This comment is directed to the goal of identifying existing standards applicable to the security of critical infrastructure. It also seeks to encourage support for the security features identified in those standards.

Background

Distributed Network Protocol (DNP3), now ratified as IEEE Standard 1815, is a SCADA protocol that has been deployed in power system applications since the early 1990's. DNP3 is currently in use in approximately three-quarters of North American electrical utilities (Source: Newton-Evans Research [1]). It is also adopted by an increasing number of water and wastewater utilities and is used in oil & gas and other SCADA applications. IEEE 1815 has been accepted into the NIST catalog of Smart Grid standards.

DNP3 was originally developed as a conventional SCADA messaging protocol which included features to ensure high integrity of data reporting and command execution through the appropriate management of errors caused by random communication channel interference and equipment faults. It was designed to operate over utilities' private isolated serial and (since 1998) Ethernet communication networks.

In recognition of the increasing interconnection of SCADA and other networks, cyber-security message authentication features were initially specified for DNP3 in 2007 with subsequent revisions providing additional functionality. This feature set is known as "DNP3 Secure Authentication" (DNP3-SA). DNP3-SA defines a set of application-layer features that allow for the authentication of specific "critical" messages (e.g.: control commands) to verify that the messages originates from a known, authorized system or user and to verify that the message has not been tampered with or replayed. A critical design element of DNP3-SA is that it allows integration of systems where some devices support the feature and some do not, and users could choose to authenticate all messages or only specific "critical" commands. In this way it minimises impact on systems that have a mixture of equipment of varying capability and vintage.

Version 2 of DNP3-SA (SAv2) was specified in IEEE 1815-2010 and the latest update, SAv5, is specified in the current revision of IEEE 1815-2012. The most significant technical difference between these versions is that SAv2 relied on pre-shared symmetric keys installed in all devices while SAv5 supports that method of key deployment and also permits remote in-band update of the keys through either symmetric or asymmetric (PKI) methods.

SAv2 has already been deployed in a number of utilities (mostly in the water industry). The first devices supporting SAv5 became available early in 2013.

Commentary

Attention is drawn to the widespread use of DNP3 for SCADA applications in critical infrastructure management and to the (relatively recent) addition of cyber-security authentication features into the protocol. Many users remain unaware of these features built into the protocol and may instead be seeking to secure the SCADA interface only through the use of other

methods such as link encryptors, VPN routers, etc. (Note: Other methods may also be applied in addition to using DNP3-SA, when appropriate).

Users are requested to consider if the authentication features of DNP3-SA conform to the needs identified in their security policy, and, if so, to add a requirement for support of DNP3-SA to their specifications and RFQs.

SCADA equipment vendors whose products support DNP3 are requested to familiarize themselves with DNP3-SA and be prepared to address the requests from users to supply this feature.

Till now, there has been something of a chicken-and-egg situation where vendors are not supplying security features in part because users are not requesting them and users are not requesting security features that vendors are not currently offering. It appears that end users need education or encouragement to identify and specify the features that they want in order to send a strong message to the marketplace that there is a demand for products that support security features. It appears that vendors only respond to this demand when it becomes apparent that there is a willingness of the users to only install equipment that supports those features. Once a critical mass of users request the features and a critical mas of vendors offer them, it seems that the majority of users and vendors then follow suite. The issue to overcome is the development of this initial demand.

Reference

[1] The World Market for Substation Automation and Integration Programs in Electric Utilities: 2011-2013, Volume 1: North American Market, Newton-Evans Research Company, December 2010

--

Andrew West
SCADA Communication Consultant
Chair, DNP Technical Committee
Email: chair_tech@dnp.org