IVI Standards Updates for Secure Network Connections

The IVI Foundation is responsible for numerous standards that facilitate creating multi-vendor test systems. Several of these standards have been updated to provide for secure communication between test system computers and instruments. These changes are:

- IVI-6.1: High-Speed LAN Instrument Protocol (HiSLIP) has been updated to make secure connections using TLS (Transport Layer Security)
- IVI VISA specifications had minor updates so VISA programs can specify and perform secure communication
- IVI-6.5: SASL Mechanism Specification (*New*) was created to enhance interoperability between instruments and VISA libraries

IVI-6.1: High-Speed LAN Instrument Protocol (HiSLIP)

The IVI HiSLIP protocol was originally completed in 2010. It provides GPIB emulation for network connections. This simplifies moving instruments between GPIB, network, and USB TMC connections, all of which support several operations important for instrument control. The key features of HiSLIP are:

Data Transfer	Transmission of SCPI (or other) GPIB messages
Service Request	An asynchronous request from the instrument to the client
Device Clear	An asynchronous clear operation to regain control of an instrument with minimum delay
Serial Poll	A mechanism that allows the client to check the status of the instrument in parallel with any GPIB message handling or measurement operations.
Remote/Local	GPIB remote/local functions provided arbitration between the front panel and GPIB control. HiSLIP extends this with general purpose locking which is important in a network environment where several clients may be using the same instrument.
Message Exchange Protocol	IEEE 488.2 defines a message exchange protocol that helps to ensure that data communication between the controller and the device is always synchronized – that is, that device responses always align with client requests. HiSLIP provides for this protocol.

The IVI HiSLIP protocol was extended in 2020 to provide secure connections along with these features. Using HiSLIP rev 2, clients connect much like a browser connects securely to a website. That is, the instrument provides a certificate that is either signed by a trusted authority or otherwise known to the client to be a valid certificate. Once the client determines that the certificate identifies the intended

instrument, it uses that certificate to establish secure encrypted communication between the instrument and the client.

Creating a Secure Connection

There are several ways that the client may determine that the certificate represents the intended instrument:

1. The instrument certificate may be signed by a trusted authority. For instance, a certain instrument vendor may sign the certificate, or the LXI consortium may have signed the certificate. The signatures are verified using standard cryptographic techniques.

2. The client may have established in advance that this instrument certificate will be provided by this instrument. For instance, an operator or some tool may have provided the client with the certificate and indicated that the instrument that presents this certificate is to be trusted.

3. There is a family of protocols known as SCRAM whereby the client and instrument both prove that they have some client credential (typically a client username and client password). The client can trust that this is the intended instrument since it has demonstrated that it knows the client's username and password. Also, the instrument can trust the client since it demonstrated that it knew the username and password as well.

These mechanisms all establish a connection that is encrypted, and the client can be assured that it is connected to the instrument it intended. This is the conventional definition of a secure connection and is what a web browser establishes before displaying the lock icon.

Client Authentication

In addition to basic secure communication, in some cases, it is important for instruments to ensure that only certain clients are permitted to connect to it. Therefore, HiSLIP revision 2 has provisions for instruments to validate that the client attempting to connect is permitted to connect to it.

To validate the client, HiSLIP incorporates a network standard known as SASL (the Simple Authentication and Security Layer specified in RFC 4422) that provides a standard way for the instrument to acquire client credentials. By using SASL, many different types of credentials can be exchanged. A typical example would be for the client to present a username and password that is validated by the instrument. SASL specifies how this exchange takes place.

Some examples of client authentication supported by HiSLIP are:

- The client may present a username and password
- The client may present a certificate that is validated by the instrument much in the same way that clients validate instrument certificates
- The clients may connect anonymously (the client is not authenticated)

The instrument configuration has to specify what credentials to accept, and the mechanism used to present them.

VISA Library Changes

As the previous sections illustrate, a secure connection requires some additional system configuration. The VISA library (which is the client) needs to know:

- How VISA will validate the certificate presented by the instrument (recall that the instrument is always identified by a certificate). This could include a list of trusted authorities, a list of specific instrument certificates to accept, and/or SCRAM credentials.
- If instruments are configured to require client authentication, the clients also need to know what client credentials to provide to the instrument so the instrument will permit this client to connect.

The VISA specifications have been updated to provide a way for the VISA programmer to indicate this information to VISA when it establishes the connection.

This information cannot just be directly put in the VISA program because it may contain credentials (such as a username and password) that should not be exposed in the customer program. Furthermore, the programmatic interface to provide this additional information would be quite complex and would make it difficult to add secure connections to new or existing systems.

VISA handles this problem by delegating the configuration of the VISA library to the VISA vendor configuration tools. Then, when the VISA connection is created, the VISA library is passed a single identifier. The VISA library then consults its own secure database to extract the appropriate instrument validation and client credentials to securely access the device.

The VISA library syntax to do this only requires adding the credential information to the instrument address string when opening a connection. The following is an example of the new syntax that in addition to specifying the device address (*MySignalAnalyzer),* also specifies the secure configuration as *CredentialInformation*:

TCPIP1::CredentialInformation@MySignalAnalyzer

The *CredentialInformation* string is a new string. This identifier indicated to the VISA library the security configuration to use for this connection. The security configuration includes information about the instrument that VISA is going to connect to so that VISA can validate the instrument and establish a secure connection. It also tells the VISA library the client credentials that VISA needs to present to the instrument to be granted access to the instrument.

VISA Changes for Security

The addition of the *CredentialInformation* in the open string is the most important change to the VISA specification since this is the key to making a secure connection to the instrument. VISA also added a handful of new attributes. A VISA attribute is a value that can be read or written from the VISA program that contains information or configuration for that VISA session.

The attributes that were added to VISA can be used by the client program to further investigate the connection it has made to the instrument so that the program can take extra steps to validate that the connection satisfies more subtle security requirements. For example, inspecting the issuer of the certificate or the type of encryption selected by TLS. The following attributes were added:

VI_ATTR_TCPIP_HISLIP_ENCRYPTION_EN	For HiSLIP, this indicates if the connection is encrypted. This can be used to turn off encryption, for instance for a higher speed transfer.
VI_ATTR_TCPIP_SERVER_CERT	This permits the VISA program to acquire the full certificate presented by the instrument so the VISA program can further confirm that this is the intended device.
VI_ATTR_TCPIP_SERVER_CERT_SIZE	Used to determine the buffer size to get the Server Certificate.
VI_ATTR_TCPIP_SERVER_CERT_ISSUER_NAME	The name of the authority that issued the certificate.
VI_ATTR_TCPIP_SERVER_CERT_SUBJECT_NAME	The name of the device the certificate was issued to.
VI_ATTR_TCPIP_SERVER_CERT_EXPIRATION_DATE	The expiration date of the certificate. Note that VISA will not accept an expired certificate as authentic.
VI_ATTR_TCPIP_SASL_MECHANISM	The SASL mechanism used to authenticate the VISA client.
VI_ATTR_TCPIP_TLS_CIPHER_SUITE	The cipher suite being used for encryption.
VI_ATTR_TCPIP_SERVER_CERT_IS_PERPETUAL	Indicates if the server certificate has an expiration date. Perpetual certificates are considered untrustworthy by some organizations. The VISA-specific configuration may enable or disable the use of perpetual certificates.

The IVI-6.5: SASL Mechanism Specification

After completing the HiSLIP and VISA standards and working with the LXI consortium, the team concluded that an additional standard is necessary to assure interoperability between VISA libraries and instruments. The difficulty is that the IVI and LXI standards all rely on other industry's standards and RFCs for most of the secure behavior, however, some of the SASL mechanisms are not sufficiently specified to assure interoperability. Therefore, IVI created the *SASL Mechanism Specification*. This is a short specification that indicates how instruments and VISA libraries should treat some of the options left up to implementors in the SASL mechanisms. Without this, devices and VISA libraries would have to make arbitrary decisions that could result in incompatibilities.

The *SASL Mechanism Specification* calls out limitations on usernames, how to make anonymous connections and some specific details of how SCRAM is implemented.

Summary

Both IVI and LXI rely heavily on the industry RFCs and standards for secure connectivity. However, limited extensions were necessary to both LXI and IVI standards to fully support secure connections.

Customers moving to securely connect to instruments should expect that they need to provide both the VISA library and the instruments with additional configuration information so that they know what devices to expect at the other end of the cable and how to identify themselves.

However, the actual programs and instrument APIs are unchanged. The only programming change to securely connect to instruments is the addition of the *CredentialInformation* in the VISA connection string. None of the actual IO instructions are impacted by the secure connection.

The IVI standards discussed here are free for download at https://ivifoundation.org

Joseph Mueller
Keysight Technologies