HP-UX Network Security

Jean-Marc Chevrot, Francisco Corella, Doug Heath, Wan-Yen Hsu,
Bob Joslin, Donna Snow and Bill Tung

6/9/2000

Abstract

The 11i release of HP-UX marks the commitment of HP-UX to lead in the Internet space. In the key area of network security, this commitment is demonstrated by a rich set of standards-based and directory-enabled network security features that will be offered in the 11i timeframe or are already available. They include, among others, an implementation of IPSec with centralized policy management, Kerberos and GSS-API libraries, kerberized internet services, directory-based authentication and name resolution, email anti-spamming capability, and an implementation of SOCKS v5, all available free of charge. HP-UX servers and workstations equipped with these features will enhance the overall security of heterogeneous networks, where they can interoperate with a broad variety of other platforms, such as Windows 2000 hosts or other Unix systems. Because network security requires cryptography, HP-UX 11i features a choice of cryptographic APIs and toolkits for application developers, as well as the fastest implementations of cryptographic algorithms, both in software and in plug-in hardware accelerators.

Acronyms

The following acronyms are used without explanation throughout the paper:

AES	Advanced Encryption Standard
CDSA	Common Data Security Architecture
DES	Data Encryption Standard
DH	The Diffie-Hellman key agreement public-key cryptosystem
DMZ	De-Militarized Zone (between the Internet and the intranet)
DSS	Digital Signature Standard
EDI	Electronic Data Interchange
HTTP	Hyper-Text Transport Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
KDC	Key Distribution Center
MD	Message Digest (MD5 is a message digest, or cryptographic hash, algorithm)
MIT	Massachussetts Institute of Technology
NIST	National Institute of Standards and Technology
PC	Personal Computer
RC	Rivest Cipher (RC4 is a stream cipher)
RFC	Request For Comments
RSA	The Rivest-Shamir Adleman public-key encryption and signature cryptosystem
SHA	Secure Hash Algorithm (SHA1 is NIST's cryptographic hash standard, revsion 1)
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transport Control Protocol
TLS	Transport Layer Security

Introduction

The 11i release of HP-UX marks the commitment of HP-UX to lead in the Internet space. This white paper shows what this means in the key area of *network security*, by surveying the network security features

available on HP-UX. Many of these features are being newly introduced in the 11i core OS or in releases of the application CD in the 11i timeframe.

The Internet was created as a medium for information exchange among academic and research institutions, and has always been characterized by a high degree of openness and collaboration. Consequently, the Internet protocols were designed with little or no concern for security.

Now, however, the Internet has become a universal medium of communication, as well as a worldwide means of selling goods, conducting business, and providing services of all sorts. As a result, security has become an unavoidable necessity. The Internet community has taken up the challenge of retrofitting security into the suite of Internet protocols, without forsaking the spirit of openness and collaboration. The result has been the emergence of an array of *network security protocols* that attempt to provide security while preserving interoperability. Most of these emerging protocols are available on HP-UX 11i.

A recent trend in enterprise networking is the use of a directory, accessible through the Lightweight Directory Access Protocol (LDAP), as a central, scalable repository of heterogeneous information. HP-UX has embraced this trend and, as a first step, is offering options for directory-based user authentication and policy management.

New security features have also been introduced for Internet services, including sendmail anti-spamming capability. These new security features complement those introduced in earlier releases, such as kerberization of ftp, rcp, rlogin, telnet and remsh, which was first provided in HP-UX 10.20.

Network security relies on cryptography for authentication, confidentiality and data integrity protection. Cryptography is computationally intensive, to the point that good cryptographic performance is a key requirement for the successful deployment of network security solutions. HP-UX 11i features a choice of cryptographic APIs and toolkits for application developers, as well as the fastest implementations of cryptographic algorithms, both in software and in plug-in hardware accelerators.

Network security protocols

Overview

A number of network security protocols have been proposed or are being developed at the IETF. At first glance, their functionalities overlap. Indeed, they all provide a similar set of security services: authentication, confidentiality, data integrity protection, etc. Furthermore, they often use the same cryptographic primitives to implement those services: RSA or DSS for authentication; RSA or DH for key exchange; RC4, DES, Triple-DES, or one of a few other symmetric ciphers for confidentiality; MD5 or SHA1 as a data integrity checksum; and the HMAC construct for data origin authentication.

However, a closer look reveals that these protocols are not interchangeable. Each of them is best suited for a particular usage.

SSL, or TLS as it is now called in the IETF, protects the traffic carried by a TCP connection. It was designed to protect web traffic, and it has no rival in that space. When protecting web traffic, it occupies a position in the protocol stack between TCP and HTTP. Usually, TLS uses RSA to authenticate the server and sometimes the client, RC4, DES or Triple-DES to encrypt and decrypt the traffic, and HMAC-MD5 or HMAC-SHA1 to verify the origin and integrity of the data.

IPSec provides security for IP traffic. Due to its position at layer 3 of the protocol stack, it can be deployed underneath legacy applications, providing protection in a completely transparent manner. (By contrast, legacy applications have to be made web-accessible before they can benefit from the protection that TLS affords to web traffic.) IPSec consists of a family of interrelated protocols, including the Authentication Header protocol (AH), the Encapsulating Security Payload protocol (ESP), the Internet Security

Association Key Management Protocol (ISAKMP), and the Internet Key Exchange protocol (IKE). Some of these protocols are currently under active development at the IETF.

IPSec is usually deployed to provide secure tunnels through the public Internet. These tunnels can be used to protect access from remote PCs to a corporate intranet, or to link geographically disjoint portions of an intranet without using expensive leased lines. They can also be used to link the computing facilities of business partners. A less well known usage of IPSec, but one that can be extremely valuable for corporations, is to provide end-to-end protection for sensitive traffic within an intranet. HP-UX has been a pioneer in this area with the IPSec/9000 product, which has provided easy-to-deploy host-to-host protection for HP-UX hosts, free of charge, since February 1999. IPSec/9000 can be used both in transport mode to provide host-to-host security, and in tunnel mode to implement Internet tunnels.

SSH is a focused protocol, which provides secure access over the Internet to individual Unix hosts, including the ability to login remotely, run remote shells, transfer files, and securely forward X11 connections and other TCP traffic. It is available for HP-UX 11 from SSH Communications Security, http://www.ssh.com/.

Kerberos is a mature protocol that uses symmetric-key cryptography (rather than public-key cryptography) for authentication over the network and key exchange. It has been adopted by Microsoft for Windows 2000. Kerberos uses a KDC that shares a secret key with each principal (client or server) in the network. When a client needs access to the server, the KDC sends the client a session key encrypted under the client's secret key, and a ticket containing the same session key encrypted under the server's secret key. The client demonstrates its identity to the server by sending the ticket and a timestamp encrypted under the session key. The client and server can further use the session key to establish a secure session.

Besides protecting network traffic, corporations must be able to filter traffic that crosses the perimeter of the intranet. This can be accomplished by a *perimeter firewall*. It may also be necessary to filter the traffic that reaches specific hosts in the DMZ or the intranet. This can be accomplished using a *system firewall* at each host. Firewalls may range in functionality from simple stateless packet filters, which decide whether to accept or discard a packet based on source and destination addresses and ports, through stateful inspection firewalls, which keep track of connection state, to application proxy firewalls, which inspect data as seen by the target application in order to detect malicious content.

Since encryption can prevent a firewall from inspecting data, when traffic filtering and encryption are both used, the firewall is usually an end-point of the encrypted channel.

The SOCKS protocol provides a generic proxy for applications that use TCP or UDP as a transport. It can be used in a perimeter firewall to relay TCP or UDP traffic between internal and external hosts, avoiding the need to route such traffic and thereby helping insulate the intranet from the Internet. Moreover, for traffic that originates on the Internet side of the firewall, SOCKS version 5 provides the option of authenticating the originator of the traffic, and establishing a secure connection between the originator and the firewall. Several methods for accomplishing this have been proposed. An HP implementation of SOCKS version 5 on HP-UX will soon be made available free of charge under the Gnu Public License.

When public key cryptosystems such as RSA or DSS are used for authentication, the entity being authenticated demonstrates its identity by proving that it knows a private key. But this is only half of the proof. The other half is verifying that the corresponding public key is associated with the purported identity. This requires a Public Key Infrastructure (PKI). In a traditional PKI, the binding of the public key to the identity is accomplished by a public key certificate[1]. The Entrust PKI is available on HP-UX 11. Furthermore, HP and Baltimore Technologies have recently announced an OEM agreement concerning Baltimore's UniCERT PKI. The text of the announcement can be found at http://www.hp.com/pressrel/jan00/17jan00d.htm.

[1] There are other alternatives. For example, the DNSSec protocol calls for associating keys with domain names by storing them as resource records in the DNS. However, a DNS PKI has not yet been deployed on the Internet.

IPSec

IPSec is a family of protocols that provide security for IP traffic, under development by a working group of the IETF. While some of the IPSec protocols are still evolving, the core of the specification is stable enough to permit interoperable implementations. HP introduced the IPSec/9000 product for HP-UX in February 1999. This implementation of IPSec has been shown to interoperate with over thirty other implementations, including those of Cisco and Microsoft.

IPSec protects IP traffic by establishing *security associations* between computer systems (hosts or gateways). A security association provides data confidentiality through the use of a symmetric cipher such as DES or Triple DES, and/or data integrity protection and data origin authentication through the use of a keyed message digest algorithm such as HMAC-MD5 or HMAC-SHA1. DH is used to establish the keys for the symmetric cipher and the message digest. Several methods have been proposed for authenticating the hosts that participate in the association, including the use of preshared keys derived from passwords and the use of private-public key pairs backed by digital certificates.

Since IPSec operates at layer 3 of the TCP/IP stack, it is transparent to applications. This makes IPSec ideal for protecting legacy applications such as EDI software, as they migrate from private leased-line networks to the Internet.

For the same reason, IPSec is very versatile. Figure 1 shows possible uses of IPSec at the periphery of a corporate IT network. IPSec can be used to:

- Create a secure tunnel through the public Internet between the corporate intranet and a remote branch office.
- Provide secure access to the corporate intranet through the public Internet for remote workers.
- Provide secure limited access to the corporate intranet to business partners.

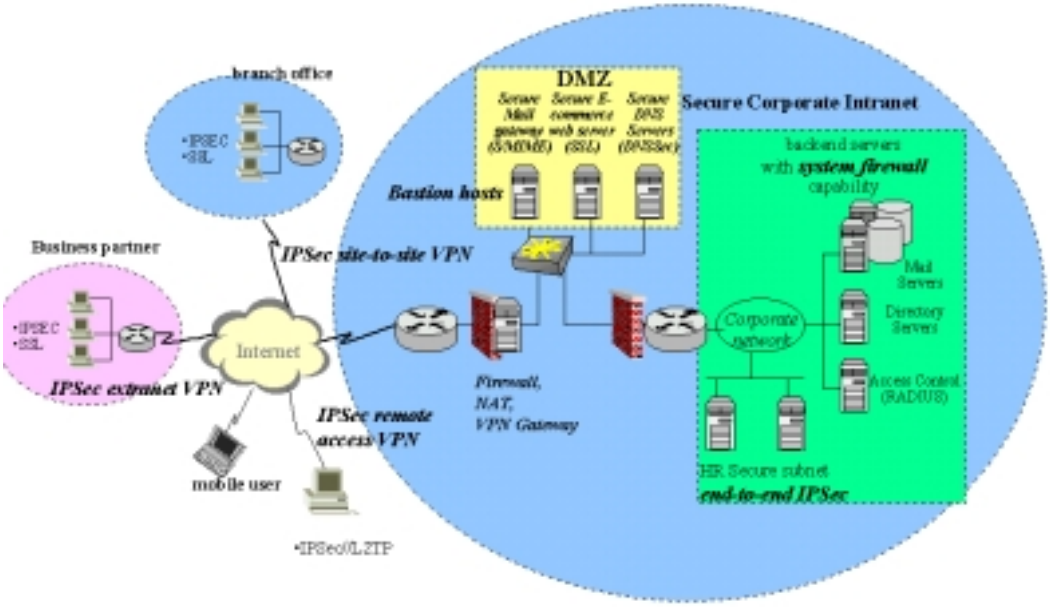


Figure 1. Different uses of IPSec

In all these cases, IPSec creates, in effect, a private network within the global Internet through the establishment of security associations. This is referred to as a Virtual Private Network (VPN).

But IPSec can also be used to provide secure links within the corporate intranet for protection against insider attacks. For example, it can be used to:

- Protect the communications between a web server in the DMZ and its back-end database server, or
- Protect the communications between computers of the personnel department throughout the corporation.

In both of these cases IPSec creates the equivalent of a secure network within the private-but-not-secure corporate intranet. By analogy with a VPN, this could be called a Virtual Secure Network (VSN).

HP-UX has pioneered the use of VSNs to protect sensitive information within the intranet by offering the IPSec/9000 product, which can be used to establish end-to-end security associations between HP-UX hosts, or to implement a tunnel-mode client.

IPSec/9000 has offered the following features, most of them since its introduction in 1999:

- *Ease-of-use*. IPSec/9000 features a GUI that allows the IPSec administrator to configure the product by pointing and clicking.
- *Flexibile authentication capabilities*. Both preshared keys and public key certificates can be used for authentication. IPSec/9000 can use Entrust or Verisign certificates, and the Baltimore PKI will be supported in the future. The IPSec/9000 administrator can obtain certificates through the GUI automatically, without any cutting and pasting between different applications.
- *Interoperability*. In VPN bakeoffs, IPSec/9000 has been able to interoperate with over 30 other IPSec implementations, including those of Microsoft and Cisco.
- *High-speed encryption*. Through the use of a hand-crafted assembly-language implementation of DES and Triple-DES for PA-RISC 2.0 that takes advantage of 64-bit registers, IPSec/9000 achieves almost twice the encryption speed of other leading software implementations.

The following additional features are being introduced in the 11i timeframe:

- Centralized policy management through an LDAP directory
- Integration with HP's VirtualVault secure web server, providing a secure channel to back-end servers.
- Support on HP 9000 series 700 systems.

The centralized policy management feature deserves special attention.

Centralized policy management

The most common method for configuring secure end-to-end communication policies is to configure each node individually. This nodal configuration works well when both the total number of nodes and the amount of effort required for configuring each policy is small. For large, security-conscious enterprises, this is not usually the case. However, the large-scale deployment of directory services allows the enterprise to centralize security-policy management.

In a nodal management scheme, policies must be configured on each individual node that is to participate in secure communications. Most of the time, this configuration is the same on each node. Sharing the policy configurations using a central resource like a directory server allows the configuration to be

performed only once for several nodes. This is a much more efficient use of an administrator's time. This efficiency becomes much more pronounced when trying to troubleshoot configuration problems. Since there is only one configuration, there is only one place for the administrator to look for configuration problems.

IPSec/9000 will soon feature centralized management of IPSec policies across multiple HP-UX systems through an LDAP directory. Furthermore, HP intends to contribute to the IETF effort to define a common policy configuration schema that will allow the centralized management of IPSec products from multiple vendors. IPSec/9000 will implement the common schema as soon as it is defined.

Kerberos

The HP-UX operating system implementation of the Kerberos version 5 protocol provides enterprise-wide strong user authentication. The validity of user passwords is verified by a central Kerberos server, but the passwords themselves are not transmitted over the network. Kerberos also provides secure key exchange between application clients and servers. Application programs can take advantage of this facility through the use of the GSS-API.

HP-UX login can use any Kerberos 5 Key Distribution Center (KDC), such as an MIT Kerberos Server or a Microsoft Windows 2000 Domain Controller. This achieves common authentication functionality in a heterogeneous intranet including other Unix hosts and Windows 2000 workstations. Furthermore, the HP-UX implementation of Kerberos supports the password-change protocol, which automates the propagation of password changes. These two features can significantly reduce user administration complexity in a heterogeneous environment.

As specified in RFC 1510 of the IETF, Kerberos uses DES, which has a fixed key length of only 56 bits. It is expected that stronger encryption algorithms, such as Triple DES or the forthcoming AES, will be specified for use with Kerberos in the near future.

The Kerberos protocol

The Kerberos protocol provides secure authentication and key exchange among *principals* that communicate over an open, non-secure network. Each principal shares a secret key with a central Key Distribution Center (KDC). Principals can be users or applications. The key of a user is derived from a password known to the user, while the key of an application server is stored in a *keytab* file.

Figure 2 illustrates the Kerberos protocol. The KDC has two components, an Authentication Server (AS) and a Ticket Granting Server (TGS). The application client is a login process acting on behalf of the user. The principal, in this case, is the user. The application server, on the other hand, is a program which plays the role of a principal.

The basic building block of the protocol is simple. The KDC provides the client with *credentials* that the client can use to request service from an application server on behalf of the user. These credentials comprise a *session key* and a *ticket*. The session key is sent encrypted with a key shared by the KDC and the client, which may be a long-term key derived from the user's password or a previously established session key. The ticket, on the other hand, is encrypted under the long-term key that the KDC shares with the application server. It contains the same session key, as well as the user's name, an expiration date, and an integrity checksum. The ticket can be viewed as a sealed letter from the KDC to the application server containing the session key and asserting that whoever else knows the session key is acting on behalf of the user named in the ticket. The client sends the ticket to the application server, together with an *authenticator*, which consists of a timestamp encrypted under the session key. The authenticator demonstrates that the client knows the session key and thus is acting on behalf of the user. As the application server decrypts the ticket, the session key becomes a shared secret between the client and the application server, from which they can derive key material to establish a secure connection providing data integrity protection and confidentiality.

The complete protocol consists of the steps shown in Figure 2:

1. The client requests login credentials from the AS including a *ticket-granting ticket* (TGT) to be used for accessing the TGS.

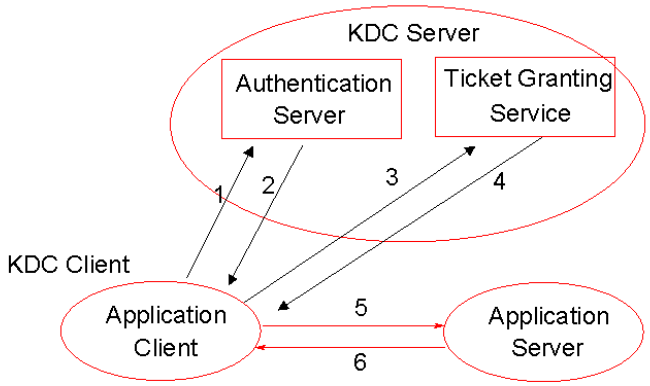
2. The KDC sends login credentials to the client, comprising a TGT and an encrypted *login-session key*. The TGT is encrypted under a secret key known only to the KDC, and the login-session key is encrypted under the user's long-term key, derived from the user's password. The client prompts the user for his or her password, derives the long-term key from the password, and uses it to decrypt the login-session key. Then the client destroys the password and the long-term key. From now on, the client can use the login credentials to demonstrate that it is acting on behalf of the user, rather than the user's password or long-term key. This reduces the exposure of the long-term secret material to capture by Trojan horse software.

3. When the user invokes an application, the client requests credentials for the application server from the TGS. To this purpose, it creates an authenticator with the login-session key and it sends the TGT and the authenticator to the TGS.

4. The TGS decrypts the TGT, extracts the login-session key, verifies the authenticator, and sends credentials for the application to the client. These credentials comprise a *service ticket* and an encrypted session key. The service ticket is encrypted under the key that the KDC shares with the application server, and the session key is encrypted under the login-session key.

5. The client decrypts the session key with the login-session key, creates an authenticator with the session key, and sends the service ticket and the authenticator to the application server.

6. The application server decrypts the service ticket, extracts the session key, and verifies the authenticator. If mutual authentication is required, the application server creates an authenticator by encrypting the timestamp sent by the client under the session key extracted from the ticket, and sends the authenticator to the client.



1. Client requests login-session credentials from AS
2. AS sends TGT and login-session key
3. Client submits TGT and authenticator to TGS, requests credentials for application server
4. TGS sends service ticket and session key
5. Client submits ticket and authenticator, requests service
6. Application server sends authenticator (if mutual authentication is necessary)

Figure 2. The Kerberos protocol

Now the session key is a shared secret between the client and the application server. They can use it to derive symmetric keys for encryption and data integrity protection, which can be used to establish a secure channel for transmission of application data. Alternatively, the client may send a sub-session key in step 5, as a field of the encrypted authenticator, and this sub-session key may be used instead of the session key to derive encryption and integrity keys.

Kerberos library and utilities

HP-UX 11i provides Kerberos utilities and Kerberos client libraries compatible with the MIT reference implementation. The Kerberos utilities, delivered as part of the OS core, comprise the following tools:

- **kinit** obtains and caches the ticket-granting-ticket (TGT) and login-session key.
- **klist** lists the tickets and associated session keys in the credentials cache.
- **kdestroy** removes a principal's login context and associated credentials.
- **kpasswd** manages the user passwords and the corresponding long-term keys stored by the KDC.
- **ktutil** maintains the keytab files.
- **kvno** returns the revision number

Kerberos client libraries, also on HP-UX 11i OS core, can be linked in either 32 or 64-bit mode.

User authentication through Kerberos

As a special case of the protocol shown in Figure 2, Kerberos can also be used to authenticate the user to the user's own host. In this case, the user's host plays the role of the application server, while the user's login process plays the role of the client as before. The host is a principal. It shares a key with the KDC, which it stores in its keytab file. At login time, after it has obtained the TGT and login-session key, the login process obtains credentials for the host itself. These credentials comprise a session key and a service ticket encrypted under the host's key. The login process submits the service ticket and an authenticator to the host's OS, which allows the user to complete the login only after decrypting the ticket and verifying the authenticator with the session key extracted from the ticket.

HP-UX provides Kerberos authentication as part of the Pluggable Authentication Module (PAM) architecture, specified in RFC 86 of the Open Group. PAM allows multiple authentication technologies to coexist on HP-UX, as shown in Figure 3. A configuration file determines which authentication module is used, in a manner transparent to the applications that use the PAM library.

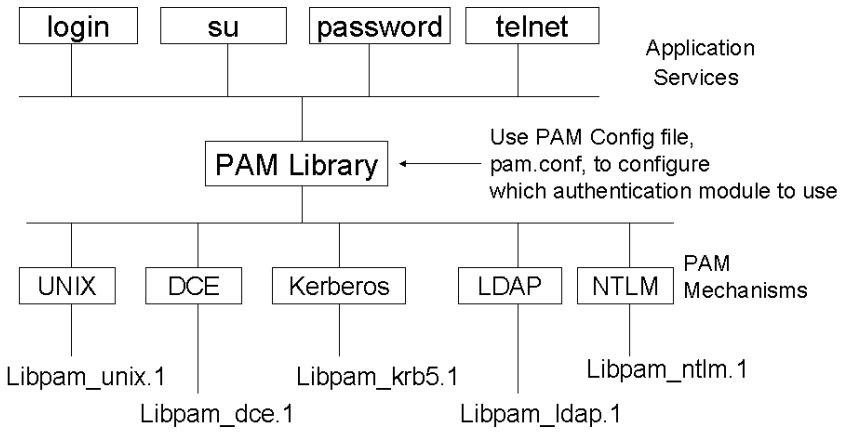


Figure 3. HP-UX authentication and PAM

The HP-UX applications using PAM include telnet, login, remsh, ftp, rexec, rlogin, dtlogin, and rcp. PAM Kerberos interoperates with a KDC operating on either a UNIX server or a Microsoft Windows 2000 server. PAM NTLM authenticates HP-UX users against a Microsoft Windows NT 4.0 domain controller using the NT LanManager protocol.

Kerberized applications

PAM Kerberos authenticates the user to the local host. As pointed out above, this is a special case of Kerberos authentication. The general case, on the other hand, makes it possible to authenticate the user to an application running on a remote host. Applications that have been modified to take advantage of this more general Kerberos authentication capability are said to be *kerberized.*

As a concrete example of a kerberized application, consider telnet. When using kerberized telnet to access a remote host, the user is not prompted for a password. Instead, the local host uses the credentials obtained from the KDC when the user first logged in to the local host (login-session key and TGT) to obtain credentials for the remote host (session key and service ticket). It uses the session key to create an authenticator, and sends the authenticator and the service ticket to the remote host. The kerberized telnet server on the remote host verifies the user's identity by decrypting the service ticket and verifying the authenticator. No password is used.

To better understand the difference between these two uses of Kerberos (PAM Kerberos vs. kerberized applications), it may be useful to compare the use of kerberized telnet just described to the use of ordinary telnet in conjunction with PAM Kerberos authentication on the remote host. If telnet is not kerberized, the telnet server on the remote host creates a login process that prompts the user for a password. This password is sent over the network to the remote host. The login process on the remote host uses the password to authenticate the user. If the remote host is configured to use PAM Kerberos, then it will rely on the Kerberos KDC to validate the password, using the process described in the previous section. The password will not travel over the network between the remote host and the KDC. However, the password has previously been sent over the network from the local host.to the remote host. This cannot be avoided by PAM Kerberos nor by any other login authentication method on the remote host. To avoid this, kerberized telnet should be used.

HP-UX 11i includes the following kerberized Internet services: ftp, rcp, rlogin, telnet, and remsh. When these kerberized services are used, the password is not sent over the network. This eliminates a major vulnerability. On the other hand it must be pointed out that these services do not establish a secure connection after the initial authentication. Therefore an active attacker may be able to hijack the connection after it has been established. IPSec/9000 can be used to prevent this.

Application developers can use the Kerberos libraries, or the GSS-API equipped with the Kerberos mechanism, described in the next section, to implement kerberized applications. If active attacks are a concern, these applications can use the shared secret established by Kerberos between application client and server to set up a secure connection. The GSS-API makes it easy to do this. Alternatively, active attacks such as connection hijacking can be blocked by establishing an IPSec security association between client and server.

GSS-API

The Generic Security Services Application Program Interface, GSS-API, specified in RFC 2743 of the IETF, provides security services for client-server applications independent of various underlying communication protocols. The services include authentication, integrity and confidentiality of data. The system administrator can configure the quality of protection to use for an application with no modification at the application level.

The Common Authentication Technology working group of the IETF has defined several cryptographic mechanisms that can be used to implement the security services provided by GSS-API. Which mechanism is used is transparent to applications. One of these mechanisms is Kerberos. 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 comprising 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.

SSL

The SSL protocol provides secure connections between web browsers and servers. An HTTP connection secured by SSL is indicated by the use of the HTTPS protocol identifier in a URL. Secure connections are used in electronic shopping applications when the user accesses the check-out register and has to enter secret or sensitive data, such as a password, a credit card number, or personal information. They are also used in home banking or other financial applications to protect access to the user's account. For utmost web server security, the HP Praesidium VirtualVault secure web server combines the connection security provided by SSL with the platform security provided by a special version of HP-UX obtained by adapting a military-grade, B1-version of the operating system to commercial use.

The SSL protocol begins with a handshake that uses public-key cryptography for authentication and key exchange. In the simplest and most frequently used variation of this handshake, the server performs a single RSA operation, using its private key, to decrypt a secret value which the client has encrypted using the server's public key. This allows the server to demonstrate its identity and establish a shared secret with the client, from which session keys can be derived to protect the subsequent connection. Although the server performs only one RSA operation, this operation is computationally so demanding that it can become a bottleneck, limiting the number of SSL connections per second that can be established by the server.

RSA operations, especially the more demanding private-key operations, are highly amenable to hardware acceleration. A cryptographic engine equipped with a large-integer multiplier can perform the operation faster than a general-purpose CPU. Moreover, the amount of data involved in an operation is negligible when compared to the amount of computation that has to be performed on the data. Thus is makes sense to offload the computation to a coprocessor board that plugs into an I/O slot of the server.

The HP Praesidium SpeedCard is such a cryptographic coprocessor. It uses the FastMAP cryptographic engine of Rainbow Technologies, which performs a 1024-bit RSA private key operation in only 5ms, thus achieving a thruput of 200 operations per second. (A version of the card carrying three FastMAP chips achieves a thruput of 600 operations per second is also available from Rainbow Technologies.) The SpeedCard is available for practically all HP-UX servers and workstations, including both newer models equipped with PCI I/O buses and older models having proprietary HSC buses.

The SpeedCard can provide a performance improvement of up to two orders of magnitude for web servers that carry a substantial load of SSL connections and use NES versions 2.x or 3.x. These versions of NES predate an optimization of the RSA algorithm for PA-RISC 2.0 introduced in NES version 4.0.

The SpeedCard works with VirtualVault and supports other software such as Entrust File Toolkit or Clearcommerce. Software developers can take advantage of the SpeedCard to improve the performance of their applications through the Cryptoki API, versions 1 or 2.01, specified in the Public Key Cryptographic Standard #11 of RSA Laboratories, or through Rainbow Technologies' SwiftAPI.

Packet filtering

A corporate intranet must be protected against intrusion and denial-of-service attacks by one or more *perimeter firewalls*. Application proxy firewalls, such as the HP Praesidium E-Firewall, provide highly effective protection by inspecting the data as seen at multiple levels of the network stack, including the application level.

However, individual hosts may need their own special protection against external or internal attacks. This is true for bastion hosts directly accessible from the Internet, or hosts in the DMZ. It is also true, within the corporate intranet, for hosts that store sensitive information, such as financial, personnel, or intellectual property databases, or hosts that provide essential network services, such as routing or domain name services.

One way of protecting HP-UX hosts is through the use of IPSec/9000. IPSec/9000 can be configured to establish authenticated security associations with selected hosts, and discard all packets that do not belong to a security association. For example, IPSec/9000 could be used to create a Virtual Secure Network (VSN) linking together all the hosts that handle personnel information within the corporate intranet.

Another way of protecting hosts in the intranet is through the use of system firewalls. 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. IP Filter, a popular public-domain stateful inspection firewall, is provided free-of-charge for use as a system firewall on hosts running HP-UX 11i.

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.

LDAP Authentication in HP-UX

As enterprises grow and demands for computing resources grow even faster, the cost of administration of these systems grows as quickly. In a highly distributed environment, local security practices and administration methods are inconsistent, redundant, and difficult to audit. Some tools, such as NIS[2], attempt to address some of these issues, but can be pushed to capacity in a large environment. Enterprise IT architects are evaluating LDAP directories as one tool to help unify many of the above practices.

LDAP directories can play many roles in an enterprise. Some typical uses include maintaining employee or customer data. As an example, many LDAP directories are used to provide an address database for email applications. Moreover, the role of LDAP directories is expanding greatly. For example, LDAP directories are also used to store common configuration profile information for enterprise applications and network management. As an example, the centralized policy management feature of the IPSec/9000 product described above uses LDAP as its central repository. LDAP directories have the potential for providing both centralized and delegated administration of applications, networks, employee data, etc.

HP has realized the potential power of LDAP directories and integrated the HP-UX operating system with LDAP. To help facilitate integration of LDAP and HP-UX, HP provides the Netscape LDAP Directory Server as a software bundle, free for intranet use. The Netscape Directory server is available on the 11i release through the application CDs, or it can be download from http://software.hp.com.

In addition, HP has added support for LDAP in the operating system itself. This first step towards

[2] NIS (Network Information Service) and PAM (Pluggable Authentication Module) are a components of the ONC+™ subsystem, developed by Sun Microsystems.

integration uses LDAP servers as both an authentication and naming service for HP-UX. This use of LDAP provides a scalable and more powerful alternative to an NIS-type architecture.

Aside from scalability, LDAP directories, with the help of a meta-directory if needed, offer the promise to integrate many disparate applications, such as HP-UX account information and a human resources (HR) database, thus consolidating data and administration. For example, a name change in a HR database could result in a change of the *finger* information for an HP-UX account.

LDAP-UX Integration

HP provides two products that facilitate integration of HP-UX and LDAP directories. These are the *LDAP-UX Client Services* and the *NIS/LDAP Gateway*.

Thanks to the NIS schema, defined by RFC 2307[3], HP-UX accounts, groups and other data can be stored in an LDAP directory. By default, the LDAP-UX Integration products use this schema to reference entries in the directory.

LDAP-UX Client Services

The LDAP-UX Client Services product provides both an LDAP-based pluggable authentication module (PAM) and a name service switch (NSS) module. These two modules provide seamless integration between HP-UX applications and the LDAP directory.

When an application needs to discover account information, it calls one of the name service APIs, such as getpwnam() or getpwuid(). This class of routines is part of the front-end to the NSS subsystem. The NSS subsystem then determines, through the /etc/nsswitch.conf configuration file, which back-end module should handle the request. If the nss_ldap module is chosen, it converts the request into an LDAP search operation, and returns the results to the caller.

Applications that wish to authenticate users (such as login or an ftp daemon) use PAM, which is a similar modular subsystem. As shown in Figure 4, the PAM front-end uses the /etc/pam.conf file to determine which back-end module should handle an authentication request. If the pam_ldap module is selected, it converts the authentication request into an LDAP bind operation. (Initially only ldap_simple_bind is used by pam_ldap.) Depending on the success or failure of the LDAP bind, the pam_ldap module returns success or failure to the caller. In addition to authentication, the pam_ldap subsystem supports password modification and password policy notification (e.g. when a password expires). One advantage of the PAM subsystem is that any transform supported by the LDAP server may be applied to the password before it is stored. The Unix *crypt* transform is traditionally used by Unix systems, but other transforms may provide better resistance to brute force or dictionary attacks.

The following diagram shows how LDAP is used with the PAM and NSS subsystems.

[3] Howard, *An Approach for Using LDAP as a Network Information Service*, RFC 2307, ftp://ftp.isi.edu/in-notes/rfc2307.txt

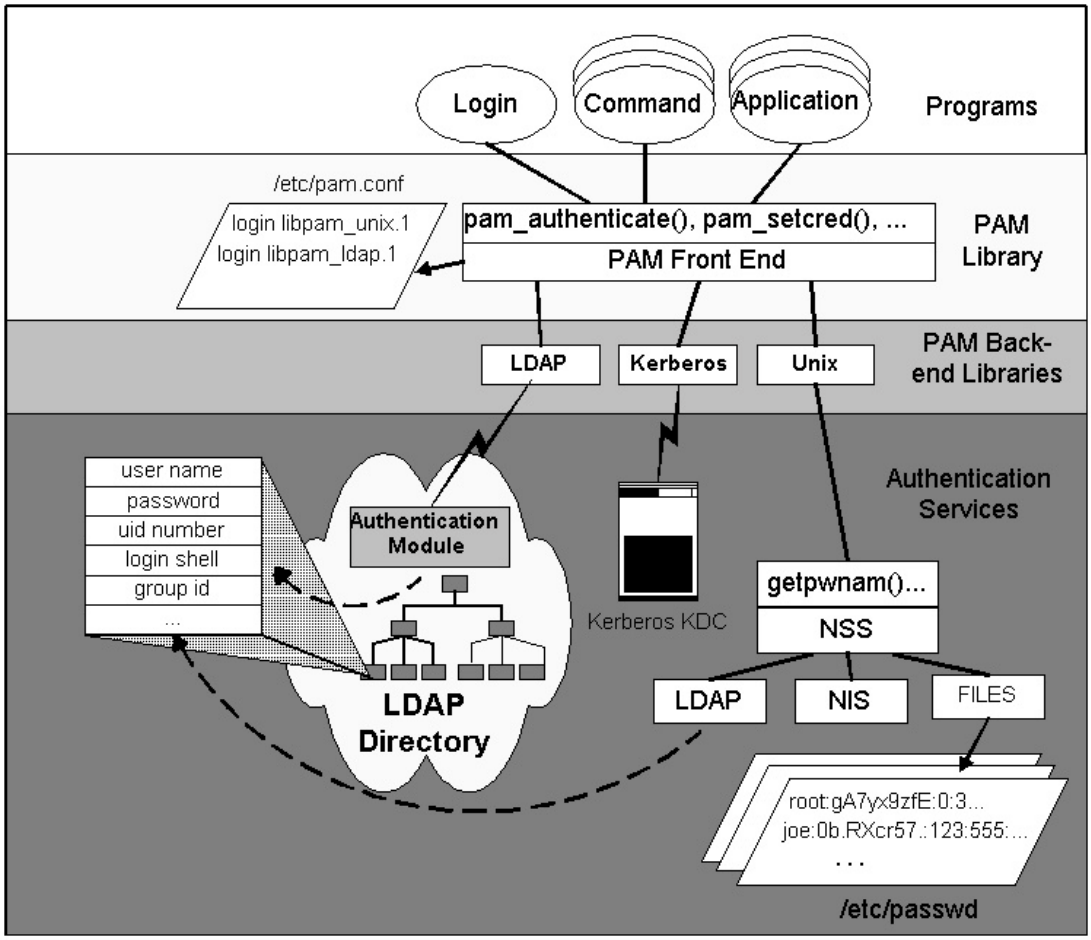


Figure 4. Integration of LDAP with PAM and NSS

NIS/LDAP Gateway

The NIS/LDAP Gateway converts NIS requests from a client into LDAP queries, then converts and returns the responses to the client. NIS is another module that is part of the NSS subsystem. NSS requests for account, group or other data assigned to this module are converted to NIS RPC requests, and are handled by the NIS/LDAP Gateway (also known as YPLDAP.) The ypldapd daemon converts the NIS RPCs into similar LDAP search operations, and then converts the response back into an NIS RPC reply.

The NIS/LDAP Gateway is easy to deploy in environments that use NIS today, where it can replace existing NIS servers, as shown in Figure 5 below. An LDAP server plays the role of an NIS master server, while YPLDAP servers replace the NIS slave servers.

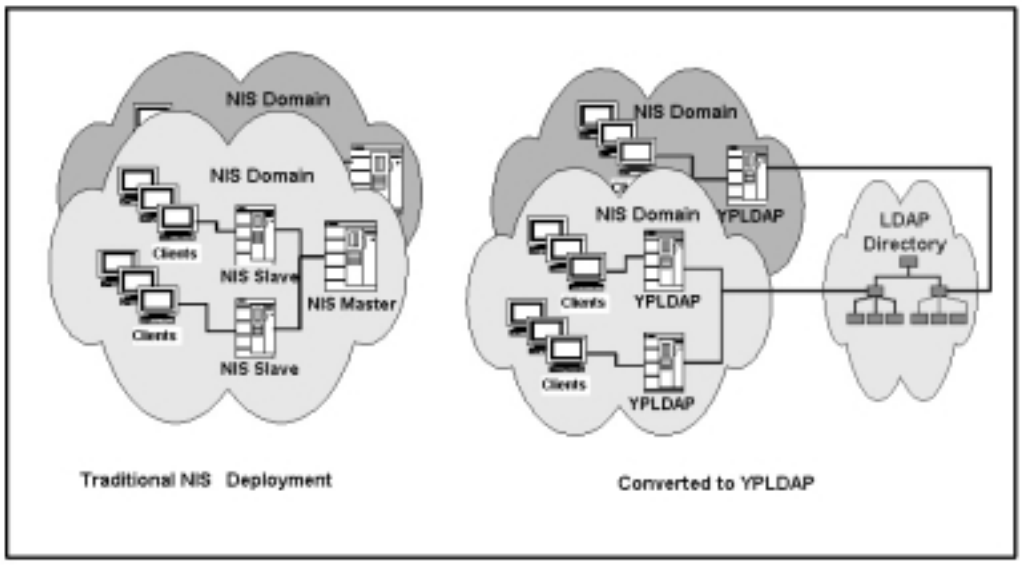


Figure 5. YPLDAP can replace existing NIS servers.

Password security considerations

LDAP-UX Client Services and the NIS/LDAP Gateway each have their own security advantages and limitations.

LDAP-UX Client Services has the advantage that passwords can be stored in the directory in any format supported by the LDAP server. Some of these formats may be stronger than crypt. On the other hand, only the simple_bind method for accessing the directory is currently supported. This means that the password is transmitted to the directory in the clear if no additional precautions are taken. However, the underlying communications channel can be effectively protected against passive and active attacks by IPSec/9000, which is available free of charge with HP-UX. The combination of IPSec/9000 and LDAP Client Services provides a highly secure authentication service.

The NIS/LDAP Gateway, on the other hand, uses the Unix crypt transform. Passwords are stored in the directory in crypt format. When the user logs in, the crypt transform of the password is retrieved from the directory by the gateway and sent to the NIS client, where it is compared with the crypt transform of the password typed in by the user. Thus, the password is not sent in the clear over the network. However, the crypt transform of the password, if snooped on the network, is vulnerable to dictionary or brute force attacks carried out by password cracking programs. Such programs are readily available and are highly effective against poorly chosen passwords. Therefore the underlying communication channels between the directory and the gateway, on one hand, and between the gateway and the client on the other hand, should by protected by IPSec/9000.

Additional white papers discuss the LDAP-UX Integration products in detail. Please refer to the end of this white paper for references to other documentation.

Security features of internet services

Internet services include the domain name system, electronic mail, routing, and facilities for file transfer, remote login, and remote shell execution.

Domain name system

The HP-UX DNS services are provided by the Berkeley Internet Naming Daemon (BIND). The version that is shipped in HP-UX 11i is BINDv8.1.2. In this version of BIND, all DNS client-server transactions are protected by ACLs. On a name server, ACLs control the following:

1. Who can query the name server.
2. Who can initiate zone transfers from the name server.
3. The name servers to which queries can be sent.
4. Who can request dynamic updates.

It must be noted that 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. HP-UX, however, makes it possible to prevent IP address spoofing through the use of IPSec/9000.

The IETF is addressing the security limitations of the Internet DNS through the introduction of DNS security protocols, including DNSSec, TSIG, and TKEY. In the near future, HP-UX will include the next version of BIND (BINDv9), which will contain implementations of these protocols.

DNSSec

DNSSec, specified in RFCs 2535 and 2541of the IETF, is a comprehensive Proposed Standard that provides the following services:

- 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.

- It binds public keys to domain names using KEY Resource Records, which are themselves stored as zone data protected by SIG records. It thus provides a public key infrastructure, an alternative to traditional PKIs based on public key certificates.

TSIG

Because public key cryptography is complex and computationally expensive, there are many situations in which a lighter approach is desirable. The TSIG protocol protects DNS transactions using symmetric-key cryptography rather than public-key cryptography. Specifically, the integrity and origin of the data exchanged in a transaction is protected by HMAC-MD5, using a key shared by both participants in the transaction. This key must be securely distributed to the participants. Key distribution can be accomplished by a manual configuration process. Note that TSIG does not provide zone data integrity or secure binding of public keys.

TKEY

The TKEY protocol addresses the problem of distributing shared keys for the TSIG protocol by allowing participants in DNS transactions to establish shared secret material.

Gated (Routing)

Gated is the routing daemon in HP-UX. Gated supports two internal routing protocols, RIP and OSPF, as well as an external routing protocol, BGP. Gated provides configurable options to rank routing information sources from most trustworthy to least trustworthy and to accept information about any particular destination from the most trustworthy source first. It also provides means to filter out some of the obviously invalid routes (such as those for net 127). In addition to this, gated has an extensive tracing facility which can be used for auditing.

Apart from the generic features that gated provides for security, there are a set of specific security features supported by each of the routing protocols. The following sections describe some of the features offered by each protocol, and how they can be used.

RIP

One of the most widely used interior gateway protocols is the Routing Information Protocol (RIP). RIP is an implementation of a distance-vector, or Bellman-Ford, routing protocol for local networks. Gated supports RIP version I and version II.

RIP II packets may contain one of two types of authentication strings that may be used to verify the validity of the supplied routing data. Authentication may be used in RIP-I-compatible RIP II packets, but be aware that RIP I routers will ignore these packets (unless nocheckzero is selected). The first method consists of a simple password. An authentication key of up to 16 characters is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security because it is possible to learn the authentication key by snooping RIP packets.

The second method uses the MD5 algorithm to create a cryptographic checksum, or digest, of a RIP packet and an authentication key of up to 16 characters. The transmitted packet does not contain the authentication key itself, it contains the digest instead. The key is a shared secret between the communicating routers. The receiving router will perform the same digest computation and discard the packet if the digest does not match. In addition, a sequence number is maintained to prevent the replay of older packets. This method provides a much stronger assurance that routing data originated from a router with a valid authentication key.

A primary and a secondary authentication method can be specified for each interface. Packets are sent using the primary method. Incoming packets are checked first with the primary method. If that fails, they are checked with the secondary method. If both methods fail, they are discarded. In addition, a separate authentication key is used for non-router queries.

OSPF

Open Shortest Path First Routing (OSPF) is a shortest path first or link-state protocol. OSPF is an interior gateway protocol that distributes routing information between routers in a single autonomous system.

All routing packets sent from an OSPF router are authenticated. However, one method of authentication is “none”. Authentication can help to guarantee that routing information is only imported from trusted routers. A variety of authentication schemes can be used, but a single scheme must be configured for each interface. The use of different schemes enables some interfaces to use much stricter authentication than others. The three authentication schemes specified in RFC 2178 of the IETF, are: none, simple and MD5 authentication.

Simple authentication is achieved by including the authentication key of up to 16 characters in the packet carrying routing information, as in the first authentication method of RIP. The key can be snooped as the packet is sent over the network.

MD5 authentication is achieved by including a digest computed with a shared secret key, as in the second authentication method of RIP. The key is not sent over the network. RFC 2178 allows multiple MD5 keys per interface.

BGP

The Border Gateway Protocol (BGP) is an exterior, or inter-domain, routing protocol used for exchanging routing information between autonomous systems.

A BGP router is configured to exchange routing information only with a specified set of peer BGP routers in other autonomous systems, over TCP connections. Furthermore, routing policy is used to restrict the

routes that can be advertised to or accepted from each of those peer routers. If desired, an underlying transport security protocol such as IPSec can be used to secure the communications with the peer routers.

Inetd

The inetd daemon is the internet superserver, which invokes internet server processes as needed. When inetd accepts a connection from a remote system, it checks the address of the host requesting the service against the list of hosts to be allowed or denied access to the specific service (see inetd(1M)). The file inetd.sec allows the system administrator to control which hosts (or networks in general) are allowed to use the system remotely. This file constitutes an extra layer of security in addition to the normal checks done by the services. It precedes the security of the servers; that is, a server is not started by the internet daemon unless the host requesting the service is a valid host according to inetd.sec.

Note that inetd.sec is a legacy Unix security feature which relies on the source IP addresses of an incoming packet to identify the sender, and thus can be defeated by IP spoofing. As pointed out above, however, HP-UX makes it possible to prevent IP address spoofing through the use of IPSec/9000.

Sendmail

Sendmail is the mail transfer agent that is available in HP-UX. Mail transfer agents are responsible for routing email through the network until it reaches its final destination. The current version of sendmail shipped with HPUX is sendmail-8.9.3.

Sendmail 8.9.3 has many built-in security related features which are listed in the following paragraphs. These features make sendmail more robust, reliable and secure.

Anti-spamming

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 anti-spam features available in sendmail-8.9.3 are:

1) Access database
2) Relaying denied by default
3) Better checking on sender information
4) Header checks

Access database. The access database is a user-defined file, used to decide the domains from which the user wants to receive or reject mail messages. The entries in the access database file are keyed by domain names, IP addresses, hosts names or e-mail addresses. Each entry determines the action to be taken upon receipt of a message whose origin matches the key. The action can be to accept the message, relay it, reject it, or respond to it with a specific error message.

Relaying denial. Transmission of messages from a site outside the host’s domain to another site outside the domain (relaying) is denied by default. There are configuration options that can be used to selectively relay messages from certain hosts.

Better checking on sender information. Sendmail-8.9.3 will refuse mail if the sender has an unresolvable domain name. This behavior can be enabled by the use of the access database mentioned above. Sendmail can also be configured to reject mails for certain recipients.

Header checks. Sendmail-8.9.3 is capable of checking headers other than the *from* and *to* headers. It can filter messages based on the value of other headers. This feature makes it possible to reject messages based on *subject* or any other standard header format. However, enabling this feature may affect the performance of sendmail, since it requires parsing the entire header.

Denial of service

Sendmail 8.9.3 has configurable options to check the system load and queue requests or drop connections based on the current load.

Other security enhancements

Sendmail 8.9.3 strictly checks the permissions of files and directories to avoid compromising security. For example, it ensures that the ".forward" file in the user's home directory, if present, has permissions 600. This ensures that it can only be read or written by the user. Furthermore, it ensures that it always runs with root as effective user id and mail as effective group id.

Sendmail uses the syslog file very extensively. It compiles accounting data for every message received or exhanged, and can provide usage statistics per user or per domain.

Sendmail uses identd for authentication of the real users. This helps in identifying and isolating bogus users and thereby protecting the system against misuse.

When it starts up, sendmail reads the contents of the aliases file into a database that it keeps in main memory. A subsequent modification of the aliases file will not affect the runtime behavior of sendmail. This provides some protection against mail spoofing.

Secure internet services

The secure internet services (SIS) bundle contains the following commands:

1. ftp
2. rcp
3. rlogin
4. telnet
5. remsh

When secure internet services are enabled all of these products use Kerberos for authentication as described above. Thus passwords do not have to be sent in the clear over the network.

If SIS is not enabled, these internet services use PAM for authentication. The authentication mechanism can be configured using the file /etc/pam.conf.

Cryptography

Data security in a network environment requires cryptography. Cryptographic algorithms are built into the network security protocols described above. Developers may also want to use cryptographic algorithms to fulfill the specific security needs of their distributed, network-based applications. The broadest range of cryptographic APIs and toolkits are available on HP-UX 11i, including BSAFE, the Entrust Toolkits, GSS-API, CDSA, as well as SwiftAPI and Cryptoki for access to the HP Praesidum SpeedCard. GSS-API and CDSA are provided free-of-charge with HP-UX. More information on GSS-API can be found above, in the section on Kerberos. More information on CDSA can be found in the white paper on core HP-UX security.

Cryptographic algorithms are computationally intensive and cryptographic computations can be the bottleneck that determines overall system performance. Therefore the performance of cryptographic algorithms can have a direct impact on the cost-effectiveness of network security solutions. HP has made and will continue to make a determined effort to achieve and maintain leadership in cryptographic performance.

Starting with version 4.1, the popular BSAFE toolkit of RSASecurity, Inc. includes an optimized version of the RSA algorithm for PA-RISC platforms. The inner loops of the modular exponentiation algorithm used for RSA operations were carefully handcrafted in PA-RISC assembly language by HP experts. As a result, applications built with the BSAFE toolkit can perform RSA operations substantially faster on HP-UX platforms than on other platforms. We have measured a latency of only 7.2 ms on a 440 MHz CPU for an RSA private key operation with a 1024-bit modulus, using the currently available BSAFE toolkit. A further optimization, already implemented in the laboratory, will bring this latency down to only 6.4 ms, again on a 440 MHz CPU. We expect that this faster implementation will be made available in the timeframe of HP-UX 11i.

HP has also worked with Netscape to optimize the performance of the RSA operation used by SSL for server authentication, using the same assembly language inner loops. In many cases, this RSA operation can be the bottleneck that limits the performance of a secure web server. The optimized code is present in version 2.7 of Netscape Security Services , which in turn is used by Netscape Enterprise Server (NES) 4.0. Again the result of the optimization has been substantially faster performance of NES 4.0 on HP-UX than on other platforms.

Furthermore, as mentioned above in connection with SSL, the HP Praesidium SpeedCard can be used to offload public-key cryptographic operations to a coprocessor board that plugs into an I/O slot of a server or workstation. The SpeedCard implements RSA, DH and DSS, and is equipped with a true random-number generator. It can perform a private-key RSA operation with a 1024-bit modulus in 5ms, which yields a throughput of 600 operations per second in a version of the card equipped with three cryptographic engines.

HP has also developed an industry-leading implementation of DES and Triple DES in CBC mode, which is featured in the IPSec/9000 product. The CBC loop is entirely written in PA-RISC assembly language and takes advantage of the 64-bit registers of PA-RISC 2.0 processors. To our knowledge, this is the only 64-bit implementation of DES and Triple DES available so far in a commercial product. It incorporates state-of-the-art techniques featured in academic implementations and additional proprietary techniques invented at HP. The Triple DES implementation achieves a latency of only 7.35 clocks per bit. (This figure is derived from a measurement of a 74.8 Mb/s thruput for Triple-DES in CBC mode on a 550 MHz processor.) This is almost twice as fast as other leading software implementations.

Looking forward, HP has unique expertise and tools to handcraft IA-64 implementations of cryptographic algorithms. Researchers at HP Labs have taken advantage of this to write very fast implementations of the five algorithms chosen as finalists in the competition organized by NIST to select the Advance Encryption Standard. These results have been presented at a recent NIST workshop[4]. They have also achieved an impressively fast IA-64 implementation of the RSA algorithm. Thus HP is poised to maintain its leadership in cryptographic performance as the industry moves to the IA-64 architecture.

Summary

HP-UX 11i offers a rich set of standards-based and directory-enabled network security features. Features newly available in the 11i timeframe include:

- Centralized policy management for IPSec through an LDAP directory
- 32-bit and 64-bit Kerberos and GSS-API libraries
- Kerberized implementations of internet services
- Directory-based authentication and name resolution using pam_ldap, nss_ldap, and the ypldap gateway
- Email anti-spamming capability
- Highest-performance implementation of cryptographic algorithms in hardware and software
- Multiple cryptographic toolkits and APIs

[4] J. Worley, B. Worley, T. Christian and T. Worley, AES Finalists on PA-RISC and IA-64: mplementations & Performance. In *Third AES Candidate Conference* (proceeding available at http://csrc.ncsl.nist.gov/encryption/aes/).

- Implementation of SOCKS version 5

HP-UX has been recognized as leading in network security[5]. HP is committed to maintaining and increasing this leadership position. In the near future we will focus our efforts in the following areas: centralized authentication and authorization in heterogeneous networks, interoperable directory-based management of security policy, fast cryptography for end customers and application developers, and platform protection through the use of system firewalls, OS hardening, and intrusion detection. Security is an HP core competency. Furthermore, our work in the security area will leverage our other core competencies, including performance, high availability, HP-UX/NT interoperability, and network management, in order to provide the best security solutions to our customers.

Product information

IPSec/9000 is provided free of charge as an independent software unit. It is available in two versions: a domestic version for the USA and Canada, and an exportable version for worldwide distribution. The product numbers are J4255AA for the international version and J4256AA for the domestic version. A datasheet can be found at http://www.hp.com/security/products/ipsec9000/papers/datasheet/.

The *Kerberos client lib*raries and the *GSS-API libraries* are part of the core OS in HP-UX 11i.

PAM Kerberos is available free of charge on the HP-UX application CD. The product number is J5849AA.

The *Netscape Directory Server 4.11* product is available on the HP-UX application CD. The product number is J4258BA for the exportable version and J4264AA for the domestic version available for US and Canadian customers.

The *LDAP-UX Client Services* product and the *NIS/LDAP Gateway* product are available for free on the HP-UX application CD, as part of the J4269AA product bundle.

For information on how to order HP Praesidium E-Security products, including IPSec/9000, VirtualVault, e-Firewall, SpeedCard and DomainGuard, visit the web site http://www.hp.com/security/.

For more information

Information on core HP-UX security, as well as detailed information on CDSA is available in the white paper "HP-UX Security". Instructions for hardening the configuration of an HP-UX system for use as a bastion host can be found in two white papers, *Building a Bastion Host Using HP-UX 10*, and *Building a Bastion Host Using HP-UX 11*.

For more information about the Kerberos protocol, visit the MIT web site http://web.mit.edu/kerberos/www/, or the web page of the IETF working group on Common Authentication Technology (CAT), at http://www.ietf.org/html.charters/cat-charter.html. Information on the GSS-API can also be found on the web site of the CAT working group.

Additional information on the LDAP-UX integration products can be found in two white papers, *Integrating HP-UX Account Management and Authentication with LDAP*, and *Preparing your LDAP Directory for HP-UX Integration.* These can be found at http://docs.hp.com/hpux/internet/#whitepapers.

Additional information on the HP Praesidium E-Security line of products, including IPSec/9000, VirtualVault, e-Firewall, SpeedCard and DomainGuard, can be found on the web site http://www.hp.com/security/.

[5] 1999-2000 Operating System Function Review, by D.H. Brown Associates, Inc

For more information about IETF standards, visit the web site http://www.ietf.org/. More specifically, for information on the IPSec family of protocols, visit the web page of the IETF working group on the IP Security Protocol, at http://www.ietf.org/html.charters/ipsec-charter.html.

For publications of the Open Group, visit the web site http://www.opengroup.org/.

General information on cryptography can be found in textbooks such as Applied Cryptography, by Bruce Schneier, published by John Wiley and Sons, Inc., or Handbook of Applied Cryptography, by A. Menezes, P. C. van Oorschot and S. A. Vanstone, published by CRC Press LLC.

Trademark notices