Utilities Facing Many Challenges

Cyber Security Is One Area Where Help Is Available

Executive Summary

Utilities are in the crosshairs of many forces in the world today. Among these are environmental global warming concerns putting pressure on the ability to generate sufficient electricity to meet future demand. Another is the multiplicity of computer and communications systems that must be protected against threats from those who would do harm to electric, natural gas and water distribution systems.

A Wall Street Journal article[1] in April 2009 focused attention on the security issue by quoting various federal officials who claimed many utilities already had been breached – especially by spies from hostile countries – with bits of code left behind that could be activated in time of war or for other reasons to bring down major portions of the U.S. electric grid. However, utilities long have been aware of these issues, and many report 10,000 or more attempted network security breaches per month, and have done so for years, according to research from Sierra Energy Group (SEG), the research and analysis division of Energy Central.

at&t

Utilities In The Crosshairs

The U.S. utility is challenged as never before in history. The challenges are myriad: from generation capacity constraints to environmental global warming remediation demands, to economic conditions, to cyber and physical security concerns. The April 2009 Wall Street Journal story referenced earlier brought additional attention to a security issue utilities have been aware of, and attempted to mitigate for years.

Before the Wall Street Journal article brought the issue to widespread public attention utilities knew they were under attack. Utilities have quietly collaborated with the FBI, various national laboratories, vendors, the Department of Homeland Security, and others to mitigate these on-going attacks. What was different about the Wall Street Journal article was the claim by various government officials that some of these attacks have been successful and that cyber spies from hostile countries have been mapping the U.S. electrical grid, and leaving behind bits of sleeper code that could be activated and used to damage the grid or cause blackouts in the event of war.[2]

Attack Vectors

The widespread use of the Internet as a communications mechanism is a major driver for increased cyber attacks, but the problems go much deeper. Since the 1980s utilities increasingly have been using computing applications communicating over wireless networks, primarily SCADA (Supervisory Control and Data Acquisition) and DA (Distribution Automation)to communicate with and control many remote devices on electrical grids, and natural gas and water distribution systems. Many of the early SCADA and DA systems that are still in service today were built with early technologies that are relatively easy for sophisticated hackers with modern tools to breach and manipulate. Recent technology trends have emphasized the "networking" of all utility computers and control systems for efficiency and collaboration. With the recent surge in wireless smart meter implementations, there now are a large number of cyber pathways which present opportunities for attack.

Prior to the Sept. 11, 2001 terrorist attacks there was not a systematic security approach to address utility critical infrastructure protection in the United States. Each utility was essentially on its own, and security of computer systems and physical security at plants, substations and other facilities were the responsibility of individual utilities without any oversight or coordination. With more than 3,000 electric and natural gas utilities and approximately 15,000 water distribution utilities in the U.S, this presented significant opportunity for security risks.

Critical Infrastructure Protection

In 2008, the Federal Energy Regulatory Commission (FERC) approved eight new critical infrastructure protection (CIP) reliability standards designed to protect the nation's bulk power system against potential disruptions from cyber security breaches. These standards were developed by the North American Electric Reliability Corporation (NERC) and provide a cyber security framework for the identification and protection of Critical Cyber Assets.

The eight cybersecurity standards address the following:

- Critical Cyber Asset Identification
- Security Management Controls
- Personnel and Training
- Electronic Security Perimeters
- Physical Security of Critical Cyber Assets
- Systems Security Management
- Incident Reporting and Response Planning
- Recovery Plans for Critical Cyber Assets

NERC CIP is a framework to help address security of United States national utility systems, but there is still much work to do. For example, there have been cases where security updates have not been installed on assets, and unfortunately many "patches" are only issued after a hacker or cyber spy already has found and taken advantage of a security flaw. Multiply potential flaws by the number of utilities and again by the number of utility networks and the extent of the cyber-security challenges becomes clear.

Cyber security is the collective set of services, procedures, and practices aimed at securing utilities from cyber attacks. These capabilities assure the information, applications and services customers want and use are secure, accurate, reliable, and available wherever and whenever they are needed.

To secure wireless and cellular infrastructures network operators should incorporate mature defense mechanisms as well as security measures including the following.

Secure Connectivity and Encryption

In any communication system, it is essential to ensure that sensitive information reaches its intended recipient and that it cannot be intercepted or understood by an individual or device attempting to intercept it. This is especially true when the information is contractual data used for billing purposes. Strong authentication processes are also mandatory to prevent hackers from accessing sensitive data, uploading malicious software or turning meters on and off. Wireless communication systems should employ strong and mature encryption protocols such as Secure Sockets Layer (SSL) – which is already widely used to protect retail and web-based payment card transactions – or Internet Protocol Security (IPSec) encryption, which is already widely used to secure virtual private network (VPN) connections.

Jamming Detection

In some higher-risk environments, defensive systems are needed to thwart deliberate network attacks. Modern smart meters should be equipped with wireless technologies that quickly detect such attacks and take appropriate actions, such as triggering an alarm, sending an alert through another communications channel, recording the event for further investigation and so on.

Autonomous Operation

In the event that meters lose connectivity with the wireless communications network, the meter must be able to continue operating. Today's industrial-grade, cellular-enabled smart meters are intelligent devices that are capable of continuing to operate even if they lose connectivity with the wireless communications network.

Secure User Access Levels

Remote management tools are critical to utility deployments, as it's typical for energy management equipment to be located in remote areas. Remote management enables IT managers to monitor and configure their cellular enabled devices from anywhere with an internet connection. With this convenience comes the additional risk of another avenue for hacking into the energy infrastructure. It's vital that remote management software is equipped with multiple user access levels and adequate security measures to ensure that only authorized personnel have access to critical infrastructure.

Cyber security capabilities include understanding and identifying emerging threats in early phases of their development. Network operators are routinely exposed to a variety of exploits, malware, flooding attacks, protocol anomalies and other threats are generally visible and often abundant on the Internet long before they have any significant affect on enterprise security.

AT&T is uniquely positioned to understand and deal with cyber threat and utilize more specific security practices to enable early detection and mitigation of pending threats. These include:

- Operation of a global IP network offers additional security algorithms over non-IP based networks;An Internet data analysis platform that examines internet threats including botnets; network worms, DoS attacks, network exploits and other activity anomalies
- An analysis team that operates 24x7 to assess any significant activities on the Internet that could affect network services
- An algorithm research team that continually investigates and tests methods for automated detection of network threats
- AT&T Labs and Chief Security Office researchers, who participate in the security and networking research communities

AT&T's advanced network technology currently transports on average more than 17 Petabytes each business day of IP data traffic and the load is expected to double every 18 months for the foreseeable future. AT&T's network technologies give the company the capability to analyze traffic flows to detect malicious cyber-activities, and in many cases get very early indicators of attacks before they have the opportunity to become major events. For example, AT&T implemented the capability within its network to automatically detect and mitigate most Distributed Denial of Service Attacks within the AT&T network infrastructure before they affect service to AT&T customers. AT&T has grown from one domestic scrubbing complex to multiple locations across the United States, as well as having scrubbing nodes in Europe and Asia. This gives the AT&T the ability to filter attack traffic as close to the source of the threat as possible.

AT&T has made significant investments in the security of its mobility network. AT&T's Radio Access Network (RAN) complies with 3GPP airlink security standards. The RAN uses secure protocols in order to maintain and manage communication with the mobile station as well as specific procedures including power control and handover management. An important security mechanism that protects the radio link against eavesdropping is encryption. Encryption protects both user data and network control information and occurs between the cellular towers and the wireless device.

Following authentication and key agreement the network and end-user equipment uses a 128-bit key and strong encryption algorithms. Significant resources have also been invested in the AT&T core mobility and wide area network in order to comply with and exceed industry security standards.

Cyber Security Best Practices for Wireless Utility Networks

Wireless communications vendors and wireless network operators often collaborate to develop a comprehensive set of security measures to ensure each utility can implement the necessary safeguards to protect their data. Specifically AT&T and Sierra Wireless have been working together to provide strong and proven security technologies enabling utilities with a secure and flexible two-way communications infrastructure to connect and communicate in real time.

A variety of tools and best practices are being established to form a baseline of security measures. While working together on these initiatives to support the utility, there is differential between what the network operator and the vendor will provide the utility.

Software Patch Upgradability

Everyone agrees that the ability to upgrade firmware, software, and capabilities remotely is essential for any utility communications technology. Support for basic firmware upgrades, however, is not efficient enough for large-scale deployments. For example, if a utility has to replace the entire 1-Megabyte firmware file on millions of Smart Meters to perform a security upgrade, the cellular data costs quickly become enormous. With the ability to roll out software changes as patches, suppliers can upgrade only those parts of the firmware code that have changed, using a software package of just a few kilobytes. In general, software patches are often a tenth the size or smaller of upgrading the entire firmware package.

Embedded SIM

Today, the 'removable' plastic Subscriber Identity Module, or SIM cards, used in some cellular networks are designed for the mobile phone market and have a projected lifespan of just a few years and are readily accessible. When used in smart metering or other residential applications, the traditional SIM is susceptible to tampering by unauthorized individuals and security could be compromised. Embedding the SIM into the communication module which must meets industrial-grade specifications will provide an additional layer of security as well as extending the life of the SIM.

Robust and Comprehensive Development Platform

Communications module vendors are responsible for not only developing robust intelligent communication modules, just as important is the service delivery platform needed to support the life cycle management and diagnosis of these intelligent wireless devices. It is only a matter of time before the lack of standards for security and interoperability of wireless utility devices (i.e. smart meters) is resolved. As such, the ability to upgrade these devices with the latest security patch, firmware or application enhancement will become part of a utilities routine maintenance program.

To enable the intelligent and secure communications modules energy suppliers need, cellular modules should be programmable and allow utilities and their device manufacturers to add additional secure capabilities per their individual requirements. Network operators and cellular communications vendors should offer a mature and comprehensive development platform that encompasses all of the elements necessary to build customized and secure solutions. The platform should also allow manufacturers to take advantage of proven, mature and open technologies for every aspect of managing wireless communications without having to reinvent these capabilities from scratch.

Backup Communication Paths

The communications system should provide the capabilities and intelligence to employ alternative communications paths if the primary mechanism is unavailable. For example, if GPRS IP communication is offline for some reason, the meter should be able to communicate via Short Message Service (SMS), i.e., a text message.

Network Quality Analysis Capabilities

To simplify deployments and reduce installation costs, the communication module should be able to analyze wireless network quality and clearly communicate results to installers. For example, instead of technicians having to check multiple SIM cards on their cell phones to measure signal strength, as is commonly done today, the module could scan and assess the signal strength of the different networks available and convey this information to the technician. Even a simple tool such as this can make it much easier and quicker for installation technicians to determine proper meter placement, which cellular network is best for the location, when an external antenna is required and where it should be located, etc.

Given the dynamic environment that AT&T supports, the library of AT&T security standards is continually re-evaluated and modified as industry standards evolve and as circumstances require. In addition, AT&T and Sierra Wireless support the following best practices in advancing cyber security through the utility enterprise programs.

Confidentiality

To ensure confidentiality, information is accessible only to those authorized. AT&T has implemented a three-tiered Information Classification framework for categorizing information based on sensitivity of the content and specific legal requirements.

Physical Access Control Requirements

AT&T operates in a highly secured environment where physical access to staff office space, switching centers, global network and service management centers and other network facilities is strictly monitored and controlled.

Network Element Access Controls

Access is provided to AT&T technical support personnel only on an as-needed basis for individuals with responsibility for network element maintenance and support.

Network Perimeter Protection. AT&T external network connections are protected by firewalls that screen incoming and outgoing traffic based on source and destination address, protocol and port, in accordance with the security policy.

Intrusion Detection

AT&T employs a combination of internally developed and commercial tools to detect attempts by unauthorized persons to penetrate AT&T Global Network. AT&T does not monitor individual customer connections for intrusions, except when part of a managed security service.

Workstation Security Management

Workstation security policies protect AT&T and customer assets through a series of processes and technologies including verification of personnel workstation accesses, PC anti-virus protection, Operating System hardening and updates, full disk encryption where permitted by law to protect sensitive information on portable assets, along with a personal firewall intrinsic to remote access software implemented on workstations or portable PCs that remotely connect to the AT&T network.

Security Status Checking and Vulnerability Testing

AT&T conducts regular tests and evaluations to ensure that security controls are maintained and are functioning in accordance with policy. These initiatives include Security Status Checking and Vulnerability Testing, Security Incident Reporting and Management. AT&T uses a consistent, disciplined global process for the identification of security incidents and threats in a timely manner, to minimize the loss or compromise of information assets belonging to both AT&T and its customers and, to facilitate incident resolution.

Business Continuity and Disaster Recovery

AT&T Corporate Business Continuity Planning Services provides technical consultation and program management expertise to address the business continuity, disaster recovery and managed security needs of AT&T and its customers.

Security Products and Services

AT&T offers managed security products and services to its customers designed to assess and protect their vital network infrastructure, including managed services in the area of Intrusion Detection, Firewall Security, Endpoint Security, Token Authentication, Encryption Services, Security Email Gateway Services, Vulnerability Scanning and Consultative and Engineering Security Services.

Managed Services and Hosting

AT&T Managed Services take advantage of the security of AT&T's global Internet Protocol/Multi Protocol Label Switching (IP/MPLS) network. MPLS technology enables the creation of feature-rich network-based services coupled with AT&T's management expertise, tools and automation. AT&T's network-based managed services include Enhanced Virtual Private Network and Managed Internet Services.

Hosting Services

Hosting services provide utility computing services that offer tailored or turnkey solutions. The mix-and-match tailored solutions offer IT infrastructure, hardware and/or software components, reliable and secure data center facilities, value-added services (i.e., security, backup and restore, professional services, monitoring, portal/reporting, utility, and disaster recovery), server virtualization and, integrated client networking. A fully managed turnkey solution provides capacity on demand, managed firewall and network Intrusion Detection System (IDS) functionality, proactive alerting and patching dedicated virtual servers and, total isolation of each client's data in a data center environment.

AT&T and Sierra Wireless have implemented in-depth access control layers with multiple levels of firewalls that isolate data element functions from customer-facing interfaces. These security perimeters enable voice and data interfaces to its customers while helping to preserve the integrity of their core wireless resources. AT&T offers a Commercial Connectivity Services (CCS) solution which allows utilities to define transport network paths for data delivery. Adding to AT&T's CCS solution, Sierra Wireless provides device and service management features that allow utilities to monitor and identify suspicious connection activity. Suspicious device activity can be terminated by the utility or network operator (AT&T) to prevent further event escalations. This enables utilities to transport data from the Advanced Metering Infrastructure (AMI) to core IT infrastructure using authorized and encrypted capabilities which can be monitored in real time to thwart possible network attacks.

CCS and Sierra Wireless embedded modules make use of custom Access Point Names (APN's) that provide linkage from the wireless network to the utility's core IT infrastructure using either frame relay circuits or MPLS connectivity. These capabilities involve multiple levels of security, access controls and encryption that many electric, natural gas and water utilities will find beneficial.

AT&T and Sierra Wireless stand ready to work with utilities and bring their extensive experience and capabilities in cyber security to the many challenges ahead.

Notes

1. Electricity Grid in U.S. Penetrated by Spies by Siobhan Gorman, Wall Street Journal, April 8, 2009.

2. Ibid.

For more information contact an AT&T Representative or visit www.att.com/business.

SIERRA WIRELESS™

at&t

10/18/10 AB-1984