Energy Utility Takes a New Approach to Ensure Smart Grid Security

THE CHALLENGE

- One of the challenges in testing and deploying mobile wireless networks and applications is the inherent limitation of traditional security assessment approaches. A large energy utility in the early stages of a major Smart Meter deployment needed to assess the security of its Advanced Meter Infrastructure (AMI). Per industry practice, it performed due diligence on the Smart Meter solution during its vendor selection process and carefully evaluated system security. The utility’s internal IT department had performed penetration and web application security testing on the AMI management system.

However, the field area network infrastructure, which consisted of dual-band wireless access points, relays, and embedded Smart Meter hardware, posed a set of new security challenges. It used a proprietary, wireless mesh networking technology, and there were no traditional means to access, monitor or interface with the network. It relied upon embedded systems technology that required specialized expertise to assess the security of the hardware and firmware. The utility engaged several outside security consultants to conduct independent assessments, but none provided sufficient depth or coverage to satisfy the utility’s need to understand the security posture of this large infrastructure investment. The utility then turned to Applied Communication Sciences because of its in-depth communications expertise; proven track record for pioneering security assessments of new technologies; and broad, cross-sector security experience.

Assessing the security of AMI and Smart Grid systems is different than traditional computer and network security assessments in both scope and technique. Smart Meter systems are composed of a large number of embedded field components that are vulnerable to attack. The wireless component may involve three or more different radio systems, such as mobile 2G/3G/4G backhaul, proprietary medium-range mesh networks, and short-range ZigBee networks. Communication is typically carried over a mix of standards-based and proprietary networking technologies and protocols. A variety of cutting-edge security controls, including public-key infrastructure, mixed asymmetric and symmetric cryptography, new secure broadcast protocols, proprietary secure-session capabilities and secure hardware are used from the circuit implementation up through the application layer. Tightly integrated,
high-density embedded system hardware renders many traditional laptop-based security tools without a means to connect.

THE APPLIED COMMUNICATION SCIENCES’ RESPONSE

Applied Communication Sciences (ACS) created a multi-disciplinary team of veteran security experts with extensive hands-on experience in software, hardware and wireless security. Our approach was direct and comprehensive — the first step, to validate the security controls and then identify potential vulnerabilities based on a threat analysis. Realizing that traditional security tools would be of limited use, we went back to security fundamentals and began innovating new test methods, using test equipment and custom-developed software and hardware tools.

An assessment of the AMI field components was conducted over a period of several weeks and included site visits and laboratory work at ACS’s research and testing facility. Prior to the testing, we conducted a paper analysis on an AMI security architecture, which involved examining numerous product documents and holding multiple conference calls with the utility and its vendors. Three categories of security were investigated using techniques such as reverse engineering, code manipulation, hardware exploitation and wireless analysis.

The analysis included:

- Network and radio security assessment
- Software security assessment
- Embedded hardware security assessment

During this engagement, ACS:

- Developed and shared its test strategy and plan with the utility
- Evaluated embedded system circuit technology and formulated a hardware/firmware attack strategy
- Conducted onsite and laboratory security testing
- Constructed multiple exploit demonstration models for proof of concept
- Reported its progress on a daily basis while onsite, and weekly when offsite
- Documented findings and recommendations in a comprehensive assessment report

ACS demonstrated that the AMI infrastructure was vulnerable to previously unknown attacks. In addition, the team discovered that several of the security controls had not been implemented. ACS enlightened both the utility and AMI vendors to potential vulnerabilities. After the assessment, ACS worked through potential methods of remediation with the utility and AMI vendors and helped determine that the mitigation strategy would also involve system hardware updates. Our findings provided the utility with critical risk information to make
informed business decisions about its immediate deployment plans and security needs for one of its largest investments.

**THE RESULTS**

- Over the course of the project, the utility worked with its vendors to redesign its AMI infrastructure, advancing the implementation of its security architecture, and conducting its own security analysis and testing. Completely satisfied with Applied Communication Sciences’ first assessment, the utility immediately re-engaged the team to conduct a focused security assessment of the redesigned AMI infrastructure. Given the significant investment of time and resources in the redesign effort, both the utility and its vendors were hopeful of the results.

ACS was provided products with newly designed electronics for analysis. After analyzing the hardware design, ACS changed its mode of attack, altered its toolset, and performed another round of detailed security vulnerability testing by working with the utility and its vendors to further identify risks and improve the security of the AMI infrastructure.

ACS worked closely with multiple management layers within the utility, including their CISO, to help them understand the risks they faced and appropriate mitigation alternatives. We also mediated interactions between the utility and its vendors to mitigate the utility’s exposure. Recognizing that the goal of mitigating all major AMI security vulnerabilities through product modifications was not practical in most cases, the utility, with ACS assistance, embarked on building new independent capabilities to detect and respond to AMI security incidents. In the process, the utility discovered that the application of these new capabilities extended beyond security into engineering, operations, maintenance, and revenue assurance areas. Currently in use, the system is integral to its AMI operations processes and of efforts to re-engineer operations to support the Smart Grid.

**APPLIED COMMUNICATION SCIENCES EXPERTISE**

Applied Communication Sciences is a pioneer in the emerging field of Smart Grid security and Smart Meter systems, and has performed multiple vulnerability assessments and security penetration testing on AMI for major North American electric and gas utilities. The company has conducted in-depth network, software, and low-level hardware security analyses on Smart Meter two-way communications and control systems that employ advanced technologies, such as spread spectrum, mesh networking, public key infrastructure and secure broadcast protocols. ACS is helping utilities define the security architecture, requirements, policies and implementation plans for Smart Grid technologies, and is the first to define Smart Meter forensics procedures.

While utilities today continue to focus on deploying Smart Meter technology, some pioneering utilities and ACS have already ventured into the next phase of the Smart Grid evolution, which involves successfully integrating and operating a secure AMI across
business functions. ACS is presently assisting utilities in dealing with the cascading changes Smart Meters are creating in utilities’ security operations, incident response, engineering, maintenance, revenue assurance, system monitoring, and service assurance functions.

ABOUT APPLIED COMMUNICATION SCIENCES

Applied Communication Sciences delivers world class research, consulting and engineering to enable government agencies, telecom carriers and commercial enterprises to fully exploit technology futures. Drawing on its Bell Labs heritage, ACS excels at creating innovative technologies and services to solve the most difficult and complex information and communications problems. Areas of particular expertise include cyber security and information assurance, network and operations, data analytics, advanced software and methodologies, wireless and mobility, application engineering and integration, smart grid, and optical networking and quantum technologies.

ACS is headquartered in Basking Ridge, NJ, and is a Vencore Company.

FOR MORE INFORMATION ABOUT SMART GRID SECURITY, CONTACT US AT:

Applied Communication Sciences
150 Mount Airy Road
Basking Ridge, NJ 07920
smartgrid@appcomsci.com
www.appcomsci.com