LXI Security

Introduction

Security is a critical attribute of industrial networks and Industry is giving a growing amount of attention to cybersecurity issues. Since LXI instruments are connected to company networks cybersecurity is also an important topic for LXI. This article gives an overview on the general security concepts and provides a summary of the current state of the LXI Security Working Group discussions and proposals for Test Engineers setting up LXI based test systems and IT departments supervising the company network.
We will follow-up with more articles on the technical details e.g. for the secure HiSLIP protocol and the secure web browser interface using X.509 certificates.

Levels of Risk Introduction

LXI instruments are connected to company networks. Depending on the test setup for the LXI instruments there are different levels of risk introduction:
Benchtop setups (e.g. peer to peer connection) w/o connection to the company network are per se very secure because there is no connection to the outside world. Test system setup with an isolated subnet are secure but the test computer needs a (second) connection to the company network. The most common scenario is a test system directly connected to company network, because in that case other test computers can also access the LXI instruments in the test system (e.g. for remote debugging). And last not least the most vulnerable setup is a test system with direct Internet connections (e.g. remote monitoring in the field). You can find the different setups and their pros and cons on the LXI Consortium web site.

LXI Security Ecosystem

The following standards are relevant for cybersecurity for A&D and industrial test systems which the LXI Security WG took into consideration:

- NIST: Framework for Improving Critical Infrastructure Cybersecurity (NIST 800 SP Series)
- Industrial Automation & Control: IEC 62443 standards (equivalent to ISA 99)
- UL CAP: Underwriters Laboratories Cybersecurity Assurance Program UL 2900 series of standards
- IIC Industrial Internet Consortium: Industrial Internet Security Framework IISF
- OWASP (Open Web Application Security Project): IoT - Top Ten Application Risks

When we look at the LXI Security Ecosystem there are commonalities which LXI instruments share with IoT (Consumer Internet of Things), IIoT (Industrial Internet of Things) and IT (Information Technology). These observed communalities are device security, data security and network security.

Primary goals for security within industrial networks are following the key principles C.I.A. which means **Confidentiality, Integrity** and **Authenticity**.
Confidentiality ensures that data transported in the network cannot be read by anyone but the intended recipient. Integrity means any message received is confirmed to be exactly the

message that was sent, w/o additions, deletions or modifications of the content and finally Authenticity ensures that a message that claims to be from a given source is, in fact, from that source.
Authorization is another important aspect - both, authentication and authorization require a strong device identity.

The following communication channels are used within LXI Test Systems:

- Remote Control of the LXI device which is SCPI based (ASCII) and using TCP/IP (either raw socket-interface, VXI-11 or HiSLIP)
- Web Browser Interface based on HTTP protocol to connect to the LXI instruments web server

To ensure secure communication between test computers and LXI instruments encryption is required. The standard for encryption for the remote control of LXI instruments is TLS (Transport Layer Security) and for the web browser interface HTTPS (secure HTTP) which combines the HTTP protocol with TLS.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a protocol that provides privacy and data integrity between two communicating applications. It's the most widely deployed security protocol used today and is used for Web browsers and other applications that require data to be securely exchanged over a network, such as file transfers, VPN connections, instant messaging and voice over IP.

TLS evolved from the Secure Sockets Layer (SSL) protocol and has largely superseded it. Key differences between SSL and TLS that make TLS a more secure and efficient protocol are message authentication, key material generation and the supported cipher suites, with TLS supporting newer and more secure algorithms.

TLS is composed of two layers – the TLS Record Protocol and the TLS Handshake Protocol. The Record Protocol provides connection security, while the Handshake Protocol allows the server and client to authenticate each other and to negotiate encryption algorithms and cryptographic keys before any data is exchanged.

Public Key Infrastructure (PKI)

In the Public Key Infrastructure (PKI), digital certificates are based on public key cryptography. The PKI consists of a set of components, policies, protocols, and technologies that provide data authentication, integrity, and confidentiality through the use of certificates, and public and private keys.

Data is protected by applying a hashing algorithm and signature algorithm to the original message. A hashing algorithm is an intricate mathematical algorithm which is applied to the message.

With public key cryptography, the key that encrypts data is called a public key. The key that is used to decrypt data is called the private key. While the public key can be publicly distributed, the private key is kept secure.

Digital certificates

Certificates are the foundation of the PKI. The certificate contains the public key of the user e.g. the LXI instrument. The public key can be used to encrypt and sign data before it is transmitted over the network to the LXI instrument. The digital certificate contains information such as the certificate version, serial number, signature, issuer, and validity period, among other information.

Certification Authorities (CAs)

A Certificate Authority (CA) is a trusted entity that generates and validates digital certificates to users, computers, applications, and services. The CA adds its own signature to the public key of the client. This essentially indicates that the public key can be considered valid, by those parties that trust the CA.

CAs can be setup in a hierarchical structure and define a CA trust model. In the CA hierarchy, you would define root CAs, intermediate CAs and leaf CAs. Users that trust the root CA would automatically trust all subordinate CAs beneath the root CA, which received certificates from the particular root CA.

Mutual Authentication & Encryption

To start the communication between a client (test computer) and a server (LXI instrument) the client verifies the server identity via the certificate. For LXI test systems this is a mutual authentication step because the server also verifies the client identity.

The next step is exchanging keys for encryption and also agreeing on the cypher suite and options to encrypt this session.

In order to prevent man-in-the-middle attacks, the public keys exchanged in the TLS handshake must be certified. Usually, this is achieved by using X.509 certificates (SSL certificates) where 3rd party trust authorities (CAs) cryptographically bind identities to public keys.

In TLS with X.509 certificates, the communication peer is identified via its DNS name (e.g. oscilloscope3.company-net.com) and/or its IP address (e.g. 192.168.0.4). For LXI devices, both can change if the device is connected to a different network. This requires a new X.509 certificate to be issued by the CA (either company internal CA or public CA).

Encryption of the communication channel is only the first step. Users authorized for using SCPI remote commands must identify themselves by providing a username and password or other authentication mechanisms.

Certificates for LXI Devices

The LXI Security WG proposes to use two different certificates for remote control and the secure web browser interface.

The certificate for the remote-control interface (SCPI) is based on a specific LXI Certificate with identity attributes like Manufacturer, Device type, Serial number, etc. This is a derivate

of the information you can get by using the “*IDN?” query. The format and metadata of the LXI Cert are standardized by the LXI Consortium.

The Root of Trust is a private trust model (compared to X.509 certificates). Deployment is through installation by the LXI vendors during manufacturing. The lifetime of the LXI cert with more than 10 years is much longer compared to X.509 certificates which usually have 2 years max.

For the web browser interface, we rely on the standard public trust model based on X.509 certificates which allows secure web server access. The problem here is that the LXI vendor has no fixed IP address for that LXI instrument.

To overcome this limitation the LXI Security WG proposes to use a X.509 provisioning service. Whenever the LXI device gets a new IP address it requests X.509 certificates via the provisioning server under a public trust domain using the LXI certificate for authentication.

During this step the device will compare the DNS records stored registered in the global DNS and update them if necessary.

Summary

The LXI Security Working Group proposes the described general security measures and concepts for LXI based test systems.
We will follow-up with more articles on the technical details for the secure HiSLIP protocol and the secure web browser interface using X.509 certificates.