State of the LXI Security Working Group

By Jochen Wolle, TSEP

The LXI standard provides a consistent, industry-wide method for communicating with LAN based instruments. To meet the ever-increasing demand for security, the LXI Consortium has chartered a Security Working Group tasked with developing an LXI Security Extended Function specification. This article provides a summary of the current state of the LXI Security Working Group discussions and proposals.

Primary goals for security within industrial networks are following the key principles 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 and finally Authenticity ensures that a message that claims to be from a given source is, in fact, from that source.

To ensure secure communication between test computers and LXI instruments encryption is required. The extensions to the standard will support authenticated/encrypted communication to T&M instruments and will also address security for LXI instrument hosted webpages, confirming device authenticity and providing secure communication

The LXI Security Working Group has developed an initial framework for secure instrument communication based on the Public Key Infrastructure (PKI) that provide data authentication, integrity, and confidentiality using digital certificates, and public and private keys. This was done in close collaboration with GlobalSign as our Certificate Authority (CA) which is a trusted entity that generates and validates digital certificates to users, computers, applications, and services. The proposed solutions were successfully prototyped and accepted by the LXI Consortium early this year 2019.

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. The certificate is a X.509 certificate derived from the IEEE802.1AR standard with Unique Device Identities (IDevIDs) for each piece of instrumentation. Deployment is through installation by the LXI vendors during manufacturing directly in cooperation with GlobalSign.

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 the X.509 provisioning service from GlobalSign. 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.

LXI Security Extended Function Specification

The concepts described above will be part of the LXI Security Extended Function. In addition, the LXI Security Working Group reviewed the LXI core and extended specifications to identify topics were security is relevant.

The LXI standard will roll to version 1.6 when the LXI Security Extended Function will be released. This allows additional editorial changes and clarifications to the existing core and extended functions to cover the requirements and extensions for security.

Topics which need more investigations are IEEE1588 and the LXI Event Messaging Extended Function because both need secure UDP multicasts. Other topics are already covered like mDNS and ICMP PING security issues.

For the remote-control communication, we are relying on the HiSLIP2.0 version which is currently developed by the IVI Foundation in close cooperation with the LXI Security WG. HiSLIP2.0 enables secure encryption of the communication based on the IDevID certificate of the LXI instruments. The release of HiSLIP2.0 is expected at the end of this year 2019.

The LXI Security Working Group will start to work on the specification as soon as the investigations on the remaining open topics are done. The plan is to distribute a draft standard to the member companies for ratification at the end of 2019.

In addition to the LXI Security Extend Function specification the LXI Security WG will work on the extensions for the LXI Reference Design and the LXI Conformance Tests to cover the LXI Security Extended Function.