Electro Industries/GaugeTech™
The Leader In Power Monitoring and Smart Grid Solutions™

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.[1]

[1] U.S. warns public about attacks on energy, industrial firms - https://www.reuters.com/article/us-usa-cyber-energy/u-s-warns-public-about-attacks-on-energy-industrial-firms-idUSKBN1CQ0IN

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. [2] 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."
>
> *Tim Erlin, director of IT security and risk strategy for Tripwire.* [3]

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.

---

[2] The Global State of Information Security Survey 2015 - https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0ahUKEwj_voH8kt3ZAhXvx1kKHcJ3CQAQFghTMAU&url=http%3A%2F%2Fmkting.csoonline.com%2Fpdf%2FGISS%25202015%2520results.pdf&usg=AOvVaw0QayVUshpbNkQDVqd_iIWK

[3] Tripwire 2016 Energy Survey: Attacks on the rise. https://europe.tripwire.com/company/research/tripwire-2016-energy-survey-attacks-on-the-rise/

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?

What can an attacker do if they gain control of a power meter?

1. By gaining access to a power meter and changing its configuration, an attacker has the ability to fool a SCADA master into thinking that energy flow is working, while then maliciously triggering operations on protective systems or disabling safety controls.
2. Changing the configuration of a power meter could also cause a circuit to look like it is out, when power is actually flowing. This could trigger false control schemes and automatic restoration attempts. These false conditions could have catastrophic effects on power system equipment, making quick restoration very difficult. Moreover, attacks like this would provide dangerous working conditions for utility line restoration and maintenance employees.
3. Results from these attacks could result in financial loss, and even the loss of human life - for example, if a hospital were to lose their main and backup power systems. These attacks could also result in sanctions or fines from governmental regulators.
4. Relying on only one source of communicating data, such as mere relay data or power meter data alone, invites undetected attacks, especially without cyber security integrated into the equipment. Power meters' and other power system sensing equipment's identification data should be confirmed as matching, before any control schemes are initiated.
5. Country espionage can occur through theft of the energy data of private facilities, such as military installations or data server farms, by determining what they may be producing or cooling.

How can you stop a cyber-attack?

1. Encrypted Configuration Power Meters – To protect against cyber-attacks, the substation equipment must utilize a cyber secured scheme for authenticating configuration requests. Cyber Secure power meters, such as the Electro Industries/GaugeTech Nexus® 1450 energy meter, provide 128 bit AES encryption on all configuration and control functions, significantly increasing the difficulty of a successful cyber-attack. 128-bit encryption refers to the length of the encryption or decryption key. It is considered secure because it would take massive computation to defeat through brute force attacks. For example, it would take 2^{128} different combinations to break the encryption key, which is out of reach for all but the most sophisticated computers. This means a power meter with a cyber-secure encrypted configuration cannot be accessed by brute force attacks, during anyone's lifetime. Moreover, the meters have a delay between password attempts, making the task infinitely more difficult.

2. Training on Social Engineering Attacks – Social Engineering hacking occurs when the one weakness in an organization that cannot be protected by technologies, is exploited:, human psychology. By utilizing social media, phone calls, emails, and human interaction, attackers will often trick workers into giving them access to sensitive information. Frequent training is required to educate workers to look out for these attempts to gain access to a company's network or hardware.

3. Digital Signatures for Firmware Verification – When firmware is uploaded to a power meter or any other technological device, it should be signed and verified. This means that the specific device leaves the factory with its own signature, and any subsequent firmware updates for the device must have the correct matching signature for the device to allow it to be uploaded.

4. Limitation of Access – Hardware and software security should offer role based access. This allows the administrator to limit access to what the user can view, edit, reset, download, etc., by setting up roles with those restrictions and assigning the user to the appropriate role.

5. Better Requirements for Passwords – It takes an attacker 4 minutes to hack into an account with a 4 character password. A password of 30 characters would take 4 nonillion years (that's 32 zeros). Better password requirements and increased frequency of password changing will greatly increase an organization's protection.[4]

As the rate of intrusions of utilities and industrials grows exponentially in the coming years, so does the need to secure power grids around the world by taking effective action before it is too late. Cyber security is often thought to be handled only by firewalls and IPS/IDS systems, but as technology grows in the utility and industrial sectors, the cyber threat to other devices including power meters, switches, and relays needs to be recognized and proactively prevented. EIG provides cyber secured configuration on most of its popular products to help utilities design substation that are safe and secure from malicious attempt to load harmful firmware or configure meters to provide false data.

[4] ELCOMSOFT Blog: How Long Does it Take to Crack Your Password? April, 2017 - https://blog.elcomsoft.com/2017/04/how-long-does-it-take-to-crack-your-password/