to the client. The client uses the TGT to obtain further service tickets, which provide the proof of the client's identity.

PAM Kerberos, PAM-KRB5, is supported on the HP-UX 11i system. It is based on Kerberos Authentication System V5, developed by Massachusetts Institute of Technology (MIT). The PAM Kerberos module is compliant with IETF RFC 1510 and Open Group RFC 86.HP-UX PAM Kerberos is implemented under the PAM (Pluggable Authentication Module) framework. PAM Kerberos works with Microsoft Windows 2000 and MIT Kerberos V5 KDC. However, it is not intended to work with the HP-UX DCE KDC.

To support single sign-on between HP-UX and Microsoft Windows 2000 or other UNIX systems running MIT Kerberos, HP-UX provides PAM Kerberos that integrates HP-UX login with any Kerberos 5 Server, such as Microsoft Windows 2000 Key Distribution Center (KDC) and MIT KDC.

PAM Kerberos authenticates entities without sending plain text passwords over the network. The Kerberos protocol uses strong cryptography (DES) so that a client can prove its identity to a server (and vice versa) across an insecure network connection, and assure privacy and data integrity in the communications.

AUTHORIZATION

Authorization controls determine what users and process will have access to information resources. These controls can be placed to prevent access at a global level, such as a firewall, or on very specific resources, such as file access controls. These two areas have been enhanced with HP-UX 11i.

HP IP Filter/9000 (B9901AA)

IPFilter/9000 is a re-write, for HP-UX, of the popular BSD IPFilter program, which is a public-domain stateful inspection firewall. It is provided free-of-charge for use as a system firewall on hosts running HP-UX 11i.

A system firewall is a packet filtering mechanism that is built into the TCP/IP stack of a host and provides filtering functionality specifically configured for the protection of that particular host. This program uses a sophisticated stateful-inspection packet filtering technology to filter traffic that enters or exits an individual HP-UX host.

Multi-homed HP-UX systems can be configured to discard incoming packets that are received through one network interface but whose destination address is that of a different interface of the same host, as well as to block the sending of outgoing packets whose source address is not that of the interface through which they are being sent. This packet filtering feature characterizes the Strong End-System (ES) functionality described in RFC 1122 of the IETF.

It can also function as a limited application proxy but is not recommended as a general-purpose application proxy.

Designed to be used as a firewall, it is quite capable of being used to protect a host from network attacks. By default the product will allow all packets to pass both in and out. However, by adding the appropriate filters to /etc/opt/ipf/ipf.conf all packets can be blocked.

It is supported on HP-UX 11, with appropriate patches, in both 32- and 64-bit mode. It is released as a no charge software product on AP0301.

File system ACLs

An Access Control List (ACL) stores a series of entries that identify specific users or groups and their access privileges for a directory or file. A file may have its own ACL or may share an ACL with other files. ACLs have the advantage of specifying detailed access permissions for multiple users and groups.

Begining with HP-UX 11i, the Journaled File System (JFS 3.3) (Veritas File System) supports ACLs. JFS require a file system with the version 4 disk layout to support ACLs. Only POSIX-compliant ACLs are supported in JFS. The compliant entries are those that specify permissions for either a user or a group, but not both. For example, entries of format (user.%) and (%.group) are POSIX-compliant, while entries of format (user.group) are not. HFS will support the latter form.

ADMINISTRATION

A centralized location (/etc/default/security) for default security parameters has been created in HP-UX 11i. Currently the login, passwd and su commands utilize this information. Each line in the file is treated either as a comment or as configuration information for a given system command or feature. If any parameter is not defined or is commented out in this file, the default behavior detailed below will apply. This file must be world readable and root writable.

Parameter definitions, valid values, and defaults are defined as follows:

- ABORT_LOGIN_ON_MISSING_HOMEDIR - This parameter controls login behavior if a user's home directory does not exist. This is applicable only for non-root users. If the parameter is set to one (1) the login session will exit if the user's home directory does not exist. If it is set to zero (0) the user will be allowed to login and his home directory will be set to the root directory (/). The default value is zero.
- MIN_PASSWORD_LENGTH - This parameter controls the minimum length of new passwords. For untrusted systems it can be any value from 6 to 8. It is not applicable to the root user on a untrusted system. For trusted systems it can be any value from 6 to 80. The default value is 6.
- NOLOGIN - This parameter controls whether non-root login can be disabled by the /etc/nologin file. If the value is 1, the contents of the file /etc/nologin will be displayed and the root user will not be allowed access. If the value is 0, the presence of the file is ignored. The default value is 0.
- NUMBER_OF_LOGINS_ALLOWED - This parameter controls the number of logins allowed per user. This is applicable only for non-root users. A value of zero (0) allows unlimited logins. The default value is 0.
- PASSWORD_HISTORY_DEPTH - This parameter controls the password history depth. A new password is checked only against the number of most recently used passwords stored in password history for a particular user. A user is not allowed to reuse a previously used password. The password history depth configuration is on a system basis and is supported in trusted system. This feature does not support the users in NIS or NISPLUS repositories. Once the feature is enabled, all the users on the system are subject to the same check. If this parameter is not configured, the password history check feature is automatically disabled. When the feature is disabled, the password history check depth is set to 1. A password change is subject to all of the other rules for a new password including a check with the current password. The default value is 1.

- SU_ROOT_GROUP - This parameter defines the root group name for the su command. The root group name is set to the specified symbolic group name. The su command enforces the restriction that a non-superuser must be a member of the specified root group in order to be allowed to su to root. This does not alter password checking. If this parameter is not defined or if it is commented out, there is no default value. In this case, a non-superuser is allowed to su to root without being bound by root group restrictions.
- SU_DEFAULT_PATH - This parameter defines a new default PATH environment value to be set when su is done. The PATH environment variable is set to new_PATH when the su command is invoked. Other environment values are not changed. The path value is not validated. This is applicable only when the "-" option is not used along with su command. By default the path is not changed.

ndd

ndd is a networking configuration tool used to customize the networking kernel. To make an 11i system more Internet friendly and easier to run "out of the box," some of the ndd tunable parameters defaults changed. Some unsupportable tunable parameters are now "supported." Also, some new tunable parameters have been added. Some of the changes reflect changes to the networking industry standards.

A number of the parameters can reduce information leakage and prevent certain types of Denial-of-Service attack.

syslog

A new parameter (-N) was added to the system logging deamon, syslogd, which tells the deamon not to listen to a socket that would otherwise be used to receive log data from other hosts on the network. This prevents an often overlooked denial of service vulnerability where false log entries could be sent to a system until the the disk is full. This option was added to HP-UX 11 patch PHCO_21023 and is included in HP-UX 11i.

HP Intrusion Detection System / 9000 (J5083AA)

The HP Intrusion Detection System/9000 (IDS/9000) enhances local host-level security by automatically monitoring each configured host for signs of unwanted and potentially damaging intrusions. IDS/9000 concentrates on detecting and alarming the HP-UX 11 operating environment at the kernel audit data level of the operating system. IDS 9000 can monitor one or more HP-UX systems for users or applications who try to break security. IDS/9000 is a no-charge option on HP-UX 11i. It requires installation of Java JRE or Java JDK version C.01.18.00

As soon as the IDS/9000 is installed it immediately provides intrusion detection. Preplanned detection templates, surveillance groups, surveillance schedules, and alerts are built into the system making basic detection and alerting are available immediately. IDS/9000 continuously monitors for patterns of suspicious activities that suggest security breaches or misuses are underway. When it detects a potential intrusion, it alerts immediately and creates audit events. The alert also has the ability to execute any HP-UX command or program. IDS/9000 uses a variety of data sources to determine misuses including:

- *Kernel audit data* which is generated by the trusted component of the operating system provides secure and robust data on use of kernel functions.
- *System logs* provide information about access to the system, utilization of network services, and the use of system utilities.
- *Application logs* record activity and utilization which enables detection of well-known attacks.

It detects a variety of exploits, such as: unauthorized access, modification of user resources, virus infections, privilege violations, Trojan horse, and “root” exploits. System conditions which can indicate misuse are race conditions, buffer overflows, unusual system states and unusual daemon behavior.

All communications within the IDS/9000 are secure and built upon the Secure Socket Layer (SSL) protocol. SSL protects the client/server messaging.

Obtaining HP-UX Security Bulletins

Security software patches are available via e-mail from the HP Electronic Support Center, which encompasses SupportLine, Software Update Manager, Custom Patch Manager, and PC, Printing, and Imaging Support. Up-to-date security patch matrix and the Security Bulletin archives are available through the HP Electronic Support Center page at:

- http://us-support.external.hp.com (U.S., Canada, Asia Pacific, and Latin America)
- http://europe-support.external.hp.com (Europe)

NETWORK PRIVACY

Network privacy has become significant as companies move to the Internet to provide communication for thier business needs. HP supplies two free VPN solutions.

HP IPSec/9000 (J4255AA, J4256AA)

HP IPsec/9000 software provides secure and private communication both over the Internet and within the enterprise without the need to modify existing applications. It provides transparent encryption for IP-based applications for privacy and supports pre-shared keys for authentication as well as PKI-based authentication from Entrust, VeriSign and Baltimore. It uses rule-based access control and the Internet Key Exchange (IKE) protocol. IPSec consists of a family of interrelated protocols, including the Authentication Header (AH), the Encapsulating Security Payload (ESP), the Internet Key Exchange (IKE), and the Internet Security Association Key Management Protocol (ISAKMP). AH and ESP define encryption and authentication methods for IP payloads. IKE and ISAKMP manage the exchange of secret keys, authenticate the communicating parties, and manage their security associations (SA).

Along with authentication, data integrity, and data privacy, IPSec/9000 offers protection against spoofing and packet tampering. IPSec/9000 has been able to interoperate with over 25 other IPSec implementations, including those of Microsoft® and Cisco.

In the 11i timeframe, IPSec/9000 has been enhanced to provide Centralized Policy Management through LDAP. The Centralized Policy Management tool consists retrieves policy configuration from the directory service, and manages certificates for that node. Policy configuration is set and retrieved using the Lightweight Directory Access Protocol (LDAP). Enabling a secure, cost-effective, and scalable security solution for enterprise networks. It ensures that corporate security rules are enforced and monitored consistently throughout the entire enterprise and reduces security administrative costs by managing corporate security policy and monitoring security events at one central location which simplifies the system administration and troubleshooting effort at each node. It is now supported on HP 9000 workstations and HP's VirtualVault secure web server.

OpenSSL

OpenSSL provides secure socket layer encryption for web applications. It includes a toolkit to provide access to SSL to non-web based applications. OpenSSL version 9.5 is a part of HP-UX Apache Product set which is part of 11.i release. This product will also be supported on 11.0 and 11.10.

SECURITY ENHANCED APPLICATIONS

X11 Security Extension

The X11 security extensions provide enhanced X server security through theaddition of the concepts of trusted and untrusted clients. The trust status of a client is determined by the authorization used at connection setup. All clients using host-based authorization are considered trusted. Clients using other authorization protocols may be either trusted or untrusted depending on the data included in the connection authorization phase.

When a connection identifying an untrusted client is accepted, the client is restricted from performing certain operations that would steal or modify data that is held by the server for trusted clients. An untrusted client performing a disallowed operation will receive protocol errors.

When a client is untrusted, the server will also limit the extensions that are available to the client. Each X protocol extension is responsible for defining what operations are permitted to untrusted clients; by default, the entire extension is hidden.

Application Group Extension (XC-APPGROUP)

The application group extension provides new protocol to implement Application Groups (AppGroups). The AppGroup facility allows other clients to share the SubstructureRedirect mechanism with the window manager. This allows another client called the application group leader, such as a web browser, to intercept a MapRequest made by a third application and reparent its window into the web browser before the window manager takes control. The AppGroup leader may also limit the screens and visuals available to the applications in the group.

This extension, along with the Netscape remote execution plug-in, allows Netscape to run programs remotely over the Web with the output appearing in the Web browser display.

The only way for an application to become a member of an AppGroup is by using an authorization generated using the new security extension. Whenever an application connects to the server, the authorization that it used to connect is tested to see if it belongs to an AppGroup. This means that the authorization data must be transmitted to the remote host where the application will be run. In the case of X, HTTP is used to send the authorization. Sites that have concerns about sending un-encrypted authorization data such as MIT-MAGIC-COOKIE-1 via HTTP should configure their web servers and web browsers to use SHTTP or SSL.

Sendmail-8.9.3

A new version of sendmail, sendmail-8.9.3, is included with HP-UX 11i. This version provides additional features compared to the previous version. Release 8.9.3 of sendmail has been called "the anti-spam release." It is the first sendmail release to include anti-spam rule sets. These rule sets and other features in release 8.9.3 give mail administrators significantly more power to keep spam at bay.

The primary security features available in sendmail v8.9.3 are:

- ***Relaying denied by default*** so that no transmission of messages from a site outside your domain to another site outside your domain is allowed unless configuration options are used to selectively relay messages from certain hosts.
- ***Better checking on sender information*** will refuse mail if the sender has an unresolvable domain name. This behavior can be enabled by the use of the access database mentioned below. Sendmail can also be configured to reject mail to certain recipients.
- ***Access database*** is a user-defined file that can decide the domains from which the user wants to receive or reject mail messages. The entries in the access database file are keyed by the domain name, the IP address, and the host name. The action can be to accept the message, relay it, reject it, or respond to it with a specific error message.
- ***Header checks*** beyond the *from* and *to* headers. This feature can filter messages based on the value of other headers, making it possible to reject messages based on the *subject* or any other standard header format. However, enabling this feature may affect the performance of sendmail, since it requires parsing the entire header.
- ***Realtime-blackhole-list-based filter*** checks each incoming message against the Mail Abuse Prevention System to block messages from hosts deemed "friendly" to spammers. The advantage of the blackhole list is that a spamming host is listed in the RBL within minutes of spamming. However, the RBL can block a host without notifying the blocked entity.
- ***Denial of service*** options to check the system load and queue requests or drop connections based on the current load.
- ***Permission checking*** strictly checks the permissions of files and directories to avoid compromising security. Furthermore, it ensures that it always runs with root as the effective user id and mail as the effective group id.
- ***Extensive logging*** through *syslog*. It compiles accounting data for every message received or exchanged, and it can provide usage statistics per user or per domain.

NFS

A number of enhancements and repairs have been made to the NFS implementation which affects the security of the NFS.

NFS Mount Access Control

The behavior of access= has been modified to conform to de facto industry behavior. Clients will have to be in the access= list to be granted access. Well behaved applications will see no change. However, applications which are using the undocumented feature to disallow the NFS mounts, will discover that the mount will now succeed.

Tighter Security for NFS Mounts

Historically, an exported filesystem using the root= option of exportfs, NFS-clients on the root= option are allowed to mount the NFS file system even when they don't appear on the rw= list and/or access= list. Now the NFS client will be disallowed from mounting the file system unless it appears in either a rw= and/or access= list.

Export of Symbolic Links

When a symbolic link to a filesystem is exported, the directory to which the symbolic link points will be exported. This change corrects the NFS implementation so it conforms to industry practice when exporting a filesystem. Well-behaved applications will not be affected by this change. Shell scripts and administrative processes may have to be changed to correctly handle this modification.

NFS support for TCP/IP

Network File System (NFS) is now supported over the connection-oriented protocol, TCP/IP for NFS versions 2 and 3, in addition to running over User Datagram Protocol (UDP). TCP transport increases security and dependability on wide-area networks (WANs). Generally, packets are successfully delivered more consistently because TCP provides congestion control and error recovery. Security features which are available for TCP connections can now be utilized to help protect and controll NFS connections.

File Transfer Protocol Daemon

A new version of ftpd is supplied with HP-UX 11i. In addition to supporting the FTP protocol defined in RFC 959, it supports secure FTP and virtual servers. The unified binary can operate as both Kerberos (secure FTP) and non-Kerberos (standard FTP) service. The services obtain the type of authentication mechanism from the system file, /etc/inetsvcs.conf, at run time. The virtual ftp server feature can be used to manage an ftp server for two separate domains on the same machine. This allows an administrator to configure different ftp banners and directories based on the address used to access the server.

More robust logging and greater control of restricting the use of the deamon have been added. The use of the new configuration options in /etc/ftpd/ftpaccess can be enabled (-a) or disabled (-A) by the appropriate option. The new security options which extend the logging information stored in /var/adm/syslog/xferlog. Additional logging information includes all files received (-i), all files transmitted (-o), and all commands sent to the deamon (-L).

Access to the deamon can be limited by the classification of the user (/etc/ftpd/ftpgroups), the location of the user (/etc/ftpd/ftphosts), and the name of the files being transfered. Users can be restricted to specific virtual hosts or enabled to all. Restrictions can be set on a per-directory basis.

Non-Executable Stacks

A common method of breaking into systems is by maliciously overflowing buffers on a program's stack. Malicious unprivileged users often use this method to trick a privileged program into starting a super user shell for them, or performing similar unauthorized actions.

HP-UX 11i provides new mechanisms to defend against this type of attack without sacrificing performance or in the vast majority of cases, enabling this feature will not affect compatibility of any legitimate applications.

By setting the kernel tunable parameter executable_stack to zero, HP-UX systems can be configured to execute protect program stacks, providing significant protection from many common buffer overflow attacks.

When enabled, the new functionality causes the termination of any program attempting to execute code located on its stack. If this occurs, you will be given an error message pointing to relevant documentation that explains the reason for the process termination and how to remedy the situation.

If a program does need to execute its stack, (typically interpreters, simulators and debuggers) you can use the “chatr +es enable” command to allow stack execution.

ELF-64 programs linked on previous releases of HP-UX will not benefit from this security feature until they are re-linked on HP-UX 11i, but will still function normally. 32-bit applications do not need to be re-linked.

By default, for backward compatibility, executable_stack is set to 1, which allows stack execution. You can use SAM to change the value to 0, preventing stack execution.

NOTE: Disabling stack execution will cause Java 1.2 programs to fail if using JDK/JRE 1.2.2 versions older than 1.2.2.06. To allow these programs to run, the executable from stack attribute will need to be set to enable for all executables contained in the JDK and JRE. Java 1.1 versions will execute with no problem.

Hewlett-Packard has made a number of security APIs available at 11i.

Fast Crypto for RSA

HP implemented the RSA cryptographic algorithms for DES and Triple-DES using advanced features in the enhanced assembly-language for PA-RISC 2.0 that take advantage of 64-bit registers. This implementation achieves almost twice the encryption speed of other leading software implementations. The enhanced performance of the cryptographic algorithms is made available to all the applications through the use of the stanard HP-UX libraries.

Kerberos Client Software

Kerberos is a network protocol which is designed to provide strong authentication for client/server applications by using secret-key cryptography. It uses strong cryptography so that a client can prove its identity to a server and vice versa across an insecure network connection. After the client and the server have established their identities, they can also encrypt all of their communications to assure privacy and data integrity. Kerberos Client Software is now provided with HP-UX 11i and is based on MIT Kerberos V5 1.1.1 which is compatible with earlier versions of the Kerberos product supporting RFC 1510. However the product does not support the Kerberos 4 protocol and Kerberos 4 to Kerberos 5 request conversions.

It enables integrating HP-UX into a secure enterprise environment. It provides tools and libraries to perform authentication (verifying tickets, creating authenticator, context management, etc.) and secure communication (56-bit DES encryption). Kerberos Client Software supports both 32- and 64-bit development. Kerberos Client Software Data encryption APIs can be used to protect data transmitted over the Internet.

This release of the Kerberos Client Software contains support for GSS API as per RFC 2743/2744. Though Kerberos APIs are made available, these are for supporting existing Kerberos Applications to HP-UX 11i. Application Developers are strongly encouraged to use GSS API for developing secure applications.

Generic Security Services

The Generic Security Services Application Programming Interface (GSS API) is a newly introduced product for HP-UX 11i. It contains all the GSS APIs in RFC 2743 and is implemented as C programming language interfaces as defined in the RFC 2744. It provides security services for client / server applications independent of various underlying security mechanisms and communication protocols. The security services available to an application include authentication, integrity, and confidentiality services. The system administrator can configure the quality of protection to use for an application with no modification to the application.

Because of GSS API independence, an application developer writing secure applications needs only to write the code once and does not need to change it whenever the underlying security mechanism changes. This will prove to be quite advantageous during this period where security technology changes are rather frequent.

A set of GSS APIs has been available in the DCE core libraries in previous releases and are in the current product release as well. But these GSS APIs are dependent on the DCE security mechanism and cannot be used as general purpose APIs. Since the symbols of GSS APIs in the DCE libraries clash with the symbols of new GSS libraries, application programmers who want to use GSS API and DCE together may need to resolve the symbol clashes by linking the libgss.sl library first and then the libdce library.

The Common Authentication Technology working group of the IETF has defined several cryptographic mechanisms to implement the security services provided by GSS-API transparently to applications. The use of Kerberos as a GSS-API mechanism is specified in RFC 1964 of the IETF.

GSS-API provides secure communication between two peers with a security context established between the peers. The context is established by an exchange of tokens. When Kerberos is used as the underlying cryptographic mechanism, the client sends a token to the application server that includes a service ticket and an authenticator. If mutual authentication is required, the application server sends a token to the client comprising the application server's authenticator. The GSS-API libraries on the two hosts are responsible for creating and processing the tokens, but the application is responsible for transporting the tokens between client and server.

HP-UX 11i provides GSS-API libraries, including the Kerberos mechanism, as part of the OS core. These libraries can be linked with either 32- or 64-bit applications.

Common Data Security Architecture

HP-UX 11.00 supports the Common Data Security Architecture (CDSA). This architecture, originally developed at Intel Corporation, provides industry standard application program interfaces (APIs) to perform cryptography and other public key infrastructure operations for electronic commerce, e-mail communications, and digital content. It simplifies the software development effort for programmers who write security utilities and secure business applications by providing an overall security infrastructure.

CDSA is available as a separate add-on product to HP-UX 11.00. It is included on the HP-UX 11.00 Application Release CD and is a prerequisite for the CDSA Cryptographic Service Provider (CSP) library. As of HP-UX 11i, CDSA is included in the Operating Environment.

The CDSA CSP is available in the following three versions:

- HP Strong Encryption CDSA CSP.
- HP Worldwide Exportable CDSA CSP.
- HP Worldwide Importable CDSA CSP.

The CDSA CSP is available at no additional charge from HP Software Depot, http://software.hp.com/.

On the Horizon

Hewlett-Packard has a number of security enhancements planned in the next year. Here is a brief summary of some of the type of enhancement that are likely to be implemented.

Specific features and the timing of their implementation is subject to change.

Identification

Enterprise management requires unique identification of all of the information users and resources. In large enterprises the Unix length restriction of user names makes it difficult to create uniform, unique user names throughout the entire enterprise. Support for *Long User Names* in HP-UX will provide for greater ease of management in the enterprise.

Authentication

More supported PAM modules to enable additional common authentication models are being investigated. In particular *Smart Card Support* on HP-UX is needed for greater flexibility with the growing use of smart cards with PKI (a key enterprise technology).

Authorization

Global definition and enforcement of authorization models or policies is crucial to being able to maintain a global enterprise. HP is addressing policy definition and distribution with HP OpenView and WebEnforcer. Enhancements to SAM will provide access to these definitions and enable their use and distribution to HP-UX systems.

Accuracy

There are a number of enhancements being investigated to add *hardening* to the HP-UX kernel. These may include configuration scripts, root partitioning, or scanner technology.

Accountability

There are numerous plans to enhance HP's new Intrusion Detection product to enhance its integration into OpenView and enable more standard templates and its ability to produce security audits. Audit information may also be made available from security scanners which are under investigation.