EFM and Cyber Security

Class # 8280.1

Orlando Camarillo

Applications Pre Sales Support

Schneider Electric Telemetry & Remote SCADA Solutions

6650 W Sam Houston PKY N Suite 420

Houston, TX 77041 USA

Summary

With a long list of potential hackers and many ways to penetrate inherently weak SCADA and EFM systems, the threat of cyber terrorism, espionage and illegal industrial intelligence gathering has gotten the attention of everyone from the Defense Department to the SCADA manager. Securing data communications from the well site/pipeline across telemetry systems and into the corporate server for SCADA or EFM processing requires some understanding of a hacker's mentality and a corporate directive from the highest levels within a company to push for updated policies not just basic IT networking but for SCADA oriented security policies that only SCADA professionals can help define. Tying these two things together is enterprise security awareness that all employees should be conscience of.

Sounding the Alarm

"We are now in a world in which countries are developing the capability to engage in the kind of attacks that can virtually paralyze a country." - Defense Secretary Leon Panetta , Oct 2012.

Some would say this statement is far-fetched, however with financial systems, power grids, pipeline operations, transportation systems and public utility services networked from the ground up into servers and workstations using standard TCP/IP and sometimes onto the Internet, Panetta's sounding of alarm is at the minimum a wakeup call that our cyber assets are in someone's cross hairs . Between the Department of Defense and the Department of Homeland Security ramping up intelligence, offering security documentation and training, they are seeing this as a type of warfare. One in which technical knowledge of programmable logic controllers, industrial firewalls, SCADA protocols and databases become the weapon. Much like the cold war, we can assume the U.S. is "pointing" worms and malware at countries and specific groups that are themselves doing the same thing. Some say Stuxnet is an example of this.

EFM Security

SCADA security has been much talked about, physically securing the remote site, encrypting messages, installing industrial firewalls, disabling guest accounts and isolating the network from the rest of the enterprise. There's been little talk of securing EFM since there is a lot of overlap with SCADA and internal networks are assumed secure. However EFM security needs to be discussed and acted on.

EFM stands for Electronic Flow Measurement; it's a common technique of calculating gas flow measurement at the wellhead or pipeline by measuring differential pressure, static pressure and temperature. These values are recorded and used to perform gas flow calculations using standardized formulas set by the American Gas Association. Gas quality data from a chromatograph can also be used in calculations, for example in determining BTUs. This data allows for availability of instantaneous flow, volume since a start of day time and hourly and daily volume information for the previous 35 days. Typical EFM systems will attempt to retrieve the EFM data from remote sites every few hours. Depending on the purpose of the flow computer, that data could be used for billing purposes if it's located at a custody transfer location.

Like other sensitive company financial information the amount of gas volume sold/purchased must be secured wherever it exists, at the wellsite, custody transfer location, polling engine or the financial database. Gas flow computers will usually be installed at a custody transfer location, how much volume was sold a monthly over a period of months/years is considered sensitive between the parties. Who could benefit from illegally obtaining this data? A competitor? Another party who buys or sells natural gas? The topic of industrial espionage and competitive intelligence come up however in the day of worldwide competition foreign entities do as well.

During the INGAA (Interstate Natural Gas Pipeline Companies) annual foundation meeting Nov 1-3, 2012; the discussion on cyber security brought up the fact that foreign entities are very much interested in obtaining confidential data from pipeline operators. Cyber security experts said foreign hackers from China, North Korea and Russia are constantly attempting to hack into U.S. natural gas company's networks to improve their global and economic positions by gaining inside information. Some of this information included merger and acquisitions, intellectual investment, trading information, infrastructure plans, pricing patterns, SCADA systems and industrial controls best practices and pipeline data. China is said to be developing its own shale gas program and it is behind the U.S. technology wise, they are looking for any edge to successfully compete and possibly even control the energy market.   (Pipeline and Gas Journal January 2013, Vol. 240 No. 1)

Potentially another set of hackers who are not so much interested leveraging proprietary data are trying to gain access to field equipment to cause disruption of utility services, cause harm to physical assets or personnel/general public. These could be 'wannabe' hackers wanting notoriety, attempting to push a political message, a hacking challenge or a concentrated effort on the part of country, that are aiming their hacking skills at U.S. companies. Data stored in EFM systems give them much needed information such as flow computer/RTU vendor, IP addresses, ports, site names, GPS coordinates and gas volume measurements.   Knowing which type of flow computer tells them what protocols are supported, IP addresses could possibly accessible via the public internet (public IP) if not once they hack into the SCADA network they can use the private IP, default ports are sometimes left at default, passwords into 3G modems as well. Some of this information isn't usually stored in a SCADA host which is typically watched more carefully by intrusion detection systems. Hacking into the SCADA systems network and into the field equipment with this information allows for a better directed attack, one that can maximize damage because they can target sites that move the largest volume of natural gas for example.

Follow the Data

Starting at the source of EFM data, is the site physically secured? If it has TCP/IP connections, can someone just plug in their computer and obtain IP address? If a technician can do it for local troubleshooting a hacker certainly can and once he/she does, how much of the network is available if this occurs? The SCADA host and EFM polling engine could be at risk from an external site with a direct

TCP/IP connection. Secure it physically if possible and verify that you cannot obtain an IP address on the network by plugging into the remote site.

Telemetry often runs on third party networks: 3G, Ethernet radio, microwave, dial up. If the method of transmitting messages to EFM field equipment and back not is not completely within ones physical control then one must not assume validity of the messages. Messages risk being snooped, stored, analyzed, replayed. Solutions exist, industrial firewall which permit stateful packet inspection, restrict communication between certain IP addresses, or types of messages between them or involve encrypting data so the message is meaningless while it's being transmitted.

EFM Polling Engines or any software that is able to poll for EFM data typically run on a Windows class server. Depending on the method of communication, it will have configured individual Flow Computer's communication settings such as IP/Port, phone number or serial communication settings, depending on how communication takes place and this data resides in a database. How secure is the server and the polling engines database? Are there any commonly used user names (Administrator), passwords; Windows shares for the database file set to 'Everyone'?, OPC connectivity to the polling engine using security?

EFM data files are exported from the EFM polling engine software. They are in a standard format that the EFM system can parse and are usually ASCII text files. They are created in a Windows folder where the EFM system expects them, often a shared folder on the server. The EFM system will process the files, update the EFM system database and store the files away for archiving. The EFM database should be secured and only have minimal security per user. The location where EFM files are stored for archiving should be secured as well. Most database administrators will backup the database on a schedule, where is the back up stored? How many copies exist? Are they all treated with upmost security in mind? To an IT department a share, a server, a database are equally important across the entire company, it's up to a cyber-security aware CIO or SCADA manager to step up and request this SCADA and EFM data be treated differently and that starts with updating security policies to include cyber-security in mind.

EFM data can have a long route before it ends up archived on a file server. One must analyze each critical point and secure it using best practices, latest technology and security policies written with SCADA, EFM and cyber security in mind.