North American Electric Reliability Corporation (NERC) – Critical Infrastructure Protection (CIP)

Utilities Facing Many Challenges: Cyber Security is One Area Where Help is Available

Art Maria, Solutions Engineering and Architecture, AT&T
Warren Causey, Sierra Energy Group

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.

at&t

Summary continued

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.

In the aftermath of the 9/11 terrorist attacks on the U.S. the federal government moved to ensure utilities take all necessary measures to mitigate these attacks. Through the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corp. (NERC) the government issued a set of standards and requirements to ensure this mitigation. These standards and requirements are called NERC-CIP (CIP=Critical Infrastructure Protection). These mostly have been developed by private enterprise through vendors and other organizations.

Telecommunications carriers such as AT&T have addressed cyber security longer than most utilities because of the public nature of their communications systems. On the average business day, AT&T transports approximately 17 petabytes of data on its network. As a result, AT&T has gained significant knowledge and experience in regard to security architectures and encryption methodologies.

Utilities in the Crosshairs

The U.S. utility is challenged as never before in history. The challenges are myriad: from generation capacity constraints and declining capacity margins 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. SEG is aware that 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]

For several years it has been general knowledge that cyber spies have been disrupting utility systems and causing blackouts in Eastern Europe and around the globe; sometimes even demanding ransom money to cease the attacks. Electric, water and wastewater utilities in several countries have been affected according to SEG. Thus far, no similar attacks have been publicly acknowledged[3] in the U.S., but the Journal article pointed to the likelihood that such attacks may be inevitable and may have even already occurred.

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 computerized communications systems and networks, primarily SCADA (Supervisory Control and Data Acquisition) and DA (Distribution Automation), to communicate with and control many remote devices on electrical grids and both 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. As more networks are linked, the pathways for cyber spies become myriad and the means of protecting such networks becomes increasingly difficult to maintain. There now are a large number of cyber pathways at most utilities and a determined hacker – particularly one backed by a less-than-benign government – likely will find one.

Furthermore, prior to the September 11, 2001 terrorist attacks there really 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 even physical security at plants, substations and other facilities were the responsibility of individual utilities without any oversight. This created a significant risk in that there are more than 3,000 electric and natural gas utilities and approximately 15,000 water distribution utilities in the U.S. Before the terrorist attacks there were many different approaches to cyber and physical security.

Critical Infrastructure Protection

In 2008, FERC approved eight new 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 NERC and provide a cyber security framework for the identification and protection of Critical Cyber Assets.

The eight Cyber security 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

As mentioned NERC-CIP is a framework to help address security of our 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 you can begin to understand the cyber-security challenges around securing utility networks.

AT&T has invested significant resources in developing cyber security systems for its networks, and thus has significant expertise that utilities may find helpful in addressing their own security needs.

For AT&T cyber security is the collective set of services, procedures and practices. These capabilities assure the information, applications and services AT&T's customers want and use are secure, accurate, reliable and available wherever and whenever they are needed. Cyber security is a corporate priority and AT&T is investing significant resources in making its network and customers' information secure.

Cyber security capabilities include understanding and identifying emerging threats in early phases of their development. Network 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 established to understand and deal with cyber threat. These include:

- Operating as the largest provider of Internet services
- Operation of a global IP network footprint
- 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

The technology within AT&T's network is rapidly evolving to support new applications and services. In the course of 2009 alone, AT&T expects to invest $17-18 billion in expanding the capabilities of its network and infrastructure to meet the rapid global expansion of advanced information technology and services to enhance reliability and security. The size and scope of AT&T's global network, coupled with AT&T's industry-leading cyber-security capabilities, gives it a unique perspective into malicious cyber-activity.

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 Assets

AT&T is responsible for managing the security of a worldwide data network, which consists of multiple components converging into a common Multi-Protocol Label Switching (MPLS) network. In order to support these objectives, AT&T maintains a comprehensive global security organization comprised of over 700 security professionals. This organization is dedicated to the physical and logical security of the AT&T global network and its service offerings. It supports a broad range of functions from security policy management to customer-facing security solutions. The AT&T global security organization reviews and assesses AT&T's security control posture to keep pace with industry security developments and to satisfy regulatory and business requirements. AT&T actively participates in a number of global security organizations, and maintains a comprehensive set of security standards based in part on similar leading industry standards (COBIT, ISO/IEC 27001:2005, 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 supports the following 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 has implemented in-depth access control layers with multiple levels of firewalls that isolate core network element functions from customer-facing interfaces. These security perimeters enable AT&T to offer voice and data interfaces to its customers while helping to preserve the integrity of its core network resources. AT&T offers a Commercial Connectivity Services (CCS) solution which allows utilities to define transport network paths for data delivery. This enables utilities to transport data from the Advanced Metering Infrastructure (AMI) to core IT infrastructure using authorized and encrypted capabilities.

CCS implements custom Access Point Names (APNs) that provide linkage from the wireless network to the utility's core IT infrastructure using either frame relay circuits or MPLS connectivity. AT&T also offers Enterprise on Demand (EOD), which enables customers to selectively activate and deactivate devices (SIMs) on a real-time basis. These capabilities involve multiple levels of security, access controls and encryption that many electric, natural gas and water utilities will find beneficial.

In addition to CCS and EOD, AT&T offers a suite of Security and Business Continuity Services that will assess vulnerabilities, secure data and infrastructure, detect attacks, respond to suspicious activities and provide for non-stop operations.

AT&T stands ready to work with utilities and bring its extensive experience and capabilities in cyber security to the many challenges ahead.

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

2. Ibid

3. Ibid

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

10/26/09 AB-1760

at&t
Your world. Delivered.