

LapLink Gold in a Secure Enterprise Environment

Understanding LapLink Security and Implementation

Disclaimer and Warranty

This paper is intended to be informational. The recommendations made are specific to the implementation and use of LapLink products in conjunction with firewall systems. This document is in no way to be considered a guide for configuring enterprise network security. Information systems security is highly complex and broad in scope. Professional assistance from a knowledgeable and reputable company is recommended for the design and implementation of an enterprise security policy.

Executive Summary

LapLink Gold combines the power, reach and flexibility of the Internet with the speed, reliability and ease of use of LapLink's core file transfer and remote control technology.

With LapLink Gold, the Internet becomes a convenient, secure tool for connection to another computer or network resources. Improved handling of adverse conditions and Internet directory support enable users to connect easily over the Internet without having to deal with poor connections or potentially changing IP addresses. As such, there are security considerations to be addressed before its deployment in a secure environment.

This paper provides IT professionals with a general overview of LapLink Gold, its security and functionality that may have an impact on security, especially in environments using firewalls.

Product Overview

LapLink Gold is an enhanced file transfer and remote control application that supports all common communication mediums. The application acts as a host service that accepts connections from clients over modems, networks (including the Internet) and cables. The services available include file transfer with synchronization, remote control and print redirection, text and voice chat.

An Overview of LapLink Gold Security

Security in LapLink Gold is implemented at the application level providing the general security policy for the application with specific options available for some services. A description of the general application security as well as the service specific options follows.

General Security

As stated previously, LapLink Gold supports multiple services that are accessed through various mediums. These mediums are presented in the form of ports. A port may represent a physical communications (COM) port using a modem or cable, or a protocol endpoint (such as TCP/IP) using a network connection and can be enabled or disabled individually.

Each LapLink system is identified by a computer name, which may or may not be the same as the Windows computer name. A user configurable logging facility is provided to track connections, security violations and file transfers.

Several services are installed with LapLink, one of which allows the option of configuring the application to startup prior to logon, enabling remote reboot and subsequent reconnect after the system restarts.

Access Control and Authentication

Access control in LapLink can be set to one of three modes:

- *Private* - No one may access this computer
- *Protected* - Access is restricted to authorized users
- *Public* - Anyone may connect to this system

For *Protected* systems, authorized users are defined in a local application account database using username/password pairs, this database is stored as <%WINDIR%>\TSI32\laplink.pwd in encrypted format. The encryption is based on XORing each data byte with a random number. When defining users, you can specify which services will be available to them, which folders they will have access to, whether to use modem dial-back and various other options.

Configuring LapLink as a *Public* system is similar to that of a *Private* system with the exception that there are no user accounts, anyone can access the system without a password and all users will have the same rights.

The authentication phase is encrypted using an MD5 one-way hash. If LapLink is configured to use a Cryptographic Service Provider (discussed in the Encryption section), then the hashed credentials are encrypted using a negotiated session key and the CSP as well. Under no circumstances are logon credentials transmitted or stored in cleartext.

Local Security

LapLink makes provisions for local security allowing a local password to be set and required and the ability to enforce the security policy for local connections (cable and wireless). The default is no security policy for local connections.

Encryption

LapLink offers the option of encrypting data traffic between a LapLink client and a LapLink host. The encryption can be configured to encrypt all data all of the time or to only encrypt data that is transmitted over a TCP/IP link (i.e.: Internet traffic).

The available encryption methods are:

- **LapLink Compatible** - This is a backward compatible encryption using a 16 or 32-bit (OS dependant) XOR of the data stream to be used with older LapLink clients.
- **CryptoAPI** - This is the recommended data stream encryption method. This method can use any installed Cryptographic Service Provider who supports the RC4 encryption algorithm and is installed on both the client and the host. The default CSP provided with Windows is a 40 or 128-bit RC4 implementation (depends on whether the OS is domestic or export software) based on the RSA toolkit.

Lockout

LapLink provides the option of configuring the system to lock out a users account after a specified number of failed login attempts.

LapLink Services

LapLink provides a number of services, some of which provide additional security configuration options. This section describes these services and their security implications.

Remote Control

The LapLink Remote Control service allows a client system to take control of a remote host system screen, mouse and keyboard. A client can also simply connect a Remote Control session and observe the host system and any activity that takes place on it.

The Remote Control service provides options for client systems to reboot the host system (disabled by default), the host system to reboot when a client disconnects (disabled by default), and the client system to black out the host systems screen.

File Transfer

LapLink's file transfer capabilities provide the ability to move files between two computers. The host system can specify which drives and folders are accessible to users accessing the system. Different privileges can be assigned to different users.

LinkToNet

The LapLink LinkToNet service allows a LapLink client to connect to a LinkToNet host and make use of the hosts' resources as well as any resources that may be available to that host on its network (including Internet connectivity). Additionally, the LinkToNet host acts as a LapLink proxy server allowing the client to LapLink from the LinkToNet host to other LapLink hosts.

Additional Services

LapLink provides additional services such as Print Redirection, Voice and Text Chat. For more information about these services, please consult the LapLink documentation.

Using LapLink Gold in Environments with Firewalls

Implementing and supporting LapLink in a firewalled environment is reasonably straightforward. Following is a description of the most common firewall types and implementations with suggestions and recommendations for permitting the use of LapLink securely. It is important to note that some firewall remote control and print redirection namely those using Network Address Translation (NAT), may not support the use of LapLink.

General Information

Most firewall implementations follow the principal of minimal access. This principal essentially specifies that if a protocol, server or service is not explicitly permitted to pass through the firewall, the request be rejected.

There are many different firewall architectures, the two most common being packet-filtering and proxy based, each with many implementation variations

that may overlap. How you enable LapLink will depend on the type of firewall you use, the implementation and your local security policy.

The LapLink host listens for client connections on its IANA assigned TCP port number 1547 (assigned and registered ports are defined in RFC1700).

Architectures

Most host, router or firewall products can act as a packet-filtering bastion host. In this scenario, all network traffic between systems on the internal trusted network and systems outside of the trusted network (such as the Internet) must pass through a single system that acts as a gateway (it may actually be many different systems but we will consider a single system for our purposes). This system will have defined a set of rules that specifies which hosts accept incoming traffic for which ports and which hosts can communicate with external hosts. The rule set can be broad and generic or highly customized and explicit.

A proxy or application firewall may be a true firewall product or a modified host (typically some variety of UNIX). Application firewalls implement rule sets similar to those of packet-filtering firewalls (and in fact most include packet-filtering functionality as well) but include much more intelligence and flexibility. An application firewall has a suite of predefined proxy services that accept service request from internal users and execute them on the users behalf to the appropriate untrusted host. Some application firewalls have an additional mechanism of packet inspection to check various criteria for a given protocol or service such as correct headers, packet formatting and length.

There are many, many more features and capabilities that are specific to one vendor or another, but they are outside the scope of this document. One last feature that is common among many application and packet-filtering firewalls is Network Address Translation (NAT).

NAT adds a layer of security through obscurity. When using NAT, systems on the internal trusted network use a range of IP addresses (typically non-routable reserved addresses as defined in RFC1918) and the NAT server maps those addresses to a range of valid Internet addresses. Systems outside of the trusted network do not know the internal addressing scheme of the trusted network and cannot communicate with its hosts directly. Additionally, some firewalls allow port multiplexing rather than mapping public addresses to private addresses. This is useful when a network does not have many or enough valid IP addresses for all of its internal systems.

Concerning NAT and LapLink, internal hosts will be able to connect to external hosts using LapLink, but external hosts will not be able to initiate connections to internal hosts. A final note on NAT; Internal hosts will be able to register with the LapLink Directory Server, but if using private, non-routable addresses, external hosts will not be able to establish a route to the LapLink host as the registered address is invalid on the public Internet (unless the client is on the same network). This can certainly cause some confusion with users, as the registration process is successful. NAT prohibits external LapLink clients from being able to communicate with LapLink hosts on a secured network; this is the intended behavior of NAT.

Sample Firewall Configuration Directives

Presented here are sample configuration directives for various firewall products. Currently there is no proxy or stateful inspection mechanism for LapLink. Access is allowed by opening TCP port 1547 to specific hosts or the network at the discretion of the security administrator. Again, for sites using NAT with private address space or NAT with port multiplexing, you will be unable to allow incoming LapLink connections. Sites using NAT and mapping their internal IP addresses to valid public addresses can, if they choose, set up static mappings for particular LapLink hosts to be reached from the outside.

For demonstration purposes, we will be referencing the private network 192.168.100.0/24 as our internal trusted network with all filtering relative to the public Internet. Implementation is similar for any external network.

For each example, we show how to permit LapLink to connect to the host 192.168.100.45; permitting LapLink to connect to multiple hosts or an entire network is a trivial modification. This does not imply that hosts with private addresses can actually be reached from outside the trusted network, but is a safe example to use.

Sample Firewall Configuration Directives (cont)

Cisco Router using Access Lists

In privileged exec mode, create the following access-list (or append to an existing access-list) then apply the access-group to the external interface.

```
access-list 110 permit tcp any 192.168.100.45 eq 1547

interface ethernet0
    ip address 192.168.100.1
    access-group 110 in
```

Cisco PIX Firewall

In privileged exec mode, create the following conduit statement (note that this is contingent on there being an existing static statement mapping the external address to an internal address, not shown here).

```
conduit permit tcp host 192.168.100.45 eq 1547 any
```

CheckPoint Firewall-1

CheckPoint Firewall-1 is accessed primarily through a GUI interface. To create a rule through the GUI interface you will need to define a Network Object corresponding to the host or network you wish to allow LapLink access to then define an access rule.

To add a rule:

Log in to the Firewall-1 GUI
Select Add Rule from the Edit Menu and choose the desired insertion point
Leave the Source as Any
Set the destination to 192.168.100.45 (you may need to create an object for the endpoint)
Set the Service to LapLink (you will need to create the LapLink Service as a TCP service on port 1547)
Change the Action to Accept
Set any additional options as desired

Consult your Firewall-1 documentation for additional information.

Axent Raptor Firewall

As is the case with CheckPoint Firewall-1, the Raptor Firewall from Axent Technologies is managed and configured through a GUI with the actual configuration files neatly tucked away in the background. The recommended and supported method of administration is using the GUI.

To enable access to an internal LapLink host, you will need to create a rule:

Click the Rules button on the Hawk toolbar
Provide a description for the rule if desired
Select All on the For pulldown menu
Select Universe in the From field
In the To field, select the LapLink Host (you may need to create this entity)
Select the Permit Certain Access radio button
Include only the LapLink protocol in the Included window (you must create a GSP for LapLink)
Set any additional options and click Create

Consult your Raptor documentation for additional information.

Network Associates (TIS) Gauntlet Firewall

The Gauntlet Firewall now provides a GUI administration tool for configuring services, though all configuration information is stored in text files that may be edited directly if desired. Here we demonstrate how to permit LapLink to our internal host system by modifying the configuration files.

Add the following line to your /etc/services file to identify our protocol

```
laplink      1547/tcp      laplink      # LapLink Protocol
```

Copy the Gauntlet proxy template script
/usr/local/etc/mgmt/rc/template to
/usr/local/etc/mgmt/rc/S1547laplink

Edit the S1547laplink script and modify the following:

```
TITLE=laplink-gw  
SERVICE="LapLink"  
PROXY=/usr/local/etc/plug-gw  
PORT=laplink  
VARIABLE=laplink_proxy  
ARGS="-as laplink-gw"
```

Edit the netperm-table file to configure the rules for the LapLink proxy service by adding or modifying the following:

```
# Add above policies  
laplink-gw: port laplink * -plug-to 192.168.100.45 -port laplink  
  
# Add to policies  
# Permit LapLink  
policy-laplink-gw_Untrusted: permit-proxy laplink-gw  
policy-laplink-gw_Untrusted: description LapLink host access
```

Using a Proxy to Validate Transmitted Data

For any sites that wish to allow external access to an internal LapLink host but have more stringent security policies, a custom proxy can be written to perform stateful inspection of the data packets destined for LapLink hosts.

The design of such a proxy service is well beyond the scope of this document and is specific to the firewall and operating system in use. What is provided here is information for identifying valid LapLink packets.

LapLink packets are easily identified by checking the first data byte of TCP packets destined for port 1547 on the LapLink host. For Ethernet frames, the Ethernet header is 14 bytes, the IP header is 20 bytes and the TCP header is another 20 bytes for a total base frame header length of 54 bytes. For a TCP segment in an IP datagram in an Ethernet header this puts the first data byte at 0x36 for frames carrying user data.

The first data byte at 0x36 in a packet destined for port 1547 on a LapLink host will be one of the following values; 0xFF, 0x0F, 0xF0, 0xE0 or 0x0E.

Verifying the destination port and first data byte of packets sent to a LapLink host should provide a reasonable degree of certainty that this is a valid LapLink packet.

Conclusion

In conclusion, to enable access to an internal LapLink host, you must allow access from outside your trusted network on TCP port 1547 to the LapLink host or hosts. To reiterate about NAT, in most cases the use of NAT will prohibit accessing LapLink hosts on your internal network from an external network. This is the design and intended behavior of Network Address Translation.

References

The MD5 Message-Digest Algorithm

<http://www.ietf.org/rfc/rfc1321.txt>

Microsoft CryptoAPI

http://msdn.microsoft.com/library/sdkdoc/crypto/portalapi_3351.htm

RC4 Stream Cipher

<http://www.rsasecurity.com/rsalabs/faq/3-6-3.html>

Assigned Numbers

<http://www.ietf.org/rfc/rfc1700.txt>

Address Allocation for Private Internets

<http://www.ietf.org/rfc/rfc1918.txt>

Cisco Access-Lists

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/sbook/sip.htm#xtocid205852>

Cisco PIX Firewall

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/index.htm

CheckPoint Firewall-1

<http://www.checkpoint.com/products/firewall-1/index.html>

Axent Raptor Firewall

<http://www.axent.com/product/rsbu/firewall/default.htm>

Network Associates Gauntlet Firewall

http://www.nai.com/asp_set/products/tns/gauntlet.asp