Remarks for FERC Technical Conference on Communications Security

Andrew Wright

April 29 2014

The version 5 CIP standards contain no requirements for encryption or authentication of critical control signals such as SCADA commands, whether those signals are carried over IP connections, serial links, or even over the public Internet.

Most major Internet businesses, such as Google mail, Yahoo mail, Facebook, Twitter, Skype, etc. are moving to adopt encryption for all communications between users and services over the public Internet. These businesses are even moving to encrypt internal traffic between their data centers that is exchanged over private networks.

While their motivations are different, the threats driving these businesses to change apply equally to the networks that carry control signals for the power grid. An increasingly sophisticated set of hardware and software exploits is available to potential attackers. Exploits are available for both IP and serial communications. Physical access to communications paths, whether fiber, microwave, or other, is not difficult to achieve due to the geographically distributed nature of these networks, hence their private nature cannot be relied on to provide security.

Strong cryptography is the only viable means of ensuring the authenticity and integrity of control communications across the diverse and geographically distributed control systems of the power grid. Protocols, applications, and products are widely available for encrypting IP links. Most modern processors contain hardware support for cryptography, enabling the implementation of cryptographic operations with minimal impact on communications.

However, a substantial portion of control center to substation communications still uses slow serial links. The challenge to encrypting serial links is not in computational capacity, but in additional overhead added to the communications line. Between 2004 and 2008, American Gas Association Working Group 12 developed a cryptographic protocol specifically for the purpose of assuring the integrity of serial SCADA communications. I was a key technical contributor to this protocol. The protocol is intended to provide retrofit protection via bump-in-the-wire link encryptors. The protocol was implemented by about a half dozen manufacturers and prototypes tested for interoperability against a reference implementation written by me. Subsequently the protocol was transitioned to an IEEE standard, and is now known as IEEE 1711, Cryptographic Protocol for Cyber Security of Substation Serial Links. Unfortunately, this protocol saw little market uptake, and most of the implementations that were built appear dormant.

Similar to IEEE 1711, DNP3 Secure provides cryptographic authentication for the DNP3 SCADA protocol, which is widely used for substation communications in the US. DNP3 Secure can provide authentication for both IP and serial DNP3 links.

Given the availability of IEEE 1711 and DNP3 Secure, FERC could consider mandating their implementation across the serial links of the power grid. An upcoming mandate would drive development of a market for products. But the specialized nature of these devices would still make them expensive. A full rollout across the grid would leave utilities even more locked in to outdated serial technology.

There is a better way.

The current CIP standards include a variety of exclusions to compliance requirements for cyber assets and sites that are connected solely by non-routable protocols, e.g. serial links. These exclusions do not exempt serial links from encryption, since control links of any kind do not require encryption. However, these "non-routable protocol exclusions" are in part responsible for utilities retaining serial links. In some cases, utilities have even removed IP links in order to simplify their CIP compliance efforts. CIP version 5 made some changes in this area, but a careful study of version 5 will show that the majority of control center to substation non-routable communications will still enjoy exclusion from many compliance requirements. Thus even as version 5 is adopted, most utilities will likely retain their serial equipment.

Eliminating the "non-routable protocol exclusions" would not directly force deployment of encryption for control traffic. But by removing this incentive to stick with serial communications, the ever decreasing costs and increasing capabilities of IP-based networking equipment would likely be sufficient to motivate utilities to modernize their communications networks. With encryption mechanisms increasingly available in networking and substation equipment, security protections such as IPSEC and SSL could be implemented at minimal additional cost as this modernization proceeds.

Switching to IP-based high-speed communications will have other benefits. These networks will enable access to high resolution "stranded data" that is generated by modern substation equipment but too large to be retrieved over slow serial inks. Higher speed connections will also better support deployment of synchrophasor measurement units, for both grid measurement and eventually control. IP-based communications will support many other applications, such as electronic locks and video surveillance, and new applications that have yet to be invented. Finally, IP-based dynamic routing that can reroute substation communications across multiple paths could provide more reliable communications during accidental outages and some defense against availability attacks.

Compliance requirements for encrypting control traffic may also be necessary, but removing compliance incentives for utilities to retain serial links will go a long way towards encouraging broader adoption of secure communications.