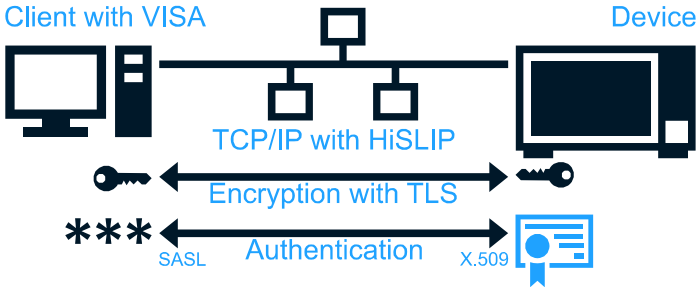
HiSLIP 2.0
Paving the way towards secure VISA connections

Fabian Güttge, Rohde & Schwarz

As the overall awareness for security has risen, the LXI Consortium has picked up this topic and is working on an LXI Security Extended Feature.[1] The intent being a general security concept for Test & Measurement devices in a network,[2] it makes sense to broaden the view beyond the scope of LXI focusing on https to connections for remote control. Hence, the IVI Foundation decided to make the HiSLIP protocol ready for security. This article provides a summary of the status of the IVI HiSLIP 2.0 working group discussions.

The HiSLIP protocol[3,4] is well suited for remote control of devices. It is fast, reliable and supports useful features like service requests and locking. However, it lacks security features, which are required in sensitive environments: connections are unencrypted and there is no client or device authentication. The goal of HiSLIP 2.0 is to extend the HiSLIP protocol by adding security features, such that secure transport does not rely on virtual private networks (VPNs).



At the core of HiSLIP 2.0 is the ability to encrypt connections with the Transport Layer Security (TLS) protocol. This protocol is commonly used for encrypting IP connections for example in the https protocol. Encryption secures the connection such that an attacker is not able to read the contents of the HiSLIP communication. This protects sensitive measurement data or device settings from eavesdroppers. Furthermore, TLS ensures that HiSLIP 2.0 connections are reliable: an attacker is not able to modify the contents of the HiSLIP communication.

Encryption is only one security feature of HiSLIP 2.0 - another one being authentication. If a connection is encrypted the device is required to authenticate itself at the client. This allows the client to verify that he is communicating with the desired device and not with an imposter. Each HiSLIP 2.0 compatible device has to be able to identify itself with an X.509 certificate. This certificate needs to be part of a chain of trust. LXI devices supporting the Security Extended Feature get equipped with an X.509 certificate, which is signed by a trustworthy LXI root certificate. The device certificate is checked when establishing the TLS connection. Furthermore, the certificate contains information about the device's serial number, model name and manufacturer. Evaluating this information the client can be certain to communicate with the desired device.

When the TLS connection is established, it is checked that the device certificate is issued by a trusted certificate authority (CA). TLS also supports mutual authentication – in this case, the client checks the device certificate and the device checks the client certificate. This is useful for device-to-device

[1] LXI Newsletter April 2018 Issue: LXI Security
[2] LXI Security Working Group
[3] LXI HiSLIP Extended Function v1_02
[4] R&S Application Note: Fast Remote Instrument Control with HiSLIP

communication, when both communication partners have a certificate. However, rolling out certificates to all clients is in general not feasible.

Hence, HiSLIP 2.0 provides various means of user authentication. Building on the simple authentication and security layer (SASL) framework, HiSLIP 2.0 supports for example username and password login, Kerberos or anonymous access. Supported authentication mechanisms are selected and implemented by the device manufacturer and might be configured on the device.

For back- and forward compatibility, a device can be configured such that encryption is not mandatory. In this case, authentication is not supported, as it is vulnerable to man-in-the-middle attacks. If encryption is not mandatory a client may switch encryption on and off at will. This is useful if the client wishes to configure sensitive device settings – something that needs to be done over a secure connection. However, if the measured data is not sensitive it might make sense to switch off encryption when receiving large amount of data from feeble devices for performance reasons.

For the client, the HiSLIP protocol is implemented by the VISA (Virtual instrument software architecture).[5] HiSLIP 2.0 requires some VISA extensions, while ensuring that existing applications using a VISA are not broken. New VISA attributes allow the client to read the attributes of the device certificate. A credential management system, relying on mechanisms the operating system provides, allows the client to securely store credentials for the devices.

As drafting the new HiSLIP 2.0 specification and modifying the VISA specification accordingly is work in progress, all statements of this article are preliminary and might be subject to change. We at the IVI Foundation are confident that the new version of the HiSLIP protocol will greatly enhance device security.

[5] VISA specification