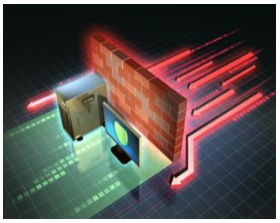
LXI Version 1.6 Security Updates

The LXI Consortium is responsible for establishing standardized behavior for LXI compliant devices that are connected to and controlled by a computer over LAN. The use of LXI compliant devices greatly simplifies the creation and interoperability of multi-vendor test systems.



The increase in cybersecurity threats is seeing more exploits involving network connections to devices. Previously, businesses would address these threats by isolating sensitive equipment and data behind firewalls. Now, the sophistication of today's bad actors and the risk of insider threats have driven the industry to add new layers of protection and promote the concept of "defense in depth". The serious threat of nation-state bad actors has further increased the need for security that is robust against highly sophisticated attackers.

The LXI Version 1.6 specifications have been updated to address the need for secure network communication with LXI devices. These updates include:

- LXI Security Extended Function: A new specification that establishes requirements for LXI instruments that provide secure network connections for both command-and-control and for the instrument's web interface.
- LXI API Extended Function: A new specification that specifies a REST API to configure and query the settings on an instrument that are important for the instrument to work in a secure environment.
- Various changes to the main LXI Device specification and other extended functions to extend them for security and make minor updates.

LXI Security Extended Function

The LXI Security Extended Function is an optional specification for instruments that need to provide secure communication. Instruments that conform with the LXI Security Extended Function are also required to comply with the LXI API Extended Function since it provides the mechanisms that are required to configure instruments for secure operation.

Communication is considered secure if:

- A client (usually the test system computer) is assured it is connected to the desired server (instrument in this case).
- The communication is exchanged exactly as intended by the client and the instrument.
- A third party is unable to observe the communication.

Verifying Instrument Identity

There are several approaches for establishing the instrument identity. In every case, a certificate is used that also provides for the encryption necessary to keep the communication private. This section describes the mechanisms required by the LXI Security Extended Function.

LXI achieves secure communication by utilizing existing network security standards. As such, secure communication always requires a certificate as specified by X.509. Generally, the certificate accomplishes two things:

1. It establishes the identity of the instrument. Allowing the client to be certain it has connected to the desired instrument.
2. It contains the cryptographic information necessary to establish encrypted communication.

Verifying Instrument Identity with Trusted Authorities

When a client receives a certificate from an instrument it needs to verify that the certificate is from the intended instrument. There are several ways that a client can determine that the certificate is from the desired instrument. It can:

- Verify that the instrument certificate was signed by some trusted authority, such as the LXI Consortium or the instrument vendor. Since the certificate was signed by a third party that is trusted (such as the instrument vendor or the customer's own signing authority) the instrument certificate itself can be trusted.
- The client can recognize the instrument certificate because it was provided to the client in advance, therefore the client knows that this certificate represents the intended instrument and is valid.
- There is a family of protocols known as SCRAM whereby the client and instrument both demonstrate that they possess a username and password. Thus, the client can trust the server, and the server can trust the client

To verify a certificate is from a trusted authority, the client uses an additional certificate that was provided by the trusted authority that can be used to verify a special signature field in the instrument certificate. Once this signature field is verified, the entire certificate, including the instrument's identity, can be trusted. This approach works well if the client wants to trust all instruments that have certificates from a known authority, such as the instrument vendor or the LXI consortium. The problem with this approach is that allows *any* instrument from that vendor (or LXI) to be used in the system. Therefore, if an attacker somehow counterfeited a vendor's signature, they could impersonate the intended instrument. Thus, verifying instrument certificates using the instrument vendor or the LXI consortium signatures provides a simple way to establish secure connections, but it provides the system designer with limited control of the permitted instruments.

Another way to use certificates from a trusted authority is to have the customer operate the trusted authority, as part of a Public Key Infrastructure (PKI). PKIs are the most common approach to secure network communication in commercial and defense networks. The customer system creates and provisions the certificates to the instruments, and the clients only trust certificates from the customer's trusted authority. This system provides excellent security and configurability, however it does require that the customer tie the instruments into their certificate authority, as well as create the infrastructure to provision certificates to the instruments.

Verifying Instrument Identity with Pre-Configured Certificates

One of the most robust ways for a client to ensure they are communicating with the desired instrument is to provide the client with the certificates of the instruments in advance. In this way, when the

instrument provides that certificate the client is certain it is connected to that instrument. An imposter is unable to fake the certificate because the cryptographic information used to communicate with the instrument is established by the certificate and is not transferrable to another instrument. This has the disadvantage that the initial configuration of the system requires that the instrument certificates are provided to the clients in advance. This also creates additional complexity in deploying systems and swapping out instruments for calibration and repair since the client needs to be configured with the certificates of any instruments that it will use.

Using SCRAM Instead of Certificates

The SCRAM protocols utilize a username/password known to both the client and server. The SCRAM protocol allows each party to verify the other party is holding the same username/password. The protocol ensures that the username/password is not accidentally disclosed when the credentials are verified. The certificates that are used for communication are all generated dynamically as needed and discarded after use. This approach has the disadvantage that it relies on less-secure username/password combinations instead of cryptographically signed certificates that include the instrument identity. In addition, usernames and passwords need to be deployed to both the instruments and the clients to setup a system.

LXI Security Extended Function Requirements

In addition to requiring the instrument identification mechanisms above, the LXI Security Extended Function:

- Specifies details of how instruments manage certificates and other credentials.
- Requires flexible configuration of the instrument generally necessary in secure environments.
- Includes provisions for controlling client access to instruments. Many customers in secure environments need to control which clients are permitted access to instruments.

LXI API Extended Function (Secure REST API)

With the addition of security, LXI has added a REST API for instrument configuration. At this time, all the APIs specified are associated with security requirements. However, it is possible that the API will be extended independent of security. There are two groups of security APIS. Some provide for fine-grained control of the instrument network configuration, and another set provides for management of the certificates that are on an instrument.

It is very common when an instrument is placed on a secure network for administrators to need very detailed control of the network configuration of the instrument. For instance, discovery protocols may be disabled to make it more difficult for attackers to discover instruments or unused protocols may be disabled to eliminate them as a point of attack. Instead of calling out detailed requirements in both the LXI Security Extended Function and the LXI API Extended Function, the LXI Security Extended Function requires that the instrument support the instrument network configuration APIs.

The LXI API instrument network configuration methods can be used to provide detailed configuration of various network protocols in an instrument, including IPv4 and IPv6 configuration, mDNS configuration, HiSLIP Configuration, and other protocols typically implemented in instruments. The LXI Security

Extended Function does not have new requirements regarding the implementation of protocols, but it requires that instruments that implement those protocols provide the API configuration as specified by LXI. The LXI instrument network configuration API is organized so that all of the settings common to the test systems instruments are in a single XML file, permitting a single configuration to be sent to all instruments in the system. The only instrument specific configuration has to do with instrument network addresses that cannot be shared with other instruments.

A second important group of LXI APIs are those that are used for certificate management. Since most conventional commercial secure networks use a PKI, it is important for customers to be able to integrate instrumentation into that infrastructure. The LXI certificate management APIs provide that by providing APIs to catalog, add, remove, and request new certificates.

The LXI API Extended Function requires that the API methods can be restricted to authorized clients using either HTTP security schemes or an API key.

LXI Device Specification and Extended Function Updates

As part of the LXI 1.6 update, the LXI base specification (known as the LXI Device Specification) and all of the LXI extended function specifications were reviewed and updated as appropriate for security and current network practices:

- LXI Device Specification: Security updates to require an HTTPS web server and not allow the use of a blank password. Several other minor updates were made to incorporate LXI Version 1.5 clarifications and other changes.
- LXI HiSLIP Extended Function: Updates to require IVI HiSLIP rev 2 which optionally supports secure connections using TLS and Client/Server authentication. These features are optional in the LXI HiSLIP Extended Function but are required if the instrument supports the LXI Security Extended Function.
- LXI IPv6 Extended Function: Updates to align with the NIST IPv6 Profile requirements, static and DHCPv6 addressing are now required, added more enable/disable capabilities and LXI Extended Functions supported on IPv4 must also be supported on IPv6.

Summary

As security becomes a more important concern in our modern world, and nation-state actors need to be considered as possible attackers, creating truly secure test and measurement systems is increasingly important. Secure network communication is an area of growing concern and rapid ongoing technical innovation. LXI has taken an initial step by providing the LXI security standard updates including the new Security and API specifications. The LXI consortium anticipates additional security updates and capabilities will be required.

The LXI standards discussed here are free for download at https://lxistandard.org

Steve Schink
President of the LXI Consortium
Joseph Mueller
Keysight Technologies