Intrusion Prevention for Sensor Networks, M2M & the Internet of Things (IoT)

William J. Miller
ISO/IEC/IEEE P21451-1-4
Working Group Chairman

This paper discusses the first joint ISO/IEC/IEEE P21451-1-4 XMPP Interface Standard and its built-in capabilities against cyber-attack. The standard is a secure data transformation approach, providing scalable intrusion prevention for Sensor Networks, Machine-2-Machine (M2M) and the Internet of Things (IoT).

P21451-1-4 is the first joint standard effort among ISO, IEC, and IEEE, specifically for Sensors Networks, M2M and IoT. The standard offers a number of attributes, including packet transition, global unique identification, packet inspection and policy control, and encryption. It offers a defense-in-depth approach with assured interoperability, provides high scalability, and built-in security, which is technology agnostic and protocol independent. This standard provides capabilities for protection of cyber-physical assets.

Today, there is an increasing interest in the Sensors Networks, M2M and IoT areas to utilize smart devices, including smart phones, tablets, and media players with cellular or Wi-Fi connection. These devices are highly susceptible to security vulnerabilities due to the wider variance and lack of a standard for the build programs used for mobile apps.

It has been a challenge for the traditional security approaches to provide proactive cyber-attack prevention. Traditionally, anti-virus software is installed to identify the virus signature. This reactionary approach is not practical for protection of sensor networks. There are now over 80,000 new viruses each year. Updates to the operating system and differences in web browsers increase the security risks due to the built-in vulnerability with operating system and web browsers.

P21451-1-4 offers intrusion prevention to address the issues. The P21451-1-4 framework is independent of the IP address since it is not used for identification of the endpoint. It defines a Service Broker to provide data sharing with other endpoints. P21451-1-4 uses a Universal Unique Identifier (UUID). P21451-1-4 is the first to utilize ISO 29161 to provide a UUID as a global unique identifier for M2M and the Internet of Things.

The P21451-1-4 standard utilizes eXtensible Messaging and Presence Protocol (XMPP). It supports low-level packet filtering and inspection, including policy enforcement at a packet level. The packet transformation includes inspection and filtering of the function requested as part of an operation can be validated. It represents a very effective means of intrusion prevention. Firewalls can be used to lock down certain port numbers and establish rules to prevent certain protocols; however, it does not provide low-level packet filtering.

In addition to intrusion prevention, which is an inherent capability of XMPP, P21451-1-4 also provides Transport Layer Security (TLS). Data is encrypted using TLS or compressed with Efficient XML Interchange (EXI). P21451-1-4 defines External Services for the XMPP Server as a Service Broker and metadata requests and responses, which are used to activate the transformation of the XMPP messages. It also defines an external service for use of an Identity Provider (IdP) for single-sign-on. The IdP mechanism facilitates the ability for devices to be mobile. All devices must be registered with the broker and authenticated with an IdP to share information with each other. .

The packet transversion, i.e. packets in transition, which is defined in P21451-1-4, is depicted in Figure 1. Packet Transversion. It denotes a change from a legacy protocol to XMPP. Its technology agnostic and protocol independence ensures interoperability for legacy protocols. While in the form of XML, the data can be compressed and sent in a metadata format, and shared with other users, devices, or applications. The web server can provide REST using XMPP over BOSH (Bidirectional-streams over Synchronous HTTP) to communicate with mobile devices, such as Android or IOS. The XML data can be restored to a binary stream at an endpoint. The originating data that uses Port 80 can transport over Port 5222 and Port 5223. P21451-1-4 also provides packet inspection and policy control. While in transition, the packets can be inspected and the policy can be applied to validate the functions.

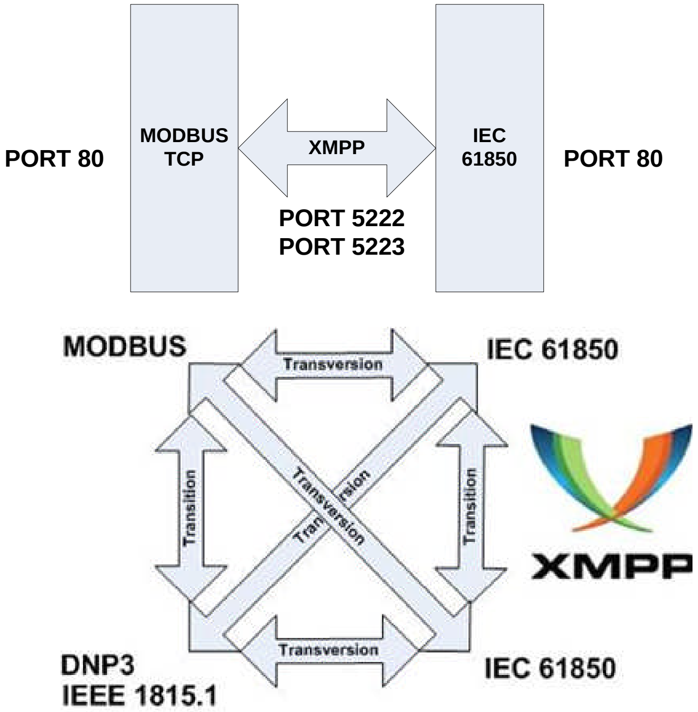

Figure 1. Packet Transversion

ISO/IEC/IEEE P21451-1-4 is the enabler for Sensor Networks, M2M and Internet of Things. It can be applied to different industries, such as the shipping and transportation, power and energy, and healthcare industry. For the transportation industry, there is greater interest to use RFID, GPS, and on-board sensors for shipment of pallets, cargo containers, truck, ships, and other vehicles. The need extends to identification of the items from anywhere in the world, and the ability to locate it by its geo-location.

Providing secure capability is a challenge for a traditional approach, such as Virtual Private Network (VPN), for large-scale heterogeneous sensor networks. P21451-1-4 offers scalable capabilities with cyber protection built-in, allowing even embedded devices to provide alerts or sensor feed viewable in XML from any web browser or mobile devices. It provides interoperability for legacy protocols. It is technology agnostic and protocol independent as well as firewall friendly.

The standard defines External Services for the XMPP Server as a Service Broker, providing a Service Oriented Architecture (SOA) used in cloud computing today. Metadata definition, used as part of a Service Activator, is used to establish the characteristics of the data flow. An attribute is available to notify the endpoint to receive the data from an adapter or send the XML traffic to the endpoint.

The P21451-1-4 metadata secure approach can be applied to Big Data applications, which currently does not use a metadata approach. Big Data is often confidential or classified, and its large data set is not easily mobilized. There are enterprise architectures under development to provide secure connection, however, they do not assure interoperability and change control. Specifically, these architectures do not provide intrusion prevention built-in at the endpoints. These capabilities are in common use today but have not been used to provide the intrusion protection. The P21451-1-4 standard can provide such a framework to protect cyber-physical systems against cyber-attack.

There are increasing cyber attacks targeting critical systems, such as power and energy, shipping and transportation industry. Department of Homeland Security stated that 40 percent of the intentional cyber attacks targeted energy systems last year.

Intrusion prevention is an important characteristic of the P21451-1-4 standard. In addition to being the first joint ISO/IEC/IEEE standard, its inherent security capability against cyber attacks offers scalable, proactive approach. It reduces cost and system complexity. On the other hand, the reactive approach of the traditional malware-detection software requires frequent virus-signature updates, and the VPN approach presents scalability concerns and increases complexity in the implementation for large-scale systems.

A cyber secure approach based on joint standards is critical to the success of the industrial internet evolution of Sensor Networks, M2M and IoT. P21451-1-4 is the first joint effort among ISO, IEC and IEEE with built-in packet transversion, providing effective intrusion prevention and protection from malicious attacks against cyber-physical system.