Why Energy and SCADA Meters for Utility, Industrial and Commercial Applications Need Cyber Secure Encryption

Over the past few decades, cyber security has become a serious concern of banks and large commercial corporations. Many of these corporations have seen large scale breaches that have affected millions of consumers worldwide. Some of these breaches have had long lasting negative effects on the customers and the core business models.

But what about the energy sector? There are considerable numbers of power and energy meters, protective relays, switches and controls in power plants and substations. These devices are used to report on power flow, protect electrical feeders and provide safety controls to apparatus. Many of these were designed years ago, and as such have only basic password protection that could be vulnerable to cyber-attacks causing outages, interrupting service, or even worse, inflicting permanent damage to the power distribution. In October of 2017, the U.S government issued a rare public warning that sophisticated hackers were targeting energy and industrial firms – the latest sign that cyber-attacks present an increasing threat to the power industry and other public infrastructure.

In the 2015 Global State of Information Security Survey, it was reported that power companies and utilities around the world saw a six fold increase in the number of detected cyber incidents over the previous year. That year, there were a total of 46 incidents reported in the energy sector, accounting for 16% of the incidents among all sectors in the US, alone. More recently, energy and electric utilities have suffered an increase in cyber-attacks according to a survey by Tripwire, a digital security firm. Over 75% percent of the 150 information technology personnel surveyed in the oil, natural gas and electricity sectors had experienced at least one successful cyber-attack within the previous 12 months. These attacks consisted of an attacker successfully infiltrating a firewall, anti-virus program or other protections at the utility. Almost half of those surveyed had seen an increase in attacks over the previous year, and more than 80% percent expected an attack that would harm physical infrastructure, that year.

“It’s tempting to believe that this increase in attacks is horizontal across industries, but the data shows that energy organizations are experiencing a disproportionately large increase when compared to other industries. At the same time, energy organizations face unique challenges in protecting industrial control systems and SCADA assets.”

Cyber-attackers are no longer motivated solely by monetary gain. Their primary motivation is cyber-warfare. Cyber-warfare is a computer or network based conflict involving attacks by one nation against another in an attempt to disrupt the activities of organizations. These attackers or hackers are becoming the 21st century soldiers. Infiltrating a power grid would allow them to disrupt a nation's economy, distract from a simultaneous military attack or create national trauma. Moreover, since power equipment often take long period of time to rebuild, this could have lasting effects on consumers concerning power reliability. Compromising safety controls in power distribution equipment could not only cause dangerous catastrophic failures, but may also leave the energy provider with few options to restore reliable energy flow.

Some hackers' maliciousness is intended for recognition and respect within the hacking community: the bigger the intrusion and disruption, the greater the recognition from their peers. With this increase in black hat hackers looking for personal gain and recognition, and growth in cyber-attacks on utilities, significantly greater measures need to be undertaken within the energy sector to better secure power grids worldwide. Utility and industrial companies fight cyber-attacks with firewalls, data loss prevention (DLP) systems and Intrusion Prevention and Detection systems (IPS/IDS), but what about the power and energy meters in your facility or in the field at utility substations?