Securing LAN-based Instrumentation Communication

LXI Working Group Status Review

Tom Sarfi
Business Development/NPI
Pickering Interfaces
tom.sarfi@pickeringtest.com

Rev NDIA_ATC_0319

www.lxistandard.org

Use the connection you already know!

Topics to be covered

- Introduction & Overview Security Standards

- LXI Communication Channels
  - Remote Control Web Browser Interface
  - Encryption

- PKI – Public Key Infrastructure
  - Certificates / Public & Private Keys / Encryption
  - Certificate Authorities (CAs)
  - Public Trust / Private Trust

- LXI Security WG Proposals for Secure Communication

Introduction – LXI Security Efforts

Background:

- The LXI standard provides an industry-wide method for communicating with LAN based instruments.
- There has been a growing demand by customers to ensure that LXI instrument communication channels are not compromised
- The LXI Consortium has chartered a Security Technical Working Group tasked with developing an LXI Security Extended Function specification.

What the Extended Function *will* address:

- Confidentiality, Integrity and Authentication of data transported across a test network
- The extensions to the standard will support authenticated/encrypted communication to T&M instruments and will also address security for instrument hosted webpages.

What the Extended Function *will not* address:

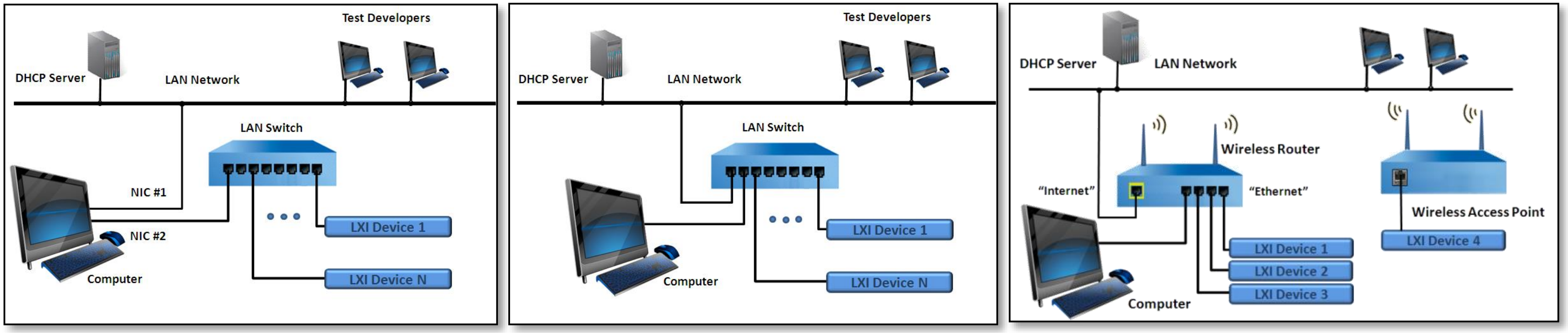
- Introduction of malicious software, counterfeit parts prevention, etc.

Status

- Initial framework for secure communication is complete and the prototyping of proposed solutions is underway.
- Draft standard for ratification is targeted for H2 2019.

Levels of risk to be considered

- Basic 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 (e.g. peer to peer connection) w/o connection to the company network
    - Test system setup with isolated subnet
    - Test system directly connected to company network
    - Test system with Internet connections (e.g. remote monitoring in the field)



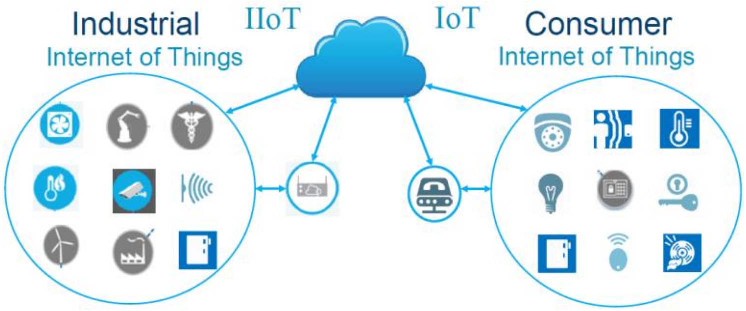
Examples for test system configurations

LXI Security - Ecosystem

- Areas:
  - IoT (Consumer Internet of Things)
  - IIoT (Industrial Internet of Things)
  - IT (Information Technology)

- There are commonalities which LXI instruments share with IoT, IIoT, IT

- Observed commonalities:
  - Device security
  - Data security
  - Network security



- Key principles: C.I.A.
  - Confidentiality
  - Integrity
  - Authenticity

Relevant Industrial Security Standards

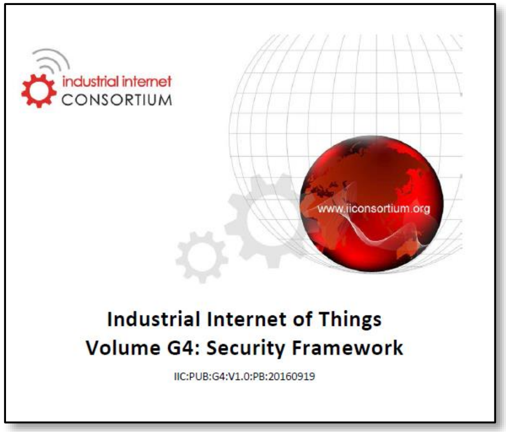
- Aerospace & Defense:
  NIST: Framework for Improving Critical Infrastructure Cybersecurity
  NIST 800 SP Series

- 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



industrial internet CONSORTIUM

www.iiconsortium.org

Industrial Internet of Things
Volume G4: Security Framework

IIC:PUB:G4:V1.0:PB:20160919

Lessons Learned

Importance of Network Security

- Primary goals for secure communications within industrial networks (and networked ATE systems) are:
  - ***Confidentiality:***
    Data transported in the network cannot be read by anyone but the intended recipient
  - ***Integrity:***
    Any message received is confirmed to be exactly the message that was sent, w/o additions, deletions or modifications of the content
  - ***Authenticity:***
    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

LXI Communication Channels

Currently LXI implements the following communication channels

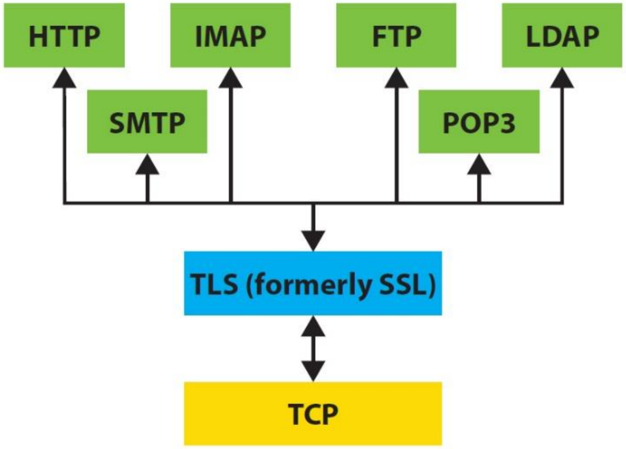
- Remote Control
  - SCPI based
  - TCP/IP: Socket / VXI-11 / HiSLIP
- Web Browser Interface
  - HTTP
- Ping, mDNS

Encryption is required to ensure secure communication between test computers and LXI instruments

- Transport Layer Security (TLS) encryption for data
- HTTPS (HTTP + TLS) for instrument web pages

TLS – Transport Layer Security

- **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.



HTTP + SSL/TLS + TCP = HTTPS

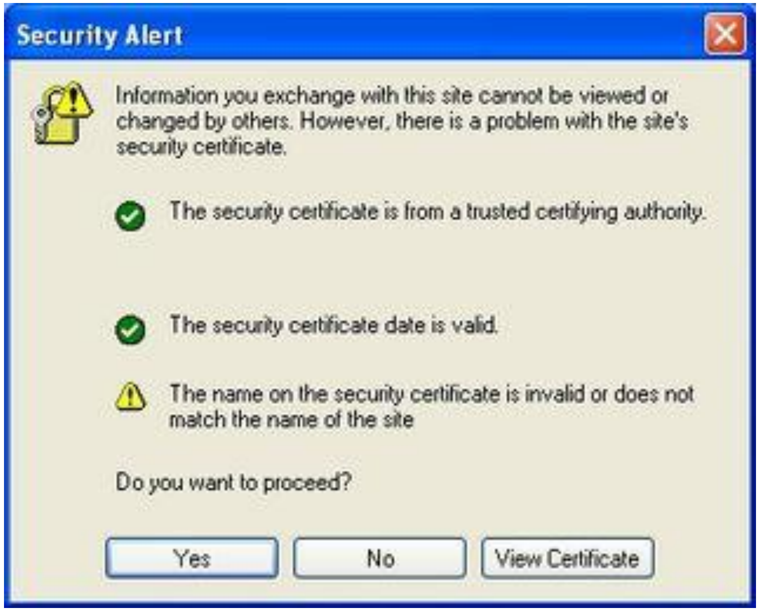
PKI – Public Key Infrastructure

- TLS uses PKI to authenticate communication channels and encrypt data
- In the **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.
- 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

Digital certificates:

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



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

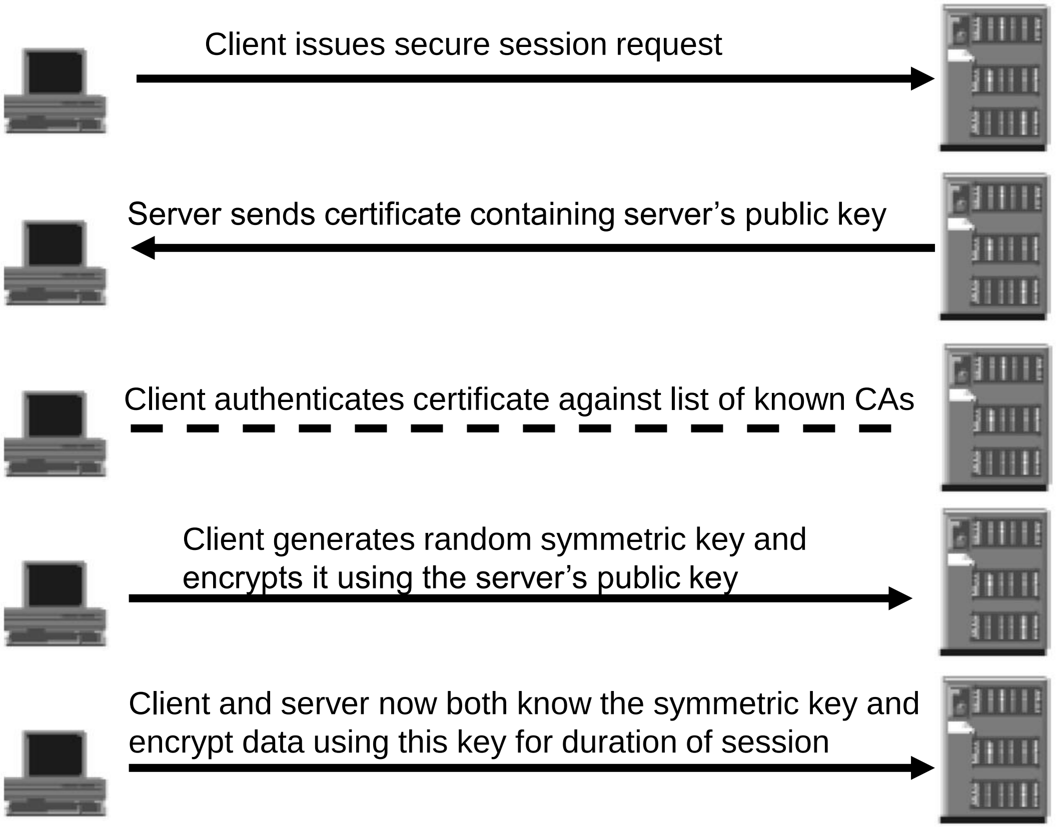
Certificate Authorities

GlobalSign®   digicert®   Symantec.

Certification Authorities (CAs):

- A trusted entity that generates and validates digital certificates to users, computers, applications, and services. It adds its own signature to the public key of the client. This 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.
- The LXI consortium has a working agreement with GlobalSign

TLS – Secure Communication


Client issues secure session request
Server sends certificate containing server’s public key
Client authenticates certificate against list of known CAs
Client generates random symmetric key and encrypts it using the server’s public key
Client and server now both know the symmetric key and encrypt data using this key for duration of session

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).

IEEE 802.1AR – LXI Adoption

- IEEE 802.1AR provides cryptographically bound, unique identifiers for devices (DevIDs), which are composed of a secure device identifier secret and a secure device identifier credential.
- DevIDs can be controlled by the vendor of the LXI device during the manufacturing process or by the end-user via a provisioning server.
- The vendor certificate is also known as the “birth certificate” - used to identify the LXI device (serial #, model, vendor). This is typically the first certificate on the LXI device and generated during manufacturing.
- End user IDs can incorporate, and fully protect, additional information like hostname and IP address of the LXI device for the DNS entries.
- Vendor certs are based on private root (“LXI Root CA”), End-User certs are based on public root (Public CA).

Two Certificates for LXI Devices

- Certs used for Remote Control (SCPI):
  - Vendor certificates with identity attributes such as:
    Serial Number, Product Family, LXI Vendor, *LXIDeviceDomain*
  - Standardized by LXI Consortium
  - Root of Trust: Root CA - LXI Device Vendor - Instrument
  - Deployment: Installation by LXI vendor (factory)
  - "Infinite" lifetime
- Certs for Web Browser Interface:
  - X.509 certificate derived from the DevID of the LXI device
  - Problem: IP address of the LXI device may change
  - Solution: Update the DNS entries (IP address) via provisioning server

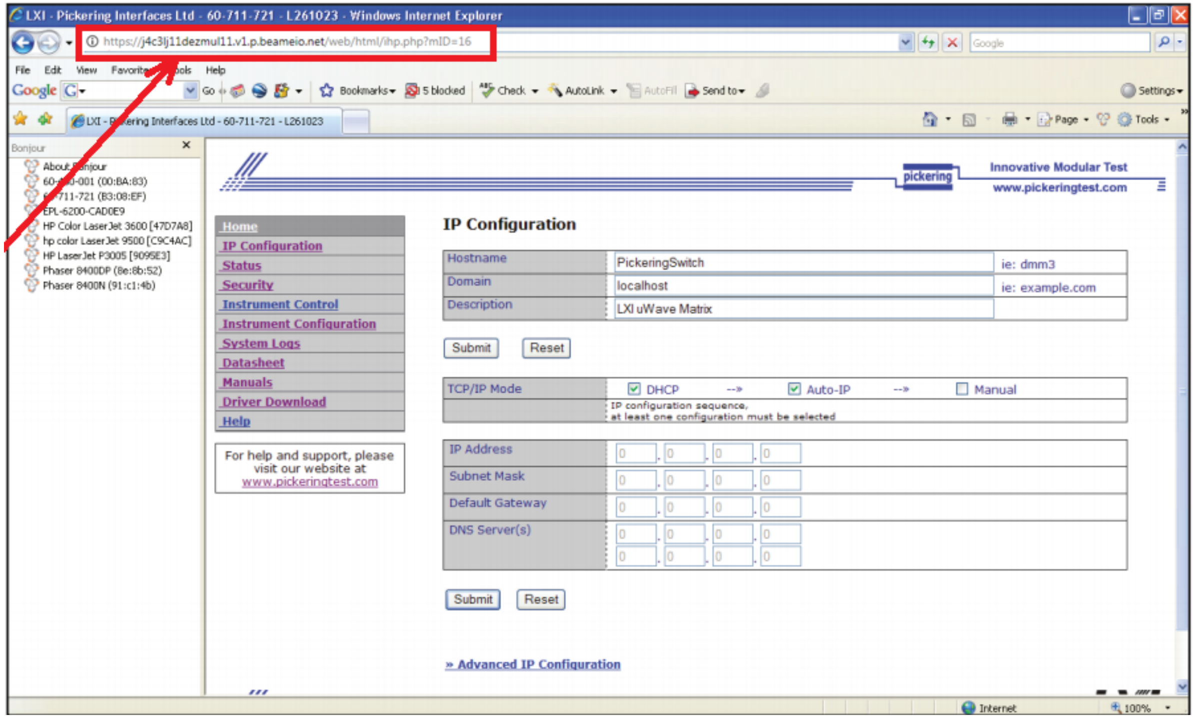
LXI Security WG Proposals

- Remote Control (SCPI):
  - Private trust model based on IDevIDs (LXI certs)
  - HiSLIP 2.0 which supports secure communication with TLS
  - Allows identification, authorization and encryption

- Web Browser Interface
  - Public trust model based on LDevIDs (X.509 certs)
  - Whenever the LXI device needs a LDevID for secure web server access (either nor present as in the initial state or the current LDevID is expired or revoked) it gets a new LDevID from the provisioning server
  - Whenever the LXI device gets a new IP address it has to assign and re-configure the host name (FQDN) to the new IP address and update the DNS entries via the provisioning server
  - Allows secure web server access

Secure Web Browser Connection

- LXI Vendor:
  IDevID (LXI Cert) installed on the LXI device
- Customer/User:
  Proxy settings for company network ⇨ Internet access
- Multi-step process between LXI device, test computer and provisioning server



LXI - Pickering Interfaces Ltd - 60-711-721 - L261023 - Windows Internet Explorer

https://j4c3lj11dezmul11.v1.p.beameio.net/web/html/ihp.php?mID=16

For help and support, please visit our website at www.pickeringtest.com

IP Configuration

Hostname	PickeringSwitch	ie: dmm3
Domain	localhost	ie: example.com
Description	LXI uWave Matrix	

Submit Reset

TCP/IP Mode	☑ DHCP --» ☑ Auto-IP --» □ Manual
	IP configuration sequence, at least one configuration must be selected

IP Address	0 . 0 . 0 . 0
Subnet Mask	0 . 0 . 0 . 0
Default Gateway	0 . 0 . 0 . 0
DNS Server(s)	0 . 0 . 0 . 0 0 . 0 . 0 . 0

Submit Reset

» Advanced IP Configuration

Local Network w/o Internet Access

Certificates issued by company internal CA (private root):

- Certificate is issued by customer PKI
- Install the certificate on the LXI device(s):
  Certificate (plus private key) is uploaded to the LXI device (REST, SCEP (Simple Certificate Enrollment Protocol) or CMP (Certificate Management Protocol) and user authentication/authorization)
- Install the root CA certificate on client systems (web browser(s) of the test computer)

Self-signed certificates:

- LXI Device creates self-signed certificate on demand
- Download certificate from device and install it manually in web browser(s) of the test computer

Thank you!

We are soliciting feedback and proposals to make sure the LXI Security WG covers all requirements

Further information on the security investigations can be found on the LXI Consortium’s website at: http://lxistandard.org/Resources/SecurityWorkingGroup.aspx

Questions may be directed to the following email address: **LXI Security WG**