Protocol Transformation defense against cyber-attack

By William J. Miller, President, MaCT USA
IEEE P1451.1.4, Chairman
ISA100 CNMIG, Chairman

The need for defense against cyber-attack has never been higher. Firewalls have served as an initial barrier but penetration of viruses by the thousands continues to grow. The protection of our most critical assets including the Smart Grid represents a huge exposure that has yet to be resolved. To unleash innovation, which will rely upon communications, security has become the most critical issue. In recent work to develop transports for various protocols, we made use of eXtensible Markup and Presence Protocol (XMPP). This protocol is generally known for its use for instant messaging services on the Internet including Skype, GoogleTalk, etc. XMPP is an extensible protocol that facilitates packet transformation. This is commonly used in the financial industry and now is finding its way for use with large-scale heterogeneous sensor networks.

This paper discusses how XMPP can offer packet inspection at an endpoint prior to transformation to another protocol. This allows the structure of the packets to be evaluated and provide assurance that the packets conform to a standard. There are variances in standard protocols that represent a key problem for interoperability, requiring the user to purchase products from a particular vendor without regard that the product may evolve or need to be changed, and that a product of the same standard can be used.

In the transformation process for example, when using MODBUS TCP, the packets' atomic structure is changed into XML. This can then be used directly within web pages or sent to Android or Apple devices. The fact that the packets are viewable the commands can also be evaluated. This is an opportunity to determine if packets are authorized to make such a change or to view the information. This packet level inspection is particularly important in an industrial plant for example, where we may not want such command to be able to do certain things. This is generally not done today. Firewalls may block certain port number or apply policy types of TCP or UDP traffic. This type of packet inspection has been referred to as deep packet inspection. There have been very few products on the market that can do this effectively and not at the scale needed to meet the requirements of today's networks.

This has promoted a change in thinking that an extensible protocol was needed and this is where XMPP was found to be a natural candidate. Today, XMPP is part of a new standard known as IEEE P1451.1.4 that is also known as ISO/IEC/IEEE 21451-1-4 Smart Transducers for sensors, actuators, and devices. This standard defines XMPP along with other common network services such as SOAP and HTTP. XMPP offers Transport layer Security (TLS) for encryption of all data traffic but more significantly, that during the protocol transport, the transformation process would protect the endpoint device from cyber attack. This is because XMPP uses TCP Port numbers 5222 and 5223 and not Port 80. (If) Legacy protocols, such is MODBUS TCP or DNP3, which have no security, can be transported via XMPP. Then the packet flow would be limited to only XMPP traffic at the endpoint.

The protocol transformation process can handle multiple devices and different types of protocol**s,** which also offers a way to harmonize variants of protocols and assure interoperability between devices and applications. It is proposed that intermediate devices would provide firewall isolation and VPN capabilities. The network also needs to provide a means to transport packets over different types of backhaul, which include wired and wireless connections. The problem space is really the same. There is a need for extensibility, which is technology agnostic and protocol independent.

XMPP offers key capabilities that are firewall friendly and security is built-in. This is important since VPNs add complexity and cost for large-scale applications. They also do not provide a secure channel that is end-to-end and may not operate over certain types of technologies. The key element is to separate the network access from the machine-to-machine control. This has been considered the same and has resulted in relatively small-scale deployments not millions that are needed. XMPP offers capabilities that provide assured interoperability, scalability, and security. The transformation of packets while in the packet flow offers the ability to inspect the packets and to prevent penetration of unauthorized packets into a region of a network and can substantially defend network assets.