HP Integrated Lights-Out security

technology brief, 6th edition

Abstract

HP Integrated Lights-Out (iLO) is the autonomous management processor that resides on the system board of ProLiant and Integrity host servers. HP built security features into iLO using multiple layers that encompass the hardware, firmware, communication interfaces, and deployment capabilities. The intent of this technology brief is to inform readers about the design of iLO itself and how it ensures security. This paper describes the mechanisms that iLO uses to ensure authorization, authentication, privacy, and data integrity. Also described here are the utilities or services providing access points into iLO or its host system, and how the iLO design mitigates access risks. A brief summary of specific security recommendations can be found at the end of the paper.

The intended audience for this paper is engineers and system administrators familiar with Lights-Out technology. The iLO security features described in this paper reflect the release of iLO 2 v1.60 and iLO v1.91. This document supports both iLO devices; however, certain functions described herein may only be supported on one and not the other. A designation of "iLO only" or "iLO 2 only" indicates that the function is exclusive to that device. iLO firmware is backward-compatible. For example, the latest versions of iLO 2 firmware support any iLO 2 processor. For consistency and best feature support, HP recommends using the latest version of iLO 2. If no designation is present, then the function is supported on both devices. The paper is not applicable to the LO-100 processors found in ProLiant 100-series servers.

Additional information about the iLO processor and feature sets for particular iLO 2 and iLO products is available on the HP website at www.hp.com/go/iLO. A glossary in the appendix includes some common computing acronyms not defined in the text.

Introduction

Information technology (IT) administrators must plan for security across the IT infrastructure. Because Integrated Lights-Out (iLO) management processors have such powerful capabilities to modify a computer setup, it is important to have strong security surrounding the iLO device. HP carefully considered security requirements of the enterprise and designed iLO to include authentication, authorization, data integrity, and privacy.

Authentication is determining who is at the other end of the network connection. The iLO processor incorporates authentication techniques through 128-bit Secure Socket Layer (SSL) encryption.

Authorization refers to determining whether the user attempting to perform a specific action has the right to perform that action. Using local accounts, the iLO processor offers administrators the ability to define up to 12 separate users and to vary the server access rights of each. The directory services capabilities of iLO allow administrators to maintain network user accounts and security policies in a central, scalable database that supports thousands of users, devices, and management roles.

Data integrity refers to verifying that no one has altered incoming commands or data. The iLO processor incorporates digital signatures and trusted Java™ and ActiveX applets (used by the Integrated Remote Console) to verify the integrity of data.

Privacy refers to confidentiality of sensitive data and transactions. Examples of the privacy protection used in iLO are the 128-bit SSL encryption of web pages and the RC4 encryption of remote console and virtual serial port data.

Security assumptions about iLO and its environment

Persons with physical access to a server can alter the host server and the iLO setup. Therefore, it is assumed that any individual with unrestricted access to the inside of a server enclosure is a super-user or administrator. These individuals may be able (by design) to delete, modify, or reset user account information for Lights-Out management security components. For example, someone with access to the inside of a server can access the security override jumper and reconfigure iLO through ROM-Based Setup (RBSU), reprogram the iLO ROM, or reprogram the boot block.

Lights-Out incorporates layers of security and uses industry-standard methods to make the server as secure as possible. For example, cryptographic keys employed in iLO use a minimum key length of 128 bits and conform to published industry standards.

HP manufactures the servers using iLO with a process designed to protect sensitive information. Unless authorized by a "Factory Special" manufacturing process, HP retains no record of initial or default management security keys and data any longer than the manufacturing process requires. The manufacturing process does not expose sensitive key or password data to manufacturing personnel in a manner that can be used to later compromise security of the iLO processor. Each server using iLO ships with a unique, unpredictable iLO password as the default Administrator account password. This ensures security out-of-the box. Customers with specific security requirements can order HP servers with pre-configured iLO passwords or use HP deployment utilities to assign customer-specific passwords.

The iLO processor automatically enforces generation of new, unique, and site-specific keys used by SSL once a customer deploys the server. HP cannot determine these site-specific keys. The iLO management processor does not transmit these keys or any other information to HP from a customer location.

Comparing the iLO processor to other service processors

The iLO management processor and feature set have been widely accepted as the standard for servers and data centers employing remote management. The evidence to support this assertion can be found in numerous technical forums and blogs. However, this has also led to the adoption of the iLO name as a generic reference for all management processors and led to some misinformation concerning the true capabilities of iLO.

Phlashing

One example of misinformation is the claim that iLO is susceptible to “phlashing” Phlashing is a permanent denial of service (PDOS) attack. At this point, phlashing attacks are theoretical, but the possibility of such attacks was made clear in a June 2008 demonstration by Rich Smith, head of research for offensive technologies and threats at HP Systems Security Lab.[1] PDOS attacks could take advantage of weaknesses in the installation process of network-based firmware updates. The installation of rogue firmware through a PDOS attack could allow unauthorized remote server access or even permanently damage the hardware.

The iLO processor is not susceptible to phlashing, as described in the following section.

iLO strengths against common attacks

Vulnerabilities that could potentially enable phlashing and other more common attacks are unencrypted ports, lack of authentication and audit trails, vulnerability to brute force attacks, no

[1] EUSecWest security conference 2008 – “PhlashDance, discovering permanent denial of service attacks against embedded systems” - Rich Smith, HP Labs

awareness of attacks in progress, and unregulated virtual media access. While service processors produced by other vendors may be at risk from the issues described here, that is not the case with iLO.

iLO has been hardened against all of these risks:

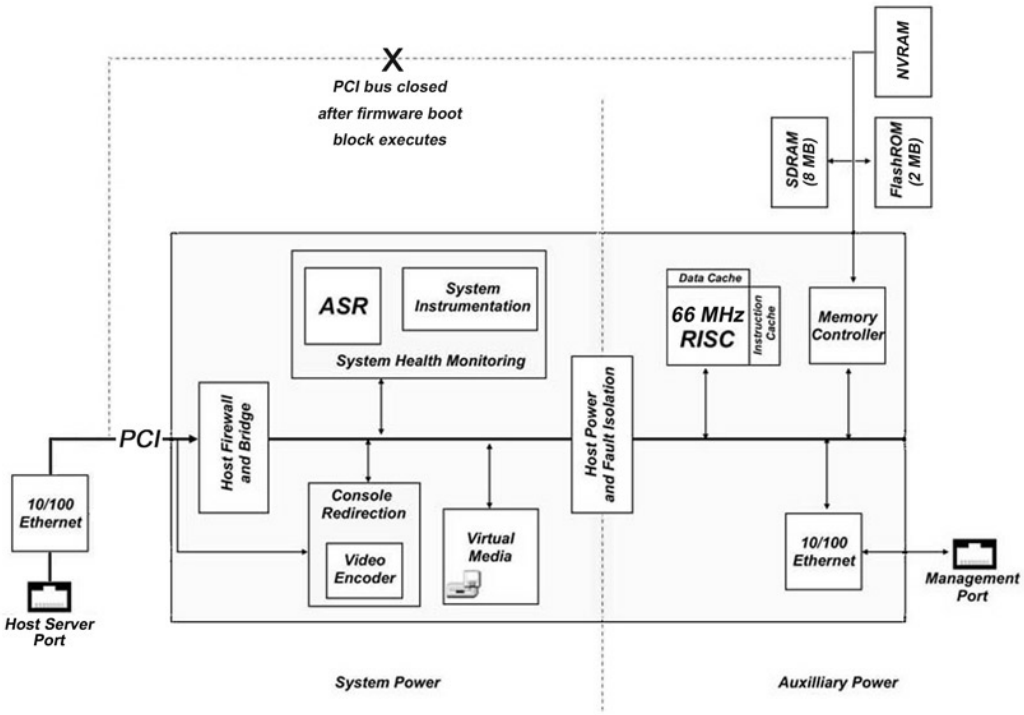
- Flash protection – iLO firmware images are digitally signed with a 1024-bit RSA public/private key and the digital signature is checked by the boot block every time iLO comes out of reset. For iLO 2 systems, the digital signature is also checked before allowing a firmware update to proceed. Flashing the iLO firmware remotely requires login authentication and authorization, including optional two-factor authentication.
- Unencrypted ports – iLO clearly defines the encryption status of the ports, and the customer can disable access to any non-encrypted ports (such as telnet). All access to iLO requires a password, or a trusted certificate if the customer so desires, unless the customer decides to disable the password (availability of this option is very limited).
- Lack of authentication and audit trails – An audit trail of authentication failures as well as successful access to the device. SSH access and failed attempts alike are logged. Using the SSH-key mode of authentication makes brute force attacks even less likely to be successful. And, iLO offers 2-factor authentication which provides an additional layer of security.
- No awareness of attacks in progress – iLO captures all login activity, successful or not. Additionally, iLO implements a progressive timed delay during unsuccessful login attempts to greatly slow the success of brute force and dictionary attacks.
- Unregulated virtual media access – iLO logs virtual media access, so potential information destroyers can be traced. Additionally, typical iLO virtual media operations are one-way, from the client to the server, so chances that critical information is copied via iLO are minimal.

All of these security issues are addressed in more detail later in this technical brief.

Security of the hardware design

The iLO processor is a 32-bit, PCI-based ASIC that includes its own 66-MHz RISC processor core with separate instruction and data caches, memory controller, NVRAM, SDRAM, FlashROM, and Ethernet controller (Figure 1). The iLO design denies or restricts access from the host server to the following areas: management ROM, memory, NVRAM, and the iLO management port.

Figure 1. Schematic diagram of the iLO processor



Management ROM

The Management ROM (flashROM) includes the iLO boot block and the iLO main firmware image. The iLO boot block is responsible for the initial hardware and software setup, location and validation of an executable image, and transfer of control to the executable image.

The iLO main image is digitally signed with an RSA[2] 1024-bit private/public key pair. The firmware image is signed with the private key known only to HP; the iLO boot block knows the public key. To produce the signed firmware image, HP uses the following firmware build process:

1. Compute an SHA 1 (Secure Hash Algorithm) hash over the entire image.
2. Encrypt and sign the SHA1 hash with the RSA private key.
3. Store the encrypted signature in the image header.

To validate and boot the signed firmware image, the iLO boot block searches memory for a viable image that contains a recognizable header. If a viable image is found, the iLO boot block decrypts the signed SHA1 hash using the RSA public key. The boot block then computes the SHA1 hash over the entire image. If the two SHA1 hashes are equivalent, the image is valid and the boot block passes control to the iLO main image to begin executing.

During the firmware flash process, an image is presented to the iLO firmware for potential flash into the Management ROM. The flash routine analyzes the incoming data stream, looking for a viable image. If iLO finds a viable image, it is flashed into the Management ROM at the next available address. Normally, the first viable image found is the main image, and it is flashed into the area just past the boot block. The flash process continues until no more viable images are detected in the incoming data stream.

[2] RSA is a public-key cryptosystem for both encryption and authentication. It was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman and is named for them.

The boot block is flashed only if the firmware flash is performed while the iLO Security Override jumper is set (disabled). For maximum security, the flash should not be performed while the iLO security jumper is set unless the specific intent is to update the boot block. It is not anticipated that the boot block will require updating; however, this mechanism is provided in case an update should become needed.

As shown in Figure 1, the management ROM can connect through a "back door" to the PCI bus on the server. Under normal circumstances, the host server CPU executes the iLO option ROM. After the host CPU locates iLO and transfers the option ROM code to the host memory, the iLO firmware closes the connection to the host PCI bus. Therefore, under normal operating circumstances, there is no chance for the server to flash the management ROM without permission. The host PCI connection remains open only if the user brings up the iLO device in safe mode (by setting the iLO Security Override jumper) or if the iLO firmware does not execute properly. This allows the host server to directly flash the management ROM through the host PCI bus if the iLO ROM is corrupted.

Firewall logic

The iLO management processor includes a host firewall and bridge logic (Figure 1) that enables iLO to control the flow of information between the host server and the management console. The firewall logic protects against unauthorized access through the host system PCI bus and therefore shields sensitive keys and data that are stored in memory and firmware.

Memory

The iLO management processor contains three classes of memory registers:

- General registers, which the host server can access through the PCI bus. These PCI registers contain only non-sensitive information. The iLO processor does not secure or try to hide these registers from the host server.
- Protected registers, in which the iLO device can lock the write access. These registers restrict unwanted behavior, such as flashing rogue firmware, but they do not restrict information. These registers are unlocked in safe mode. Once iLO locks these registers, the host server cannot regain control through the PCI bus.
- Secure registers, which secure sensitive information such as the configuration data and user passwords. No host application on the PCI bus can write to these registers, regardless of the state of the host server.

The host server can only read the areas of iLO memory that iLO exposes to the server. Applications on the PCI bus can only access the memory that iLO permits, such as the general registers and the protected registers under certain conditions. Applications running on the PCI bus cannot change the configuration of any shared memory region.

NVRAM—non-volatile data storage

The host server and applications running on the system PCI bus can only read the exposed areas of NVRAM: the integrated management log and host configuration information. There is also no chance for an application on the PCI bus to change the iLO configuration by means of the exposed NVRAM.

Network and management ports

Because of the host firewall and bridge logic within iLO, there is no connection between the iLO management port and the host server Ethernet port (Figure 1). Even when using the shared network port (SNP), it is impossible for the iLO processor to bridge traffic between the two network interface controllers (NICs) so that data flows from the management NIC to the host server NIC. An iLO device

will not be able to route packets between its 10/100 Ethernet port and an Ethernet port (possibly embedded) on the host server.

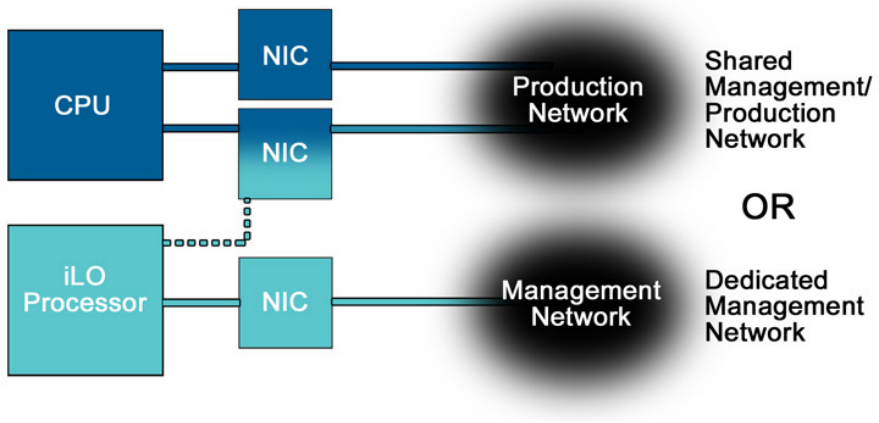
Therefore, if the host is compromised, iLO cannot be exploited as a means to compromise the management network. Conversely, in the unlikely event that the management port is compromised, there is no chance that the server network will be compromised as a result.

SNP for select ProLiant servers

Most G4 and later ProLiant ML and DL servers with iLO now support SNP, but there are exceptions. Users should consult the server documentation to determine whether a specific ProLiant server supports SNP. HP ProLiant servers supporting iLO are identified on this HP web page: www.hp.com/servers/ilo/supportedservers. At this time HP does not plan to support SNP on HP BladeSystem.

In HP server platforms that do support SNP, iLO management traffic uses the host NIC rather than the iLO management port. In this case, one of the server network ports shares its traffic with iLO management traffic (Figure 2). This capability is an advantage for customers who do not want to maintain a separate network for management traffic.

Figure 2. Shared network port is available for most ProLiant servers with the iLO processor.



Even though network traffic and iLO management traffic both flow through the same port, it is impossible for management data to flow to the host data stream. To ensure that all packets travel to the appropriate destination, the shared network port contains two separate Media Access Control (MAC) addresses inside the NIC – one for the iLO traffic and one for the host server traffic. The MAC layer is a sub-layer in the hardware data-link layer of the Open System Interconnection (OSI) model. It is responsible for moving data packets to and from one NIC to another across a shared channel. Because iLO maintains its own MAC address, it also maintains its own IP address. This ensures that other devices can address iLO independently of the host server, even though the network and management traffic share a port.

Shared network port with Virtual LAN

Security for the iLO SNP is enhanced by implementing the Virtual LAN (VLAN) feature. This feature is available with the release of iLO v1.80 and iLO 2 v1.10 and later.

A VLAN is a logical network that isolates network traffic to segments. It increases security because rules are established that restrict traffic on one segment from entering another segment. The Institute of Electrical and Electronic Engineers (IEEE) 802.1Q specification stipulates the use of VLAN tags. A

VLAN tag is a 32-bit number inserted into each 802.1Q Ethernet frame. The VLAN ID is a 12-bit number within the VLAN tag that identifies the Ethernet frame as belonging to a particular VLAN. Each port in an 802.1Q-compliant switch[3] can be configured to belong to the same VLAN or to a different VLAN. The switch examines the tag field in an incoming 802.1Q Ethernet frame and forwards the Ethernet packet to the ports that have the same VLAN ID.

The SNP NIC checks the Ethernet frame for a VLAN ID and compares it against its configured value. If they match, then the frame is stripped of the VLAN tag and forwarded to iLO. If they do not match, the frame is forwarded to the host. For outgoing packets, the SNP NIC inserts a VLAN tag into the Ethernet frame.

For customers who have been reluctant to use the iLO SNP feature because they wanted to separate regular Ethernet network traffic from management Ethernet network traffic, VLAN capability can now act as an Ethernet frame filter.

Security techniques used by iLO

The fundamental issue for enabling a secure system is whether a specific person, computer, or device knows that another person, computer, or device can be trusted: Has the end user or client node been authenticated against some indisputable standard to prove authenticity? If the end user is authenticated, at what level is that user authorized to make changes or access a requested environment? Finally, is it possible for data being sent through iLO to remain confidential?

The following sections identify the three essential techniques that iLO has or an iLO administrator can use to verify trust:

- Authentication and authorization
- Encryption
- Disabling ports and changing port locations

Every function of iLO – such as the remote console, virtual serial port, virtual power capability, and virtual media – builds on one or more of these techniques.

Authentication and authorization processes for browser access

System administrators can access the key functionality of iLO either through a web browser HTTP interface or through the iLO command-line interface (CLI) or Command Line Protocol (CLP). When users access iLO through the browser, the iLO management processor authenticates them differently, depending on whether they log in through a local account or use directory services. In either case, every time a user makes a request, iLO re-evaluates the user's privileges to ensure that the privileges are still valid. Although these access methods use JavaScript or ActiveX control, both are signed and no additional login process is required.

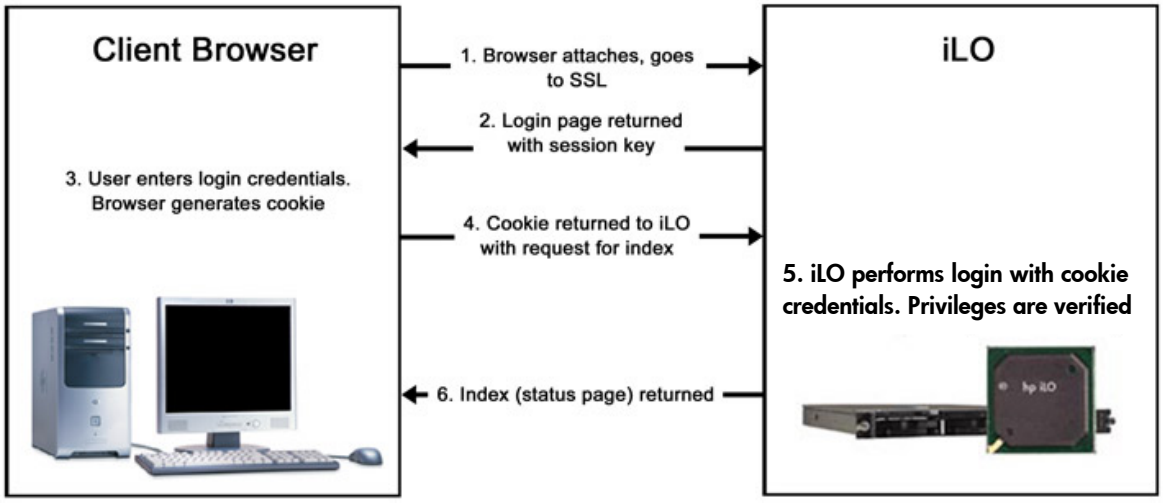
Using iLO firmware 1.80 and iLO2 v1.10 or later, a system administrator can use two-factor authentication to augment the security provided by iLO. This form of authentication is provided on top of either local accounts or directory services. This section describes each of the progressively more secure login models.

[3] The network switch must also support VLAN

Login process using a local account

Figure 3 shows the iLO login process using a local account.

Figure 3. User login process when using a local account



The first step in the login/authentication process is for the web browser on the management console to connect with the web server in the iLO device. iLO provides incorporates a progressive login delay. After an initial failed login attempt, iLO imposes a delay of five seconds. After a second failed attempt, iLO imposes a delay of 10 seconds. After the third failed attempt, and any subsequent attempts, iLO imposes a delay of 60 seconds. All subsequent failed login attempts cycles through these values. An information page is displayed during each delay. This will continue until a valid login is completed. This feature assists in defending against possible dictionary attacks against the browser login port. iLO saves a detailed log entry for failed login attempts, which imposes a delay of 60 seconds.

The iLO management processor uses 128-bit SSL encryption and the accompanying digital certificates to encrypt web pages (HTTP data) transmitted across the network. SSL encryption ensures that all information and commands issued through the web pages are private. An integral part of SSL is a digital certificate (see "Appendix A: Digital certificates"). The iLO management processor creates its own self-signed certificate by default. Administrators can also import a certificate from a third-party Certificate Authority (CA) or from the customer's own internal CA or PKI rather than the self-signed iLO certificate.

NOTE:
This step, SSL encryption, is performed both when logging in using directory services and when logging in using a local account.

Customers can use the digital certificate capabilities within iLO to prevent malicious attacks (such as Trojan horse attacks) in which an impostor appears to be a trusted iLO web server. For example, if someone were to put a server that emulated iLO onto a corporate network, that server would not have a legitimate iLO certificate. Therefore, if any user browsed to this emulated iLO device, the browser would, at a minimum, flag the lack of a recognized certificate. An administrator can configure the browser to reject a connection to any unrecognized certificates.

Once an SSL connection is established, login authentication commences. The iLO device returns a login page to the user that includes a unique session ID and a random session key. The unique session ID points to a session control block, an area of memory where all the session information is stored for that user and that session. Without the session control block, every user request would result in the need to re-authenticate all of the user credentials.

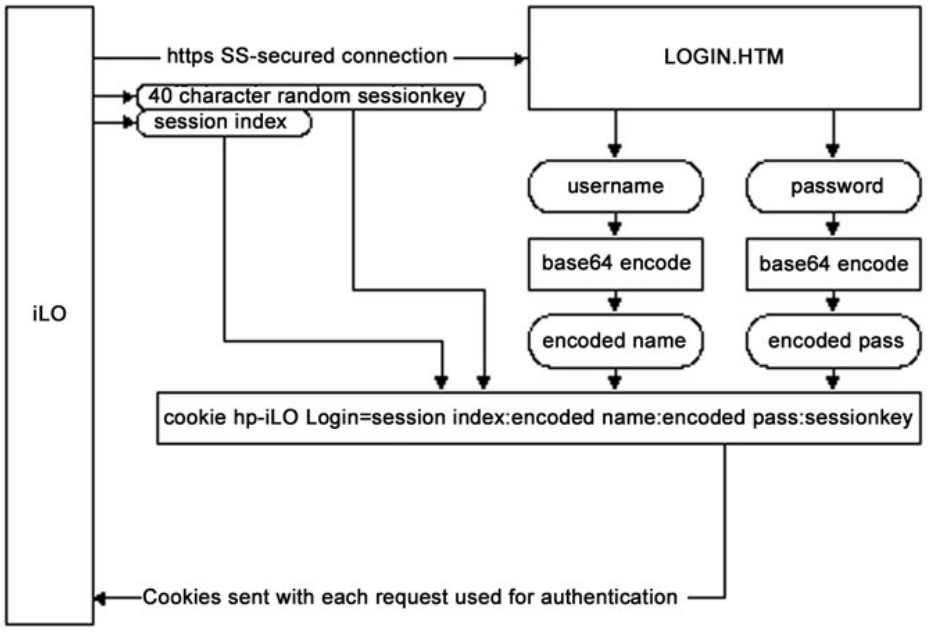
The session ID is time-stamped and valid only for the length of time defined by the SESSION_TIMEOUT parameter. Administrators can set the SESSION_TIMEOUT parameter to 15, 30, 60, or 120 minutes. iLO 2 releases after v1.30 support an Infinite Inactivity Timeout request. This request extends sessions indefinitely.

The combination of the session ID with the session key prevents a session from being hijacked by another authenticated connection.

At the client browser, the user enters his login credentials, and the browser generates a unique cookie,[4] called hp-iLO-Login. The web server within iLO uses this cookie for authentication and authorization (Figure 4). The browser encodes both the username and the password using a base-64 hash function and incorporates it into the cookie. The cookie also includes the unique session ID and the random session key sent with the login page.

The cookie links the browser window to the appropriate session in the firmware. The firmware tracks browser logins as separate sessions listed in the Active Sessions section of the iLO Status page.

Figure 4. How the browser generates the login cookie used for authentication



example cookie:

HTTP header line: Cookie hp-iLO-Login=00000007:QWRtaW5pc3RyYXRvcg=:Y29toGFx:
EUOHEFQUMYVZVYLQFDBSHJQJZUVVYTGQMOSZQGA

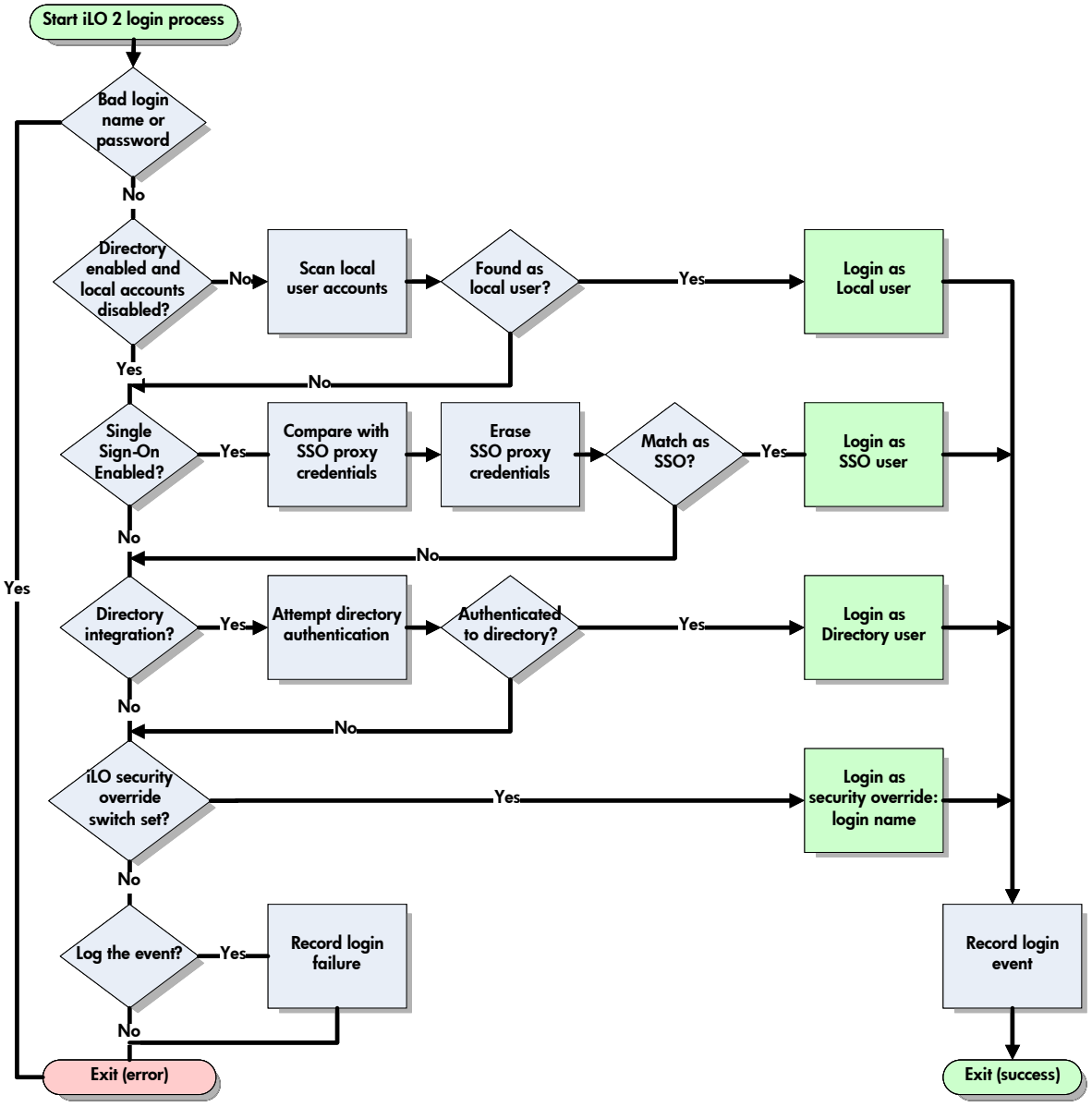
The cookie is stored in the memory of the client machine while the browser session is open. Any open browser session may preserve a cookie, including a "spawned" browser session such as the remote console window. The client browser never writes the cookie to its disk drive, and only the client

[4] The iLO cookie has been available in iLO firmware releases beginning with version 1.40.

session that generated the cookie can access it. When the user closes the browser or logs out of iLO, the browser destroys the cookie. Therefore, users should close all browser instances to guarantee the cookie is destroyed.

After the browser creates the cookie, it returns it to iLO with a request for a status page. The iLO device then begins the process of looking up the assigned user privileges. The iLO processor uses a generic login interface (application program interface, or API) to centralize the login functionality and abstract the local and directory user accounts. The common login API authenticates first against the directory, and then against local user accounts. Figure 5 shows the common login API that iLO performs using the authenticated credentials in the cookie.

Figure 5. Common login API flowchart



After authenticating the user, iLO calculates the current privileges, as described in the section titled "Calculating current privileges." Then iLO sends the iLO Status Summary page to the client browser

(Figure 6). The iLO Status Summary screen provides general information about iLO, such as all logged in users, server name and status, iLO IP address and name, and latest log entry data. At that point, the login process is complete. The iLO processor has fully authenticated the user who can then perform authorized functions.

Figure 6. Example of iLO Status Summary page

Login process using directory services with HP schema extensions

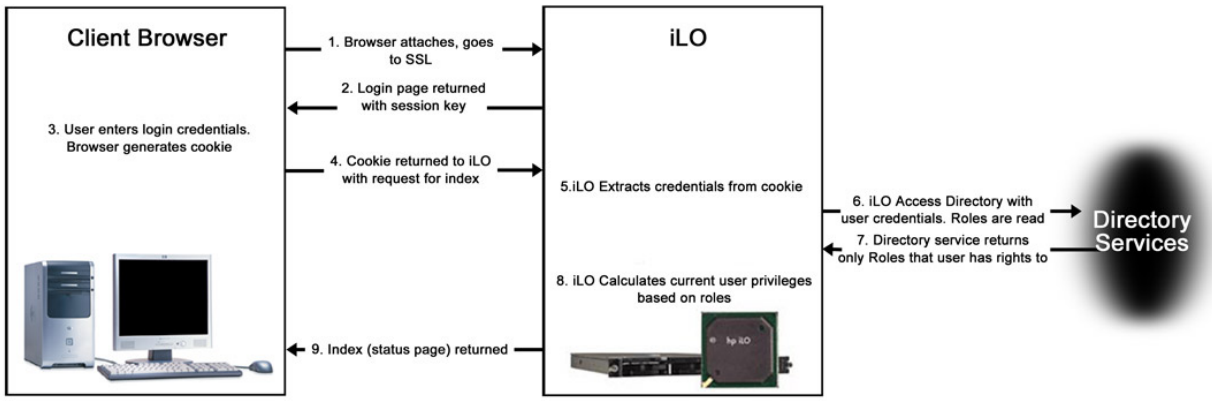
Administrators can choose to enable directory services to authenticate users and authorize user privileges for groups of iLO management processors. The iLO directory services feature uses the industry-standard Lightweight Directory Access Protocol (LDAP). Information about LDAP is provided in "Appendix C: LDAP/LDAPS definitions" of this document. HP layers LDAP on top of SSL to transmit the directory services information securely to the directory servers. More information about directory services is available from the HP website at: http://h18004.www1.hp.com/products/servers/management/directorysupp/index.html.

Using directory services, the login process includes the steps illustrated in Figure 7. After the web browser sends the cookie to iLO, the iLO processor extracts the user credentials from the cookie and accesses the directory service to determine which roles are available. First, iLO uses the credentials to access the iLO device object in the directory. The directory service returns only the roles for which the user has rights. If the user credentials allow read access to the iLO device object and the role object,[5] iLO determines the distinguished name[6] (DN) of the role object and the associated user privileges. Then, iLO calculates the current user privileges based on those roles and returns the iLO Status Summary page to the client browser.

[5] This happens when the user is a member of the role object or if the user is granted read access to the iLO and role objects.

[6] The distinguished name is the name that LDAP uses to access devices or objects in the directory.

Figure 7. Login process when using directory services



Login process using directory services with HP default schema

Using the HP Default Schema method (sometimes referred to as Schema-free method), access to iLO can be controlled using directories without requiring schema extensions. iLO acquires the user's name to determine group membership from the directory. iLO then cross-references the group names with its locally stored names to determine user privilege level. iLO must be configured with the appropriate group names and their associated privileges.

For HP default Schema login, the user's full distinguished name is required to look up his or her group memberships. iLO cannot efficiently convert a username into the user's distinguished name (DN). To do this, an IADsNameTranslate object is created and its Get method is used to retry the user's DN. If ActiveX is enabled, the login script will call IADsNameTranslate to write the DN to a cookie. The purpose of the login script is to get the user's login credentials (user name and password), get session information from iLO, and combine these into a security cookie. iLO then uses this cookie to ensure that the user has access to the pages and resources he or she is trying to use.

If ActiveX is disabled in the browser or the call fails and the name used for login is a DN, then the login script will work. The login script will also work if this name is only a user object name; then it is combined with a user context to build a DN. Essentially, if the IADsNameTranslate command is unavailable, then schema-free login reverts to the operational characteristics of the login process with HP Schema. See http://msdn2.microsoft.com/en-us/library/Aa706046.aspx for more information and examples.

The username and password information in the cookie is sufficient for authentication and authorization using the local account database or the directory using HP schema.

NOTE:
Using IADsNameTranslate allows the user to login using NetBIOS format (that is, domain/login name) or email format. Some IT organizations may prefer to disable ActiveX for security reasons. See the earlier section about local accounts for details about using SSL, session keys, and cookies.

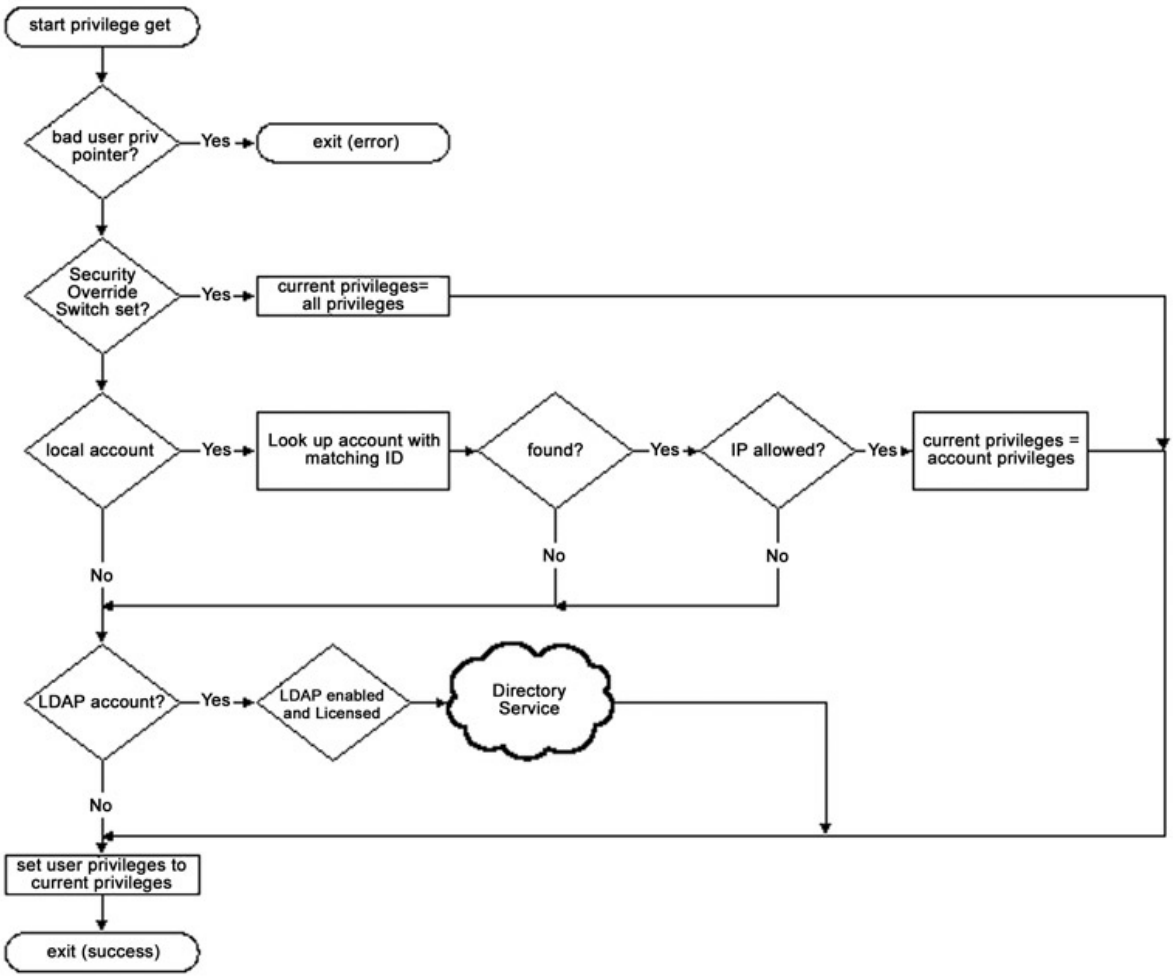
Calculating current privileges

A user's privileges can change at any time, even while the user is logged in. For example:

- An administrator could change a user's rights while that user is logged into the iLO device and the browser session is open.
- A user might be authenticated with directory services but authorized to access the system only between 8 a.m. and 5 p.m.
- XML scripts could alter privileges, administrators could delete a user account, directory settings could change, and time or address-based restrictions could apply.

Therefore, every time a user makes a request, iLO re-evaluates the user's privileges (see the flowchart in Figure 8). If the evaluation is successful, the user's request proceeds. If the evaluation is unsuccessful, the user's request is blocked or the user is logged out.

Figure 8. Flowchart for calculating current privileges



NOTE:
This section describing user privileges applies to local accounts as well as directory accounts.

Login process using two-factor authentication

With the version 1.80 firmware release, iLO provides a more robust authentication scheme supporting Microsoft Internet Explorer only. This authentication scheme involves using two factors of authentication. The user is authenticated by providing both of these factors:

1. Something the user knows, a password or PIN
2. Something the user possesses, the private key for their digital certificate

Users have the ability to store their digital certificates and private keys wherever they choose. It is likely, however, that smart cards and USB keys will be widely accepted due to their portability and secure methods of protecting private keys.

When two-factor authentication is required, access to the OS on a remote server will use smart card device support within Windows Remote Desktop Connection (RDP). iLO provides access to RDP with the Terminal Services pass-thru function.

NOTE:
Support for smart cards in RDP requires that the remote server be running Microsoft Windows Server 2003 or later.

The authentication layer will continue to be a middle layer between HTTP and LDAP or local accounts. It will be extended to provide certificate validation for local users, and it will perform the necessary LDAP calls to authenticate with the directory.

When two-factor authentication is enabled for web browser access, access to the following ports is automatically disabled:

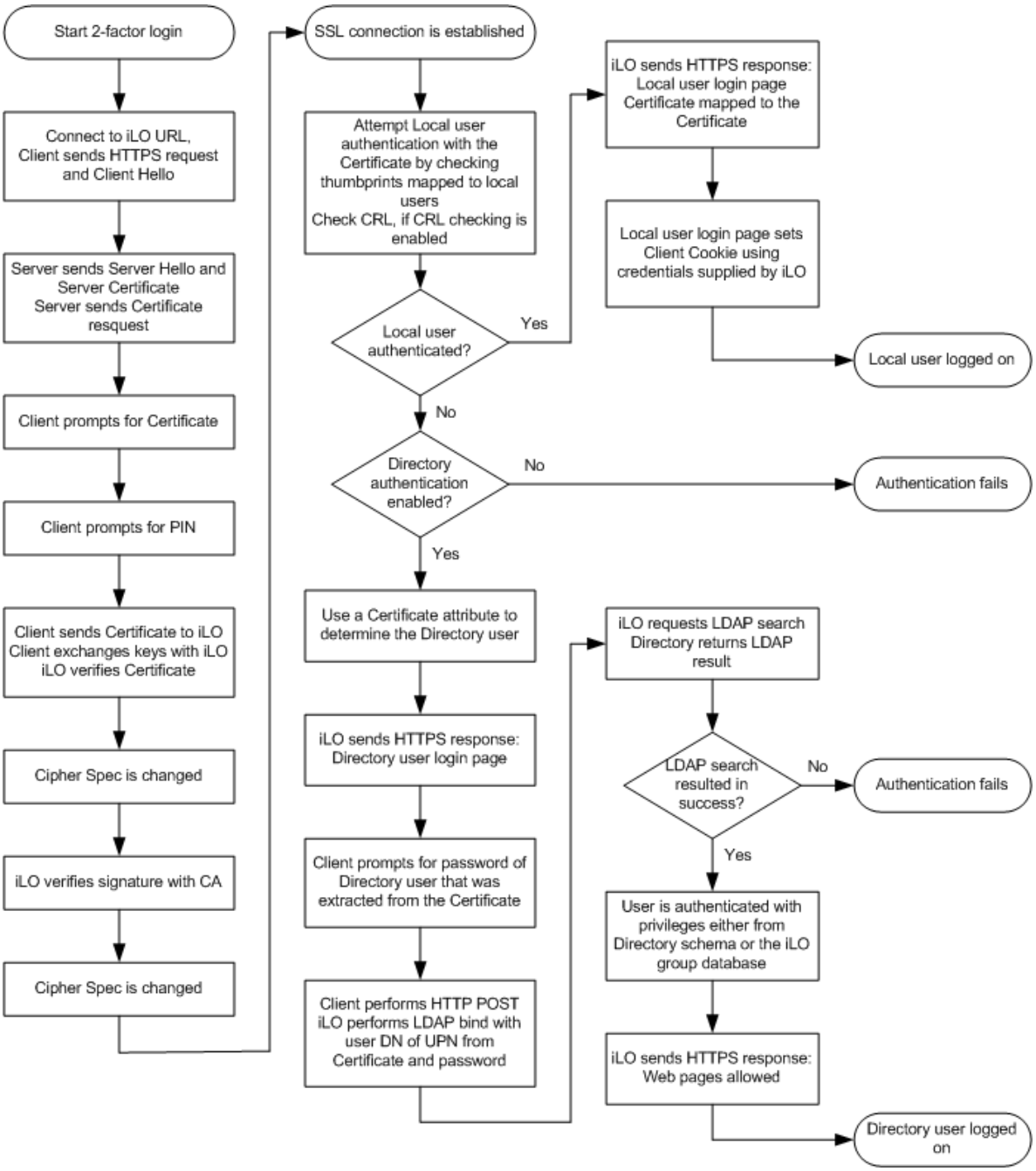
- SSH
- Port 22
- Telnet, Port 23
- SSL, Port 443 (XML traffic only; all other traffic remains unaffected)

If the user wishes, the SSH and/or Telnet ports can be selectively re-enabled through manual intervention. It is important to know that the XML port (CPQLOCFG access) cannot be enabled while two-factor authentication is enabled. Performing group administration activities while two-factor authentication is enabled requires use of the HPONCFG utility.

Figure 9 shows the messages that are exchanged to establish secure communication channels and authentication between the client and iLO, and between iLO and the directory in two-factor mode.

NOTE:
The Microsoft Internet Explorer browser uses the Microsoft Cryptographic API to enable communication between the browser and the certificate contained in the smart card.

Figure 9. Two-Factor authentication dialogue between the client and iLO, and between iLO and the directory server



Login process for remote console and virtual serial port

The iLO remote console server monitors the remote console port for connections from the remote console and virtual serial port applets and possibly Telnet. Figure 10 shows the steps in establishing a remote console session:

1. The user launches the Java applet by clicking on a link in the client browser.
2. The link opens a separate browser window.

3. The iLO device securely sends a one-time login token to the second browser window. The token contains base-64 encoded hash values of a random secret key and a random session key. This token is sent securely over SSL so a LAN sniffer cannot capture it.
4. The Java applet in the second browser window decodes (using base-64) the information within the token.
5. The Java applet passes the decoded information back to the remote console applet as the username and password.
6. The remote console applet compares the original login token with the decoded username and password from the Java applet, and allows a login if the data match.

This process is identical for the Integrated Remote Console ActiveX control.

Figure 10. Initiating a remote console session

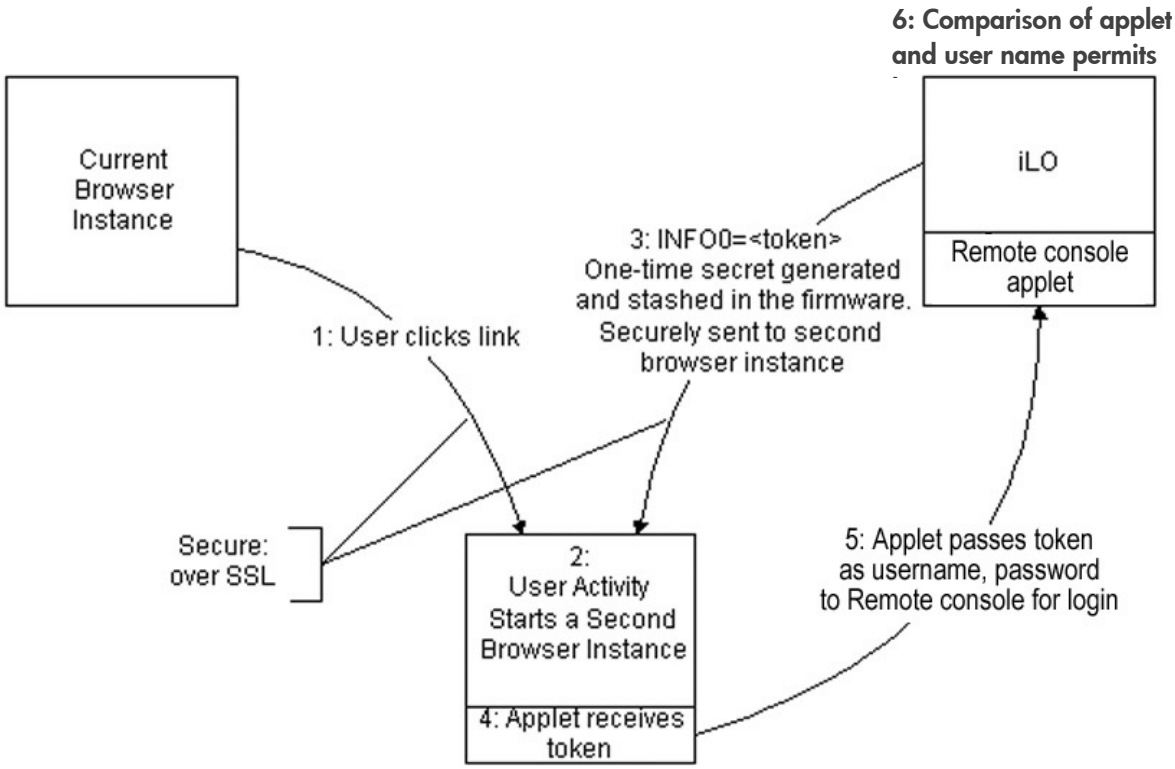


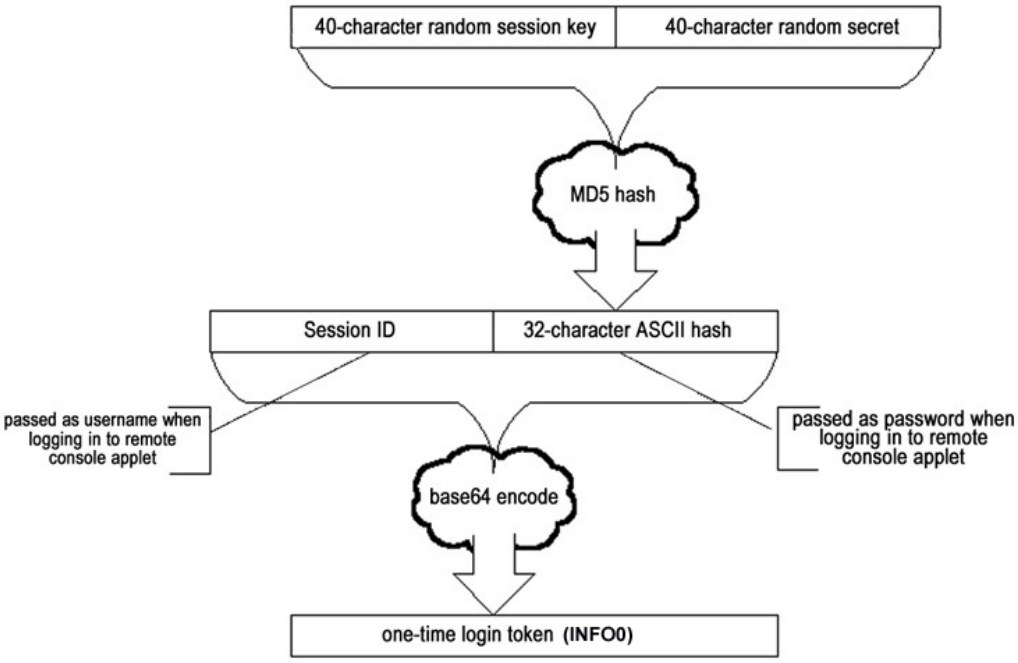
Figure 11 shows schematically how iLO constructs the one-time login token:

1. The original browser session contains a 40-character random session key. Programming code stored in the remote console applet generates a 40-character random secret. The random session key is concatenated with the random secret.
2. The iLO device performs an MD5 hash[7] on the concatenated line, and then converts the MD5 hash to ASCII. This step guarantees that the session key remains obscured. This prevents a user from hijacking another session accidentally or deliberately by using his valid session key to reattach to a different user's session.
3. The session ID is concatenated with the 32-character ASCII hash to obtain a second new line.

[7] An MD5 hash is a one-way encryption method that takes a message and converts it into32 digit hexademical number, also called a message digest.

4. The result is base-64 encoded and sent to the applet.

Figure 11. Process iLO uses to create the one-time login token for Java applet login



The result is that the applet passes the web server session ID as username and the ASCII hash as password to iLO. If iLO detects a match with the original 40-character random secret, which has been stored in firmware, iLO allows the login, and the connection credentials are matched with those stored in the session. The process of comparing the password with the stored secret destroys the secret. Successive attempts to connect using that 40-character secret will fail.

In addition to supporting the one-time secret login, the remote console applet also supports traditional username and password login. For example, if the remote console port configuration is enabled, and the remote console data encryption is set to <no>, then Telnet can employ the username and password credentials to connect iLO to the remote console port.

The new connection that the Java applet will use stays open as long as the server receives a "heartbeat" once every 30 seconds. If the server does not receive a heartbeat within one minute, the connection will be closed.

The iLO v1.91 and iLO 2 v1.30 and later releases include the Remote Console Computer Lock feature. With Remote Console Computer Lock, the operating system console self-locks when the session is closed or is timed out. Even though the session is closed, the connection remains active and authenticated to the OS. Without The Remote Console Computer Lock, another iLO user could access that open connection and start a new session. The console also self-locks if the network connection is broken during a remote session. This feature is supported in Microsoft® Windows® and Linux® operating systems. Configurable through programmable keys like the RC hot-keys, Remote Console Computer Lock allows iLO users remotely logged in to a server to maintain a connection.

Single Sign-On (SSO)

This feature, available with the release of iLO v1.91 and iLO 2 v1.30, is called Systems Insight Manager (SIM) Single Sign-On (SSO). SIM SSO allows a SIM user to access iLO directly from Systems Insight Manager without requiring an extra iLO login step. iLO rights are governed by the

user's HP SIM role. iLO 2 will trust SIM and, implicitly, users authenticated by SIM. The SIM SSO implementation uses a trusted certificate model for iLO to allow authentication to users from within the SIM framework.

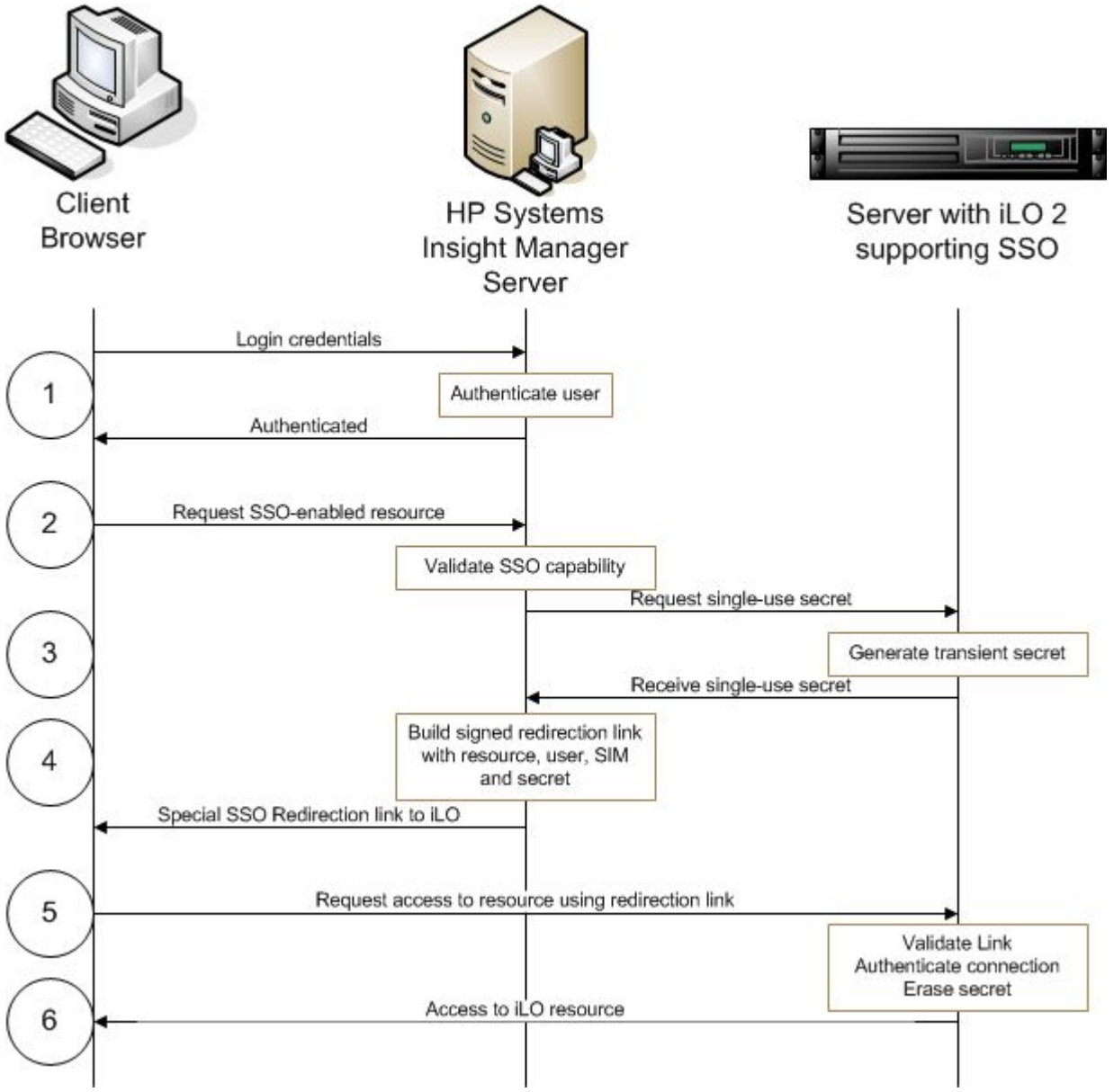
Use of this feature was introduced with the release of iLO v1.91 or iLO 2 v1.30, and HP SIM 5.1 with SIM 5.1 Hotfix to add SIM SSO support. For blade servers, adding the BladeSystem Integrated Manager 2.4 or later exposes SSO capability for iLO processors in blades.

The SIM SSO provides the following capabilities:

- Importing one or more SIM certificates
- Automatic certificate importation to ease initial setup
- Manual SSO certificate importation
- Support for certificate revocation
- SIM role to user privilege mapping
- Redirect to the SIM console for SSO
- Modification of the iLO login process to support automatic login from supported SIM SSO redirections

Figure 12 illustrates the authentication process from within the SIM framework.

Figure 12. HP SIM Single Sign-On to iLO process



The numbered steps shown in Figure 12 describe the authentication process:

1. The user logs-in to HP Systems Insight Manager Central Management Server.
2. The user follows a link in HP SIM. This link initiates the SSO connection.
3. iLO generates a timed, one-time secret to prevent replay attacks.
4. HP SIM builds a signed link incorporating the resource, secret, user, and HP SIM.
5. Client browser redirects to the link at the Integrated Lights-Out processor.
6. iLO validates the request based on the request contents, iLO configuration, secret, and HP SIM source. Authenticated requests receive the resource.

SIM SSO does not affect the local iLO user. SSO trust is iLO-based and can be determined by server name, by certificate, or by both. HP recommends using certificates. Certificates must be imported to

iLO, but there is limited space to store certificates. When full, no additional records may be added unless other records are first removed. Record removal occurs when the buffer rolls over and any earlier certificate information is lost.

Authentication and authorization processes for CLI access

The iLO command-line interface gives customers another way (in addition to the web browser) to access critical iLO functions such as the virtual power capability, text-based remote console, and virtual serial port. The iLO CLI uses the industry-standard Secure Shell (SSH) protocol to encrypt the data stream and all keystrokes sent between iLO and the client.

When a user requests an SSH session, the iLO processor performs the following negotiation steps to ensure a secure login:

1. The iLO processor retrieves the encryption keys from NVRAM. If the keys are not present or are invalid, the iLO processor generates the keys.

NOTE:
The keys are preloaded at the HP factory. However, in the case of a field upgrade, there could be up to a 25 minute delay after upgrading the firmware before the keys are created. If users try to login through SSH immediately after upgrading, they could experience a wait of up to 25 minutes. During this time, iLO response to other functionality is slow and the iLO status page displays a message indicating that key generation is in progress.

2. The iLO processor listens for a request on the SSH port. When it gets a request, it starts a protocol negotiation task for exchanging the public and private keys during the SSH protocol negotiation.
3. The protocol negotiation task completes the key exchange.
4. The protocol negotiation task then spawns a task for checking authentication timeout and another task for performing the authentication. The authentication task is also used for reading from the SSH port once authentication completes successfully.
5. The task for protocol negotiation then terminates while the authentication task and authentication timeout task continue to run.
6. The authentication timeout task waits for one minute. If authentication does not complete successfully during that time, this task will terminate the connection.
7. The authentication task will attempt to authenticate the user. The iLO device allows a maximum of three attempts. If authentication is unsuccessful, iLO terminates the connection. If authentication is successful, this task will start the CLI session task for the SSH session and the SSH task for writing to the SSH socket. After initiating the CLI and SSH tasks, the authentication task becomes the read task for the SSH socket.
8. The write task for the SSH connection will write data to the socket. If there is no session activity for a period equal to the session timeout, the SSH session will close.

The iLO management processor supports only version 2 (SSH-2) of the protocol. “Appendix B: SSH-2 support” lists the SSH features supported.

Encryption

The iLO management processor uses 128-bit SSL and SSH frameworks to ensure privacy of iLO actions depending on the access modes and types of functions being performed. Within these frameworks, various ciphers can be used for encrypting network traffic.

The purpose of a cipher is to make data private, so that only parties to the cipher and keys can read the data. The frameworks enable cipher negotiation as well as the secure exchange of keys used to initiate encrypted communication within the cipher algorithm.

iLO supports RC4, 3DES and AES ciphers. Key exchange uses RSA/Diffie-Hellman, and keys are rotated every 3 minutes. Certificates are generated using 1024-bit RSA keys signed with MD5RSA and using a SHA1 fingerprint.

Secure Sockets Layer (SSL)

The iLO management processor encrypts all web pages using 128-bit SSL encryption. This ensures that all information and commands issued through the web browser are private. See the section titled "Authentication and authorization processes for browser access" for more information.

SSL allows a list of ciphers to be compared between the client (browser) and server (iLO). Generally, they negotiate to use the strongest common cipher. A client may include a long and permissive list of ciphers, but it is often desirable to restrict the list of ciphers. iLO 2 v1.30 has this capability.

AES encryption

iLO 2 v1.30 can restrict ciphers to AES/3DES using browser settings (through the Global Settings page), XML scripting, or SM CLP.

The following is a complete list of communication channels that can employ AES encryption:

- Web browser (UI) – The current Mozilla browser, Firefox 2, supports AES Encryption. Internet Explorer 7 is the first Microsoft product to do so.
- LOCFG/XML – A command line switch will be implemented that allows the user to select AES encryption and the cipher strength
- SSH – Both OpenSSH in Linux and PuTTY are capable of initiating AES sessions.
- LDAP– This is an outbound method of communication where iLO provides client-side communication, and the LDAP server provides server-side communication.

Popular AES cipher strengths are supported through the web browser, XML and SSH.

Remote console and virtual serial port data encryption

The iLO processor uses the RC4 streaming cipher algorithm, a variable key-size stream cipher with byte-oriented operations, to encrypt the remote console and virtual serial port sessions. Unlike a block cipher, which encrypts several bytes of data at a time, a streaming cipher encrypts individual bytes of data, using a different key for each. For more information on RC4, visit the website at www.rsasecurity.com.

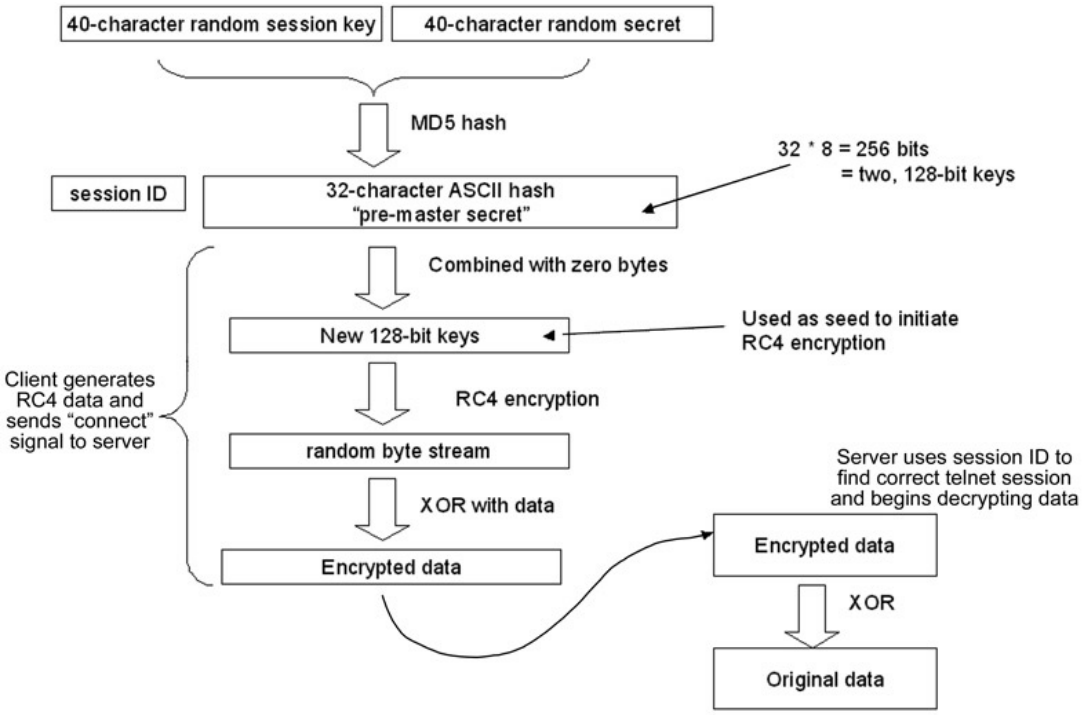
When a user requests either a remote console or a virtual serial port web page, iLO responds by using the MD5 hash algorithm to create a pair of random 128-bit keys (the "pre-master secrets") and a time-stamped session ID, as shown in Figure 13. These are the same session ID and MD5 hash values discussed in the section titled "Login process for remote console and virtual serial port." One key is used for encrypting data from the client to the server; the other is used to encrypt data from the server to the client. The time-stamped session ID is part of an array entry that identifies the Telnet session. This ensures that when the client browser attempts to start an encrypted data session, it can identify itself with this session ID. The browser passes the128-bit keys and the session ID to the client by means of JavaScript files included in the browser. This ensures that the security keys and IDs are sent encrypted.

Next, the client generates the RC4 encryption data by combining the pre-master secrets with a set of zero bytes to generate the new 128-bit keys that will be used to initiate the RC4 encryption cipher. The new keys are stored with the pre-master secrets in the dynamic memory space of the client machine. They are not written to disk. The RC4 cipher algorithm generates a random stream of bytes.

This random stream of bytes is combined in a Boolean XOR operation with the data being sent to create the encrypted data.

The client then sends a "connect" message to the server. Part of the "connect" message is a "start encryption now" signal and the session ID, after which all bytes are sent encrypted. The server uses the session ID to find the correct Telnet session and then begins decrypting the data using the RC4 cipher. Another Boolean XOR operation is performed on the encrypted data to recover the original data.

Figure 13. Remote console and virtual serial port encryption process



Every three minutes, the server will combine the pre-master secrets with the generated 128-bit keys to generate new 128-bit keys. These new keys are used to create a new set of RC4 data. The server sends a signal to the client indicating that it has generated the new RC4 data and will begin communicating using the new cipher. The client will perform the same operation when it sees the signal. It then sends a signal to the server indicating that it is using the new RC4 data. The signal is implemented with a byte-insertion protocol.

Secure Shell encryption

As previously discussed, the CLI uses SSH to encrypt the data stream both to and from the host server. The iLO processor encrypts the SSH data using either the 3DES-CBC or AES128-CBC protocols (refer to "Appendix B: SSH-2 support"). The SSH client negotiates with iLO to use one of those two protocols.

Disabling and changing ports

Administrators can use the flexibility of the iLO design to change the port numbers of services or to disable services and utilities that are not necessary.

Administrators can manually configure the port numbers of the HTTP port for the Web and XML server, the Telnet port, remote console port, Terminal Services Pass-Through port, virtual media port, and the SSH port. The only port numbers that cannot be reconfigured are the SNMP ports. For example, when given an IP address, a web browser normally attempts to connect with port 80. However, an administrator can redirect the HTTP ports to administrator-defined ports. Once the HTTP port is re-directed, a user must specify that port and the IP address to access the iLO login screen. This reduces the chance that others can access the port without specific knowledge of the port number.

Administrators can also selectively disable the services they do not need in their environments. Table 1 gives the complete list of default port locations and indicates whether the port is enabled or disabled.

When two-factor authentication is enabled for web browser access, access to the following ports is automatically disabled:

- SSH, Port 22
- Telnet, Port 23
- XML, Port 443

If desired, the user can selectively re-enable the SSH and/or Telnet ports.

Table 1. Default port locations for iLO

Port Number	Protocol	Can Port Number be Changed?	Supports	Enabled by default
22	SSH	Yes	SSH Connections	Yes
23	Telnet	Yes	• Remote graphical console • Remote text console • Virtual serial port	Yes
80	Remote Insight browser port	Yes	HTTP interface to iLO management board	Yes
161	SNMP get/set	No	HP SIM polls	No
162	SNMP trap	No	HP SIM agent events	No
443	Remote Insight browser access encrypted port	Yes	• SSL access to iLO management board • Encrypted XML access	Yes
636	Lightweight Directory Assisted Protocol (LDAP)	Yes	Secure connection to the directory server	Yes, if directory support is enabled
3389	Terminal Services Pass-Through (RDP)	Yes	Terminal Services session-software-based remote console using Microsoft Windows (RDC/TS)	Yes
9300	Telnet	Yes	Multi-user remote console	No
17988	Virtual Media	Yes	Virtual Media	Yes
17990	Telnet	Yes	Console replay	No

Connectivity among iLO, the host server, and the network

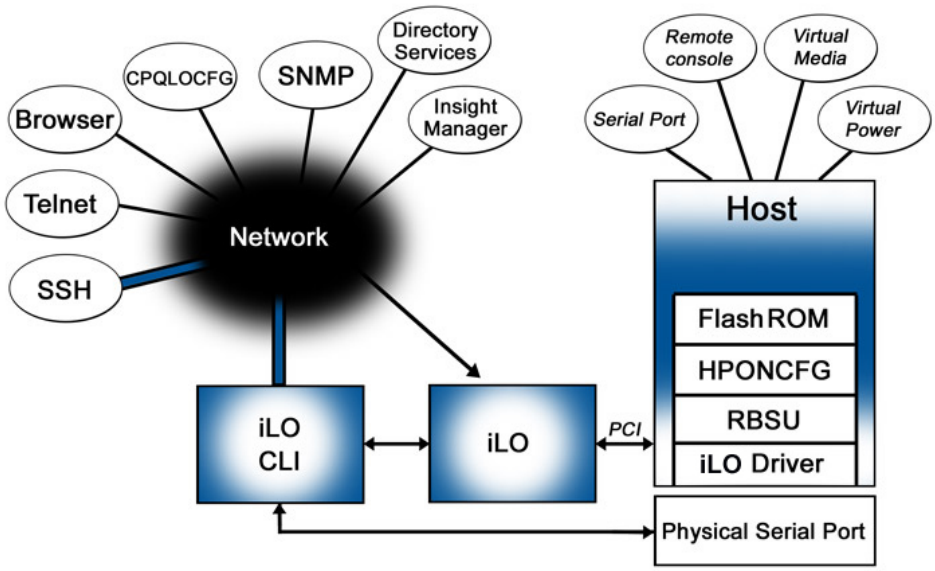
Thus far, this paper has explained the techniques that iLO uses to ensure secure communications. To better understand potential security risks in their environments, administrators may also want to be aware of the points of access to and from iLO, the host server, and the client. The following sections briefly describe how the iLO design or its configuration mitigates those risks.

Access to iLO by means of the network

As shown in Figure 14, several utilities have access to the iLO processor through the network: the web browser, Telnet connection, SSH connection, the CPQLOCFG utility,[8] directory services, the Lights-Out Migration Utility (for directory services), SNMP, and Systems Insight Manager or Insight Manager 7.

HP generally recommends that iLO management traffic reside on a separate management network and that only administrators be granted access to that network. This not only improves performance by reducing traffic load across the main network, it also acts as the first line of defense against security attacks. A separate network allows administrators to physically control which workstations are connected to the network.

Figure 14. The iLO processor relative to the network and host server



Web browser

The browser encrypts the data stream using 128-bit SSL to provide privacy and integrity. The iLO device accepts digital certificates, so users can import certificates from a guaranteed certificate authority to prevent someone from placing a Trojan horse server on the network. Administrators can change the default port location for the web browser. Finally, access to the iLO device is restricted through the web browser by the user access privileges and the strong authentication process.

[8] The CPQLOCFG utility allows users to configure iLO devices. It is a Windows-based utility that sends RIBCL (XML) script files to iLO using a secure connection over the network.

Telnet, remote console, and virtual serial port

Because Telnet is not an inherently secure protocol, administrators may be reluctant to use its functionality. The following section describes how iLO facilitates secure Telnet access. The remote console and virtual serial port functions use the standard Telnet port to connect to the iLO device.

Although Telnet itself is not encrypted, invoking the remote console applet enables its encryption feature. This forces iLO to connect using the remote console applet rather than a standard Telnet session for a text-based console session. iLO maintains exclusive control over the port when using the remote console applet.

Administrators can configure the Telnet port to allow only the remote console and virtual serial port functions— the "automatic" setting for port 23. This means that iLO disables the port except when it senses the remote console or virtual serial port applets starting. Because the iLO device refuses any other connection attempt to port 23, the host server will be inaccessible through a standard Telnet application.

There are two instances in which a standard Telnet application could connect to the server. The first instance occurs after the user clicks on the remote console or virtual serial port but before the applet connects to iLO. For this case, if the user has enabled encryption, iLO will close the connection as soon as it realizes the client has not sent valid information to begin the encrypted communication. The second case is if one of these clients terminates abnormally. In that case, iLO will not close the socket until it realizes it has not received a keep-alive signal during the specified interval (one minute).

The Telnet port number can be changed to any unused port number, or an administrator can disable the Telnet port entirely. When the remote console port is in the "Disabled" mode, no application (including the remote console or virtual serial port applet) can connect to port 23.

Finally, any potential security risk of the Telnet port across the network is reduced because the remote console and virtual serial port applets have strong authentication and authorization processes.

Multi-user Integrated Remote Console (IRC)

Beginning with the iLO v1.91 and iLO 2 v1.30 releases, IRC is available as an iLO Advanced and iLO Select feature. The IRC is a user-configurable setting and supports up to four simultaneous remote console sessions on the same server.

The first user to initiate a remote console session is designated as session host. The session host has the option to deny access, grant full access, or allow read only access. Participant sessions are terminated when the host session is terminated. All console sessions are encrypted. For added security, the Remote Console Computer Lock feature provides the ability to self-lock the operating system when the session is closed or timed out.

The IRC is supported on Windows and Linux. The client browser on the management console must use a Windows Internet Explorer browser because the IRC uses the ActiveX code, not Java.

SSH for the command-line interface

Administrators with access to the CLI have access to most of the iLO functionality; however, they access iLO in text mode rather than in graphical mode. To ensure the data and keystroke integrity, the SSH data stream is encrypted. Administrators can disable the SSH/CLI functionality, change the SSH port number, or restrict user privileges to ensure that only authorized personnel can access the CLI.

CPQLOCFG utility

The CPQLOCFG utility connects to the iLO processor across the network using the encrypted SSL port. Because the connection is over the network, users can only access the CPQLOCFG utility with valid user credentials and privileges authorized by the strong iLO authorization process. Administrators can change the HTTPS port number to reduce the likelihood of unauthorized persons accessing iLO.

Directory services

The iLO processor uses SSL-protected LDAP (LDAPS) to communicate with the directory server. For a more detailed discussion of LDAPS, refer to "Appendix C: LDAP/LDAPS definitions" in this document. Using directory services is generally considered to be more secure than using local iLO user accounts for the following reasons:

- Administrator accounts are not shared among multiple people (a common practice with local accounts).
- Password protection is enforced by the directory.
- Role-based access allows for detailed time and place access restrictions.
- Maintenance functions (such as changing rights for multiple users) are performed once at the directory rather than multiple times for each iLO device.

Administrators who use the Lights-Out migration utility to migrate from local accounts to directory accounts also access iLO through the network. The utility is built on top of the XML infrastructure of CPQLOCFG, so it has the same security advantages as CPQLOCFG: strong authentication, ability to change port numbers, and the use of encryption.

SNMP

The iLO device acts strictly as a pass-through service for SNMP functions. The SNMP port is one of only two ports in iLO that allow traffic to be passed to the host OS through the iLO driver. Because it does not encrypt data, there could be security concerns about the data that iLO passes from the host server, such as the OS, type of processor, number of I/O devices, and so on. If administrators want to continue to use the SNMP functions, they can set firewalls and routers to accept only specific source and destination addresses. For example, an administrator can allow inbound SNMP traffic into the host server only if it comes from a predetermined management workstation. Administrators can also set the passwords (community strings) according to the same guidelines as administrative passwords. Finally, administrators can disable SNMP entirely.

Systems Insight Manager

Systems Insight Manager checks for an iLO presence by starting an HTTP session. The default port setting for this session is Port 80. Administrators can change this port number. Tight integration between iLO and Systems Insight Manager means that information such as the server serial number, iLO status, iLO serial number, hardware revision, and firmware revision is available through the Insight Management software. By using the following settings, administrators can control whether information is returned for a Systems Insight Manager request:

- Enabled—associations are present and data is present on the summary page.
- Disabled—no data is returned to Systems Insight Manager.

Access to iLO by means of a physical connection

Someone physically present at the host server can access iLO in one of two ways:

- through the physical serial port on the host server
- by means of the iLO Security Override jumper

Host server serial port

Users with access to the host server serial port can access the iLO CLI and perform many iLO functions (such as reset power or text-based remote console) on the host server. A potential risk is that the connection from the host serial port to the CLI is not encrypted. However, because this is a point-to-point (and physical) connection, it is presumed that anyone with physical access is authorized to access iLO. There is no risk of someone intercepting the data with the point-to-point connection. Because the server serial port connects to the iLO CLI, administrators can disable the SSH/CLI

functionality or restrict user access by requiring authentication to the CLI. In addition, administrators can change the host server OS to disable any support for the host server serial port.

iLO Security Override jumper switch

As stated in the section titled "Security assumptions about iLO and its environment," people with physical access to a server can alter the host server and the iLO setup. Therefore, it is assumed that any individual with unrestricted access to the inside of a server enclosure is a super-user or administrator. Someone with access to the inside of a server can access the security override jumper, reconfigure iLO through RBSU, reprogram the iLO ROM, or reprogram the boot block. The location of the iLO Security Override jumper depends on the host platform, so system administrators must consult the host documentation for details.

Access to the server from iLO

Users can directly access the server through the iLO functions such as virtual serial port, remote console, virtual media, and Terminal Services (Figure 13). The question for administrators is whether a user has authorization to perform specific functions on the host server.

Any of these functions is secure from the host by means of the host OS. More importantly, iLO secures the environment through the strong user authentication and authorization processes that have already been discussed.

iLO software on host using the PCI bus

Several pieces of iLO software reside on the host server, thus providing an entry point into the server. The iLO driver enables the other iLO integration services, such as RBSU, Terminal Services pass-through, HPONCFG, and the agents.

RBSU

RBSU allows users to initially configure iLO and iLO user accounts. Every time the server boots, RBSU is available to anyone with access to the server console. Therefore, RBSU requires strong security. Administrators can configure RBSU to require valid user credentials for authorization, using the robust iLO login mechanisms. Those who do not want RBSU to be accessible at reboot can disable RBSU in the Global Settings preferences. Disabling RBSU prevents reconfiguration from the host unless the iLO Security Override Switch is set.

iLO firmware (FlashROM)

The firmware boot block protects the iLO main-line code by using a digital signature. A digital signature for the firmware image is generated using a private key known only to HP. The iLO boot block verifies the digital signature by using a corresponding public key. No one can modify the firmware contents without generating a new digital signature, which requires the original private key from HP. The boot block examines the digital signature of the iLO main-line code and refuses to transfer control to the main-line code if the signature is invalid. This prevents loading corrupt or rogue firmware.

HPONCFG

The HPONCFG utility is a host-based service that allows configuration of iLO using XML scripts. Because it is host-based, the iLO firmware ignores login credentials and assumes that the user has the rights to configure iLO. This potential security risk is reduced because HPONCFG requires a root login (in Linux operating systems) or administrator login (in Windows operating systems) to access the utility.

CPQLODOS

Administrators can use the CPQLODOS utility for initial deployment of the iLO processor. It is used only in a DOS environment, such as during SmartStart scripted deployment, and not over the network. Therefore, it requires a reboot to DOS. The administrator must have a DOS image loaded on a host or a floppy, which means that the user either has physical access or a virtual media privilege, with all the accompanying user rights and authentications.

Terminal services

The iLO processor uses a pass-through service (HPLOPTS.EXE) to access Windows Terminal Services. When the administrator requests a remote console connection, the iLO remote console applet activates the Terminal Services client application and sets up a socket, listening on port 3389. The iLO processor forwards all data that it receives from the Terminal Services client to the server. The iLO processor forwards back to the Terminal Services socket all data that it receives from the server. Because it is a pass-through service, when iLO is using the Terminal Services connection, it implements security identically to the Windows Terminal Services Remote Desktop Protocol (RDP) implementation. This means that any active security measures are established between the Microsoft terminal services client and Microsoft's RDP service.

The Terminal Services port is the second of two ports in iLO that allow traffic to be passed to the host OS through the iLO driver. Administrators can disable the Terminal Services Pass-Through port.

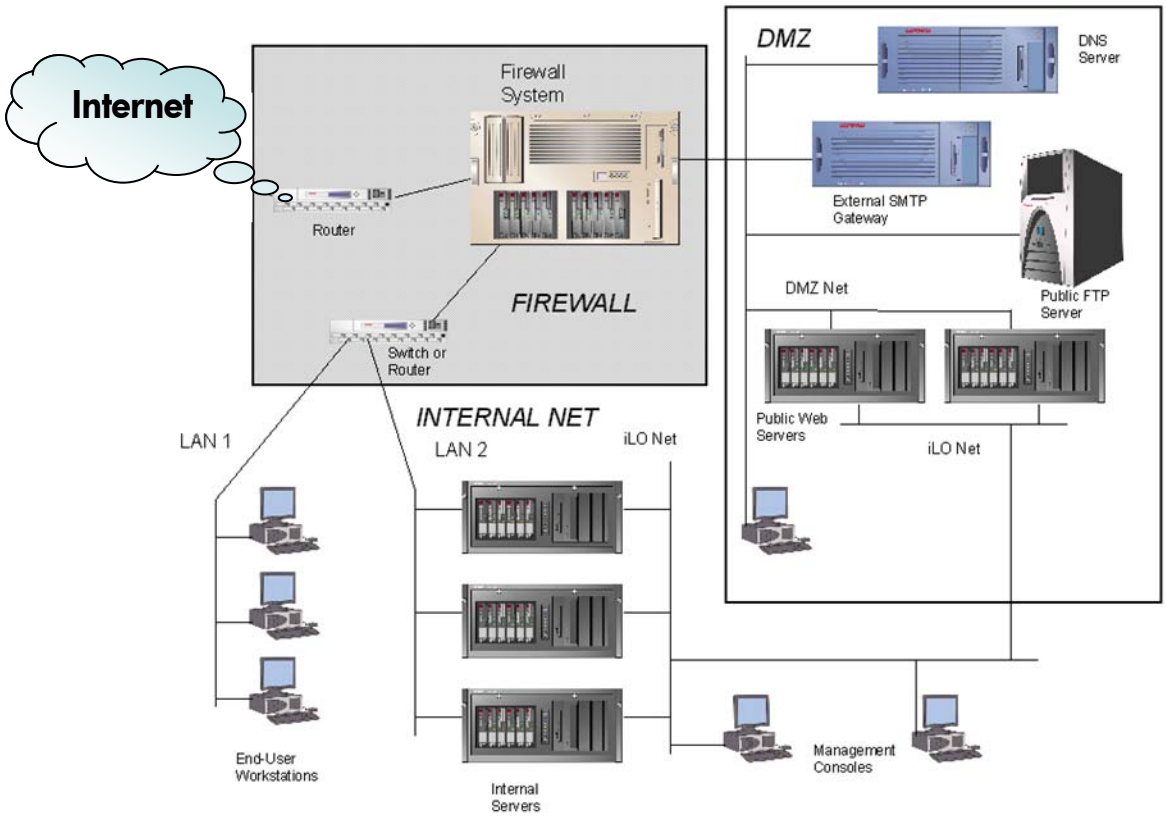
Specific IT infrastructure concerns

Customers have questioned security issues regarding two particular IT environments: when operating iLO in the infrastructure between an external firewall and an internal network (DMZ), and when operating iLO in a server blade environment.

Operating iLO servers in the DMZ

Within an Internet connected architecture, there is typically a more secure zone, commonly referred to as the de-militarized zone (DMZ). This zone is positioned between the corporate servers and the Internet, usually separated from both by firewalls that restrict traffic flow. With this architecture, servers that provide publicly available Internet services can be accessed through a firewall, but these services are inaccessible on the internal network. This more secure zone provides an area that is isolated from the internal network and is hardened against external attack (Figure 15). The security challenges in the DMZ require a careful balance between critical security requirements and the need to effectively manage and maintain the systems.

Figure 15. Example configuration of a DMZ



iLO provides the capability to create a separate, secondary network (iLO Net in Figure 14) that is parallel to the primary or production network. This dual network architecture has the benefit of completely segregating management traffic from production network traffic. It facilitates system-wide server management activities, including servers inside the DMZ, while maintaining maximum security by limiting access to the production network.

Figure 15 shows a packet-filtering router that acts as an initial line of defense. Behind this router is a firewall system. There is no direct connection from the Internet or the external router to the internal network. All traffic to or from the internal network must pass through the firewall system. An additional router, which filters packets destined for the public services in the DMZ, protects the internal network from public access.

The firewall is a multi-homed host, and it can be configured to evaluate traffic according to different rules based on the traffic source and destination:

- from the Internet to the DMZ
- from the DMZ to the Internet
- from the Internet to the internal network
- from the internal network to the Internet
- from the DMZ to the internal network
- from the internal network to the DMZ

Servers inside the DMZ and on the internal network can use iLO processors. Because the network connection to iLO is completely isolated from the network ports on the server, there is no possibility for data to flow from the DMZ network to the iLO network, or vice-versa. Therefore, even if the DMZ network is compromised, the iLO network will remain secure. This architecture permits administrators to use iLO on servers located in the DMZ or in the internal network without the risk of compromising sensitive data. This separation is accomplished by using a dedicated NIC or the Shared Network Port (SNP) with its VLAN (see the section "SNP for select ProLiant servers").

For best protection of the servers operating inside the DMZ, administrators should set the SNMP trap destinations to the loop back address and enable the SNMP pass-through in iLO so that SNMP traps are routed onto the iLO network. While this SNMP pass-through option does not enable all management functions, it allows for passing status, inventory, and fault information to HP Systems Insight Manager or another SNMP-capable management application. This option has the benefit of being very secure because the host operating system does not recognize the Lights-Out product as a NIC.

Lights-Out Management Integration with Rapid Deployment Pack

The Rapid Deployment Pack (RDP) Deployment Server Console provides secure access to the management features of iLO and Remote Insight Lights-Out Edition (RILOE).

IMPORTANT:
If Rapid Deployment Pack—Windows Edition and HP SIM will be installed on the same server, Rapid Deployment Pack—Windows Edition must be installed before HP SIM and the other products on the Management CD.

The Rapid Deployment Pack combines an off-the shelf version of Altiris eXpress Deployment Solution and the ProLiant Integration Module. The ProLiant Integration Module consists of software optimizations including the SmartStart Scripting Toolkit, Configuration Events for leading industry-standard operating systems, sample unattended files, and ProLiant Support Packs containing software drivers, management agents, and important documentation. Servers can be deployed through Altiris' imaging feature or through scripting using the SmartStart Scripting Toolkit. For more information on the ProLiant Essentials Rapid Deployment Pack, visit the website at www.hp.com/servers/rdp-we.

Communication between iLO and server blades

In the HP BladeSystem architecture, a single enclosure houses multiple servers. A separate power subsystem provides power to all server blades in that enclosure. ProLiant c-Class server blades (see the website at www.hp.com/servers/blades) use the iLO management processor to send alerts and management information throughout the server blade infrastructure. However, there is a strict communication hierarchy among ProLiant c-Class server components. The Onboard Administrator (OA) management module communicates with the iLO processor on each server blade. The OA module provides independent IP addresses for each server blade. The iLO firmware exclusively controls any communication from iLO to the OA module. There is no path from an iLO processor on one server blade to the iLO processor on another blade. The iLO processor has information only about the presence of other server blades in the infrastructure, and whether there is enough amperage available from the power subsystem to boot the iLO host server blade.

Within BladeSystem c-Class enclosures, the server blade iLO network connections are accessed through a single, physical port on the rear of the enclosure. This greatly simplifies and reduces cabling. Note that the iLO on a server blade maintains an independent IP address.

Security Audits

Recent legislation may mandate periodic security audits. iLO maintains an event log containing date- and time-stamped information pertaining to events that occurred in the iLO configuration and operation. This log can be accessed manually through the System Status tab of the iLO browser interface. An automated examination and parsing is available for extraction through XML commands. The log can be parsed by date/time and authenticated user for information relating to security events.

General security recommendations

For more complete information about iLO security, consult the *HP Integrated Lights-Out User Guide,* the *HP Integrated Lights-Out 2 User Guide*, and or the *Planning and configuration recommendations for Integrated Lights-Out processors*. These documents are available at these HP web sites respectively: http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00209014/c00209014.pdf, http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00553302/c00553302.pdf, http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00257375/c00257375.pdf respectively.

HP recommends that customers observe the following security practices, stated here in abbreviated form:

- **Use a separate management network.** For security and performance reasons, HP recommends that customers establish a private management network separate from their data network and that only administrators be given access to that management network.
- **Do not connect iLO directly to the Internet.** The iLO processor is designed as a management and administration tool, not as an Internet gateway. Typically, customers would connect to the Internet using a corporate VPN that provides firewall protection.
- **If using local accounts, change passwords frequently.** The default iLO password should be changed immediately to a more relevant password. Administrators should change the iLO management passwords with the same frequency and according to the same guidelines as the server administrative passwords. Passwords should include at least three of these four characteristics: numeric character, special character, lowercase character, and uppercase character.
- **Implement directory services.** This allows authentication and authorization using the same login process employed throughout the rest of the network. It provides a way to control multiple iLO devices simultaneously. Directories provide role-based access to iLO with very specific roles and privileges based on time and location.
- **Implement two-factor authentication.** This provides additional security, especially when connections can be made remotely or outside the local network.
- **Restrict access to remote console port**. To provide tighter security, a user with supervisor rights can restrict access to the remote console port and can turn on encryption. For maximum security when the remote console is enabled, HP recommends that the administrator turn on the remote console encryption. For maximum security for customers who do not require the remote console feature, HP recommends disabling the remote console port.
- **Protect SNMP traffic**. Administrators should reset the community strings according to the same guidelines as the administrative passwords. Administrators should also set firewalls or routers to accept only specific source and destination addresses. If SNMP is not desired, administrators can disable this feature at the host. Administrators can also disable the iLO SNMP pass-through.

Conclusion

The design of the iLO processor allows customers to deploy their ProLiant servers without worry that the management processor will allow non-secure actions. The iLO processor uses strong authentication, highly configurable user privileges with strong authorization processes, and encryption

of data, keystrokes, and security keys. The hardware design protects keys and sensitive password information. The hardware design also facilitates a separation of the iLO management traffic from all host server traffic.

A networked environment has inherent security risks. The iLO processor mitigates many of these risks through authorization, authentication, and encryption. Administrators can further decrease the chance of attacks by following security recommendations, being aware of access points to the iLO devices and their host servers, and configuring their networks to eliminate any unnecessary services.

Appendix A: Digital certificates

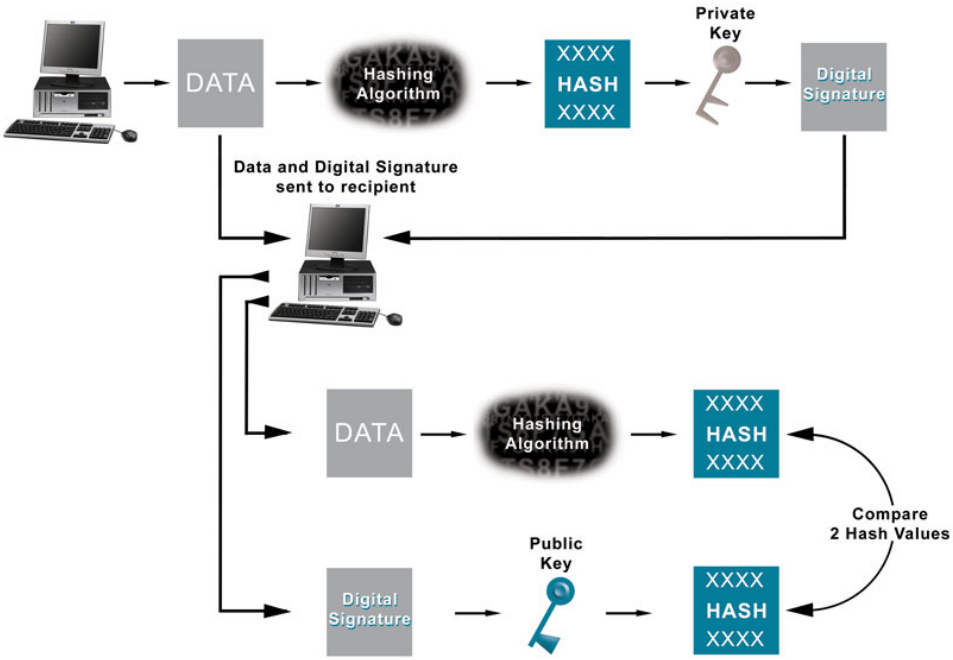
A digital certificate is an integral component of the SSL encryption technology. The digital certificate provides data integrity by ensuring that a third party cannot insert false data into the encrypted data stream. A digital certificate includes a public key based on RSA encryption and an accompanying digital signature (see Table A-1).

Table A-1. Components of digital certificates

Digital certificate component	Example
Unique name of owner	Subject DN: cn = Bob Smith, c = ACME, C = US
Unique serial number	8391037
Period of validity	Start: 1/5/97 1:02 End: 7/5/98 1:02
Revocation Information	CRL: cn = CRL2, 0 = ACME, c = US
Alternate subject identifiers	SubjectAltName: IP, DNS, email
Public key	mQCpAi3aE40AAAEE4KSlkYOhLlSNTrVcbogQuto…
Digital signature of certificate authority	wJD3Wsm8VqCQSjK/YpwOcVCcCG+Ai+drsqz4E…
Name of issuing certificate authority	CA DN: o = ACME, c = US

A digital signature typically uses the sophisticated encryption of the RSA encryption algorithm rather than a simple hashing signature (Figure A-1). The RSA algorithm, developed by Rivest, Shamir, and Adleman, is widely used for encrypting data using a public key/private key system. Also known as "asymmetric" cryptography, this system uses a widely distributed public key and a private key that remains secret to the owner. The two keys are mathematically linked so that data encrypted with the public key can be decrypted only with the private key. Conversely, data encrypted with the private key can be decrypted only with the public key. Because the algorithm uses two large prime numbers (the public key and the private key) that are difficult to factor, the algorithm is difficult to compute and therefore gives any data encrypted with that algorithm a reasonable amount of security.

Figure A-1. Example of how a digital signature works



Appendix B: SSH-2 support

The following table lists the SSH features supported by iLO.

Table B-1. Relationship between iLO SSH and the SSH-2 standard

	SSH-2 Standard	iLO SSH
Algorithm		
Server Host Key Algorithms		
ssh-dsa	Required	Supported
ssh-rsa	Recommended	Supported
X509v3-sign-rsa	Optional	Not supported
Encryption (same set supported both ways)		
3des-cbc	Required	Supported
blowfish-cbc	Recommended	Not supported
twofish256-cbc	Optional	Not supported
twofish192-cbc	Optional	Not supported
twofish128-cbc	Recommended	Not supported
aes256-cbc	Optional	Not supported
aes192-cbc	Optional	Not supported
aes128-cbc	Recommended	Supported
serpent256-cbc	Optional	Not supported
serpent192-cbc	Optional	Not supported
serpent128-cbc	Optional	Not supported
Arcfour	Optional	Not supported
idea-cbc	Optional	Not supported
cast128-cbc	Optional	Not supported
None	Optional; not recommended	Not supported
Hashing algorithm		
Hmac-sha1	Required	Supported
Hmac-sha1-96	Recommended	Not supported
Hmac-md5	Optional	Supported
Hmac-md5-96	Optional	Not supported
None	Optional	Not supported
Compression		
Zlib	Optional	Not supported

	SSH-2 Standard	iLO SSH
Algorithm		
None	Required	Supported
Language		
English (same as current Telnet)		Supported
Key exchange		
Differ-hellman-group1-sha1	Required	Supported
Public Key algorithms		
ssh-dss	Required	Supported
ssh-rsa	Recommended	Supported
X509v3-sign-rsa (certificates)	Optional	Not supported
X509v3-sign-dss (certificates)	Optional	Not supported
Spki-sign-rsa (certificates)	Optional	Not supported
Spki-sign-dss (certificates)	Optional	Not supported
Pgp-sign-rsa (certificates)	Optional	Not supported
Pgp-sign-dss (certificates)	Optional	Not supported
Client/User Authentication Method		
None	Must not be listed	
Public key	Required	Not supported
Host based	Optional	Not supported
Password		Supported
Client/User authentication parameters		
Default authentication timeout	10 minutes recommended	Hardcoded to 1 minute
Default SSH port	Default 22	Configurable. Defaults to 22.
Default number of attempts	20 recommended	Hardcoded to 3
User initiated key generation		Not supported

Appendix C: LDAP/LDAPS definitions

The LDAP/LDAPS protocol provides access to directories supporting the X.500 models but does not incur the resource requirements of the X.500 Directory Access Protocol (DAP). The LDAP/LDAPS protocol is specifically targeted at management applications and browser applications that provide read/write interactive access to directories. When used with a directory supporting the X.500 protocols, LDAP/LDAPS is intended to be a complement to the X.500 DAP.

The following are key characteristics of the LDAP/LDAPS protocol:

- Protocol elements are carried directly over Transmission Control Protocol (TCP) or other transport, bypassing much of the session/presentation overhead.
- Most protocol data elements can be encoded as ordinary strings (for example, Distinguished Names).
- A lightweight basic encoding rules BER encryption is used to encode all protocol elements.
- Referrals to other servers can be returned.
- Simple Authentication and Security Layer (SASL) mechanisms can be used with LDAP to provide association security services.
- Attribute values and Distinguished Names have been internationalized through the use of the ISO 10646 character set.
- The protocol can be extended to support new operations, and controls can be used to extend existing operations.
- Schema is published in the directory for use by clients.
- The LDAP protocol is used to read from and write to Active Directory. By default, LDAP traffic is transmitted unsecured. System administrators can make LDAP traffic confidential and secure by using SSL/Transport Layer Security (TLS) technology. Administrators can enable LDAP over SSL (LDAPS) by installing a properly formatted certificate from a certification authority (CA).
- To enable LDAPS, administrators must install a certificate that meets the following requirements:
- The LDAPS certificate is located in the personal certificate store of the local computer (programmatically known as the computer's MY certificate store).
- A private key that matches the certificate is present in the local computer's store and is correctly associated with the certificate. The private key must not have strong private key protection enabled.
- The Enhanced Key Usage extension includes the Server Authentication (1.3.6.1.5.5.7.3.1) object identifier (also known as OID).
- The Active Directory fully-qualified domain name of the domain controller (for example, DC01.DOMAIN.COM) must appear in one of the following places:
  - The Common Name (CN) in the Subject field
  - DNS entry in the Subject Alternative Name extension
- The certificate was issued by a CA that the domain controller and the LDAPS clients trust. Trust is established by configuring the clients and the server to trust the root CA to which the issuing CA chains.

Appendix D: Glossary

Table D-1. Common acronyms used in this document

Term	Definition
ASCII	Acronym for the American Standard Code for Information Interchange. ASCII is a code for representing English characters as numbers, with each letter assigned a number from 0 to 127. Most computers use ASCII codes to represent text, which makes it possible to transfer data from one computer to another. (Source: www.pcwebopedia.com)
ASIC	Application-specific integrated circuit (a custom-designed chip).
Boolean XOR	Boolean values are either true or false. The XOR, or exclusive-or operator, returns TRUE when comparing other values and only one of the other values is TRUE. If more than one other value is TRUE or if all other values are FALSE, then the Boolean XOR operator returns FALSE.
CA	Certificate Authority. A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. (Source: www.pcwebopedia.com).
CPU	Central processing unit
IP	Internet protocol. This term is used synonymously with IP address, or the numerical representation of a network node that supports IP. IP addresses consist of four "octets" separated by dots; for example, 192.168.1.1.
MAC	Media access control. The MAC layer is a sublayer of the data-link layer in the OSI model of network communication. In the Ethernet standard, every network connection must support a unique MAC value.
NIC	Network interface controller
NVRAM	Non-volatile random-access memory. This is memory that maintains data across power cycles.
OSI model	OSI stands for Open System Interconnection, a seven-layer protocol model for defining a networking framework.
PCI	Peripheral component interconnect. The industry-standard interconnect for input/output devices.
PKI	Public Key Infrastructure. A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. (Source: www.webopedia.com).
POST	Power-On Self-Test. The series of steps that the host system CPU performs following power-on. Steps include testing memory, initializing peripherals, and executing option ROMs. Following POST, the host ROM passes control to the installed operating system.
RISC	Reduced instruction-set computing. A type of processor representing a simple set of instructions that can be run at very high speeds. The alternative CISC processor, or Complex instruction-set computing processor, can perform powerful instructions that generally run at slower speeds.
ROM	Read-only memory
SDRAM	Synchronous dynamic random access memory
SNMP	Simple Network Management Protocol. A set of protocols for managing complex networks.

Term	Definition
VPN	Virtual private network, or a network that is constructed using public wires (the Internet) to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. (Source: www.webopedia.com).
XML	Extensible markup language. HTML and RIBCL are subsets of XML.

For more information

For additional information, refer to the resources listed below.

Resource description	Web address
Integrated Lights-Out home page	www.hp.com/go/ilo
Industry-standard servers technology papers	www.hp.com/servers/technology
Integrated Lights-Out Documentation Includes links to the Planning and configuration recommendations for Integrated Lights-Out processors, Integrated Lights-Out user guide, and other documents related to iLO	http://h18004.www1.hp.com/products/servers/management/ilo/documentation.html
Directory support on Lights-Out management products	http://h18004.www1.hp.com/products/servers/management/directorysupp/index.html
Software and drivers for lights-out processors	www.hp.com/go/ilo
Lights-out supported servers	www.hp.com/servers/ilo/supportedservers
Information about iLO 2 Advanced licenses	www.hp.com/servers/iloadv2

Call to action

Send comments about this paper to: TechCom@HP.com

TC081001TB, 10/2008