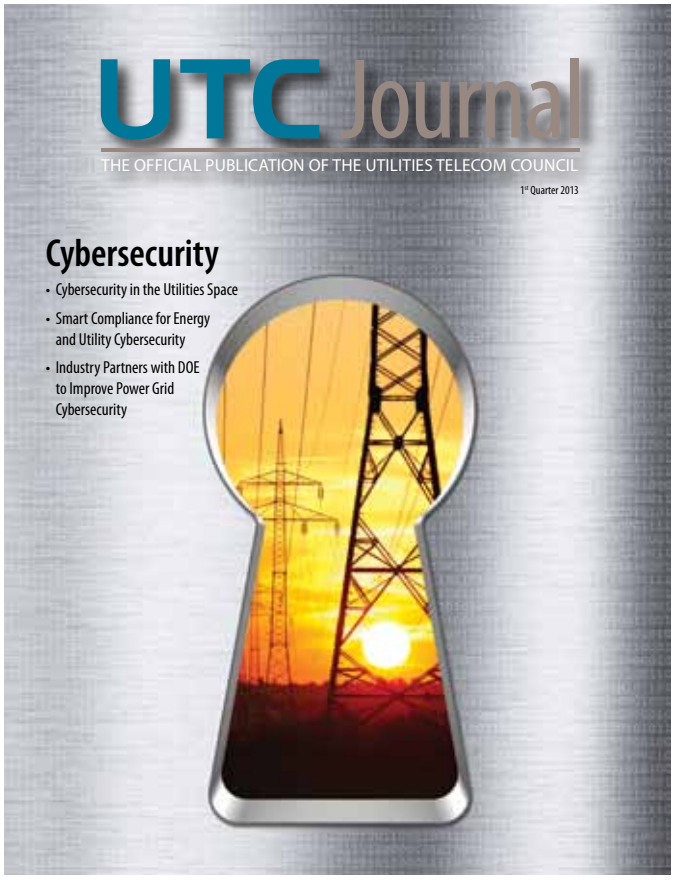
Security Safeguards + Customer Privacy = Smart Grid Success

The modern business world is awash in data, and utilities are certainly no exception. Smart grid architectures use sophisticated technologies to collect and transport vast amounts of data. While the proliferation of data provides valuable insight into energy demand and usage patterns, it comes with an expectation that utilities will keep that data secure and protect consumer privacy.

Since the appearance two years ago of the Stuxnet computer virus, which targeted a nuclear plant's Supervisory Control and Data Acquisition (SCADA) system, we've learned a lot about control system security and vulnerabilities. While we've yet to unlock all the secrets of Stuxnet, we know it has had a profound influence on the smart grid and cybersecurity market. The Government Accountability Office, Department of Energy, National Institute of Standards and Technology, Department of Homeland Security, and others are working internally and with industry to ensure the smart grid is secure.



Distribution automation, substation automation, Advanced Metering Infrastructure (AMI), and all other smart grid technologies that rely on new digital control, monitoring, and instrumentation, as well as more ubiquitous networking technologies, such as the Open Shortest Path First (OSPF) routing protocol, are generally considered to be more cyber-vulnerable. Like other common routing protocols, OSPF creates routing tables complete with IP subnets of all devices on the network. This would be very valuable information to anyone attempting to infiltrate the network. Connecting AMI into the utilities' distribution automation, IT, and communications systems also creates new vulnerabilities. Traditional IT security policies, technologies, and testing may not be applicable to, or sufficient for, control systems. In addition, cloud-based storage of AMI data represents a rich target for hackers.

While security concerns are very high, security-related investment is lagging. In June, the National Association of Regulatory Utility Commissioners encouraged state commissioners to work with utilities to increase security investments. I believe we, as an industry, need to listen. The demand for greater smart grid security will only increase. Where traditional security logic says we should isolate our vulnerable operational control systems and customer data, smart grid causes us to "open

By John Chowdhury

up" access to our customer data, and our command and control systems to integrate and interconnect with other systems.

For example, consider the way that an AMI, applauded for its ability to help utilities and consumers better understand energy usage, could increase vulnerabilities. AMI, particularly when paired with Home Area Networks (HANs), means consumers are no longer quarantined or protected from outside hackers. Data collected by AMI meters can be highly detailed. For example, individual appliances used by the consumer, along with the days and times those appliances are used, may be identified through AMI data. The transmission of this personal information over communications networks makes it subject to potential interception or theft as it travels network segments.

According to the report, S*mart Meter Data: Privacy and Cyber Security*, published in February 2012 by Congressional Research, federal privacy and cybersecurity laws may apply to consumer data collected by residential smart meters. This data may be protected from unauthorized disclosure or access under the Stored Communications Act, the Computer Fraud and Abuse Act, and the Electronic Communications Privacy Act. Authors of the report also state that consumer data may be subject to Section 5 of the Federal Trade Commission (FTC) Act. The FTC has recently focused its consumer protection enforcement on entities that violate its privacy policies or fail to protect data from unauthorized access. This authority could apply to electric utilities in possession of smart meter data. Furthermore, general federal privacy safeguards provided under the Federal Privacy Act of 1974 protect smart meter data maintained by federal agencies, including federally owned electric utilities.

Facing everything from government penalties to market backlash, it's critical that utilities implement sufficient smart grid security and privacy measures. Utilities should determine the types of feedback and protection loops that are needed to prevent unauthorized penetration of the network to the home and improper access to internet-based monitoring portals. Unauthorized changes to customer usage data must be prevented at all times, and customer data must never be inappropriately transmitted externally. Utilities should keep in mind their liability in the event customer data is ever accessed and misused.

As our industry works toward evaluating security alternatives and standardizing on the chosen security measures, the following checklist can help utilities ensure that security is being considered with every step in the path to smart grid deployment. Keep in mind that these considerations should not be used on rare occasion—in the event of a compliance audit, for example—then set aside. Rather, treat this list as a guide in a continuous process that makes security and privacy a top priority.

Elements of Customer Privacy Protection

- Any in-home device that connects to the utility's meter should be certified or approved to comply with cybersecurity standards or operational characteristics so that the utility's meter data is not compromised.
- Customers should have access to historical usage data and billing data for a reasonable period, via a utility-provided web portal.
- Customer authorization should be required for access to any customer-specific meter data by a third party. Third-party use of meter data should be limited to the specific purposes disclosed by the third party to the customer.
- Customers need to be fully informed about the information to which they are granting access. Third parties must fully disclose this in plain language.

Elements of Data Privacy Protection

- Switch encryption methods using the IEEE 802.1ae MACsec standard.
- Virtual Private Network connections using Generic Routing Encapsulation tunnels (RFC2 2784) and IPSEC (128 bit 3DES or AES).
- Audit processing failure triggers, alerting designated personnel in the event of an audit processing failure.
- Automatic labeling of information in storage, in process, and in transmission in accordance with access control

requirements; special dissemination, handling, or distribution instructions as required by the system security policy.
- Use of metering protocols (e.g., ANSI C12.18, C12.19).
- Use of wireless communications protocols (e.g., IEEE 802.16b).
- Embedded security algorithms (e.g., encryption, message authentication).
- Installation of anti-virus software.
- Implementation of firewalls.
- Compliance with networking data security protocols and technologies.
- Use of application-specific security protocols.
- Use of appropriate routing and switching protocols.
- Mutual authentication and authorized levels of access control.

Strategies for Avoiding Widespread Disruption of Service

- Secure interconnections and interdependencies between transmission systems.
- Secure boot loader on every device to verify image signature.
- Distributed key management with unique keys per network link.
- Very limited range of control—restricted to only directly connected devices.
- Link-layer security to check trust status of any device before allowing full participation.
- Link-layer security for protection of routing information.
- Hardware security module to prevent over-the-air theft of cryptographic material.
- Rate limiting of critical commands.

Strategies for Avoiding Local Attacks

- Secure storage of private keys.
- Code reviews of any changes to any components of the smart grid (e.g., NAN, FAN, WAN, switches, routers, meters, sensors, etc.)
- Hardening techniques for servers, communications modules (NICs), switches, routers, etc.
- Logging of security errors and suspicious activity.
- Tamper resistance.
- Certificate revocation.

Strategies for Preventing Insider Threat

- Continuous review of relevant stakeholders' roles and privileges.
- Separation of duties.
- Logical and physical security perimeters.
- Multiple signers.

As an industry, it's imperative we work together to ensure the security of the smart grid and protect the privacy of the connected customer. A prudent control system cybersecurity program should make the utility more secure; ensure customer data is secure; maintain, and when possible improve, system reliability and availability; and meet regulatory requirements.

A major security or privacy breach would be a significant setback to the evolving smart grid movement. Let's make sure we take all realistic steps to minimize this possibility and continue powering forward in architecting utilities' networks of the future.

As utility practice director at Fujitsu Network Communications, Inc., John Chowdhury develops unique network integration solutions, modernization programs, and network operations offerings tailored to support utilities as they adapt their communications networks to meet new demands for scalability, reliability, standards, and security. During his 25-year career, Chowdhury has provided strategic business and technology guidance to energy entities in the areas of smart grid/AMI/distribution automation, business case development, customer relationship management, billing, and telecommunications/wireless networks. His work with utilities and governments included architecting the first smart grid solution in the United States. He is a member of the UTC Smart Networks Council Board of Directors.

Realize Your Future Network Vision Today.

For a turnkey end-to-end communications network customized to the unique needs of your utility, turn to Fujitsu. Our Master Network Integration solutions offer a broad range of choices for designing, deploying and operating a multivendor network to support your modernization initiatives.

As a trusted advisor and partner, we work with you as part of your team to speed deployment, drive down costs and keep pace with rapidly evolving business requirements. We'll put you on the path to the utility of the future.

FUJITSU

shaping tomorrow with you

Fujitsu Network Communications, Inc • 2801 Telecom Parkway, Richardson, TX 75082 Tel: 800.777.FAST (3278) • us.fujitsu.com/telecom