White Paper

## Stopping the Next Breach:
## Why a Non-Proprietary, Standards-Based Solution is the Best Approach

Landis+Gyr
manage energy better

# Is Your Organization Following Best Practices for Today's Rapidly Evolving Threats?


Michael Demeter (CISSP, CSSLP)
Security Architect

Stephen Chasko (CISSP)
Solutions Director, Security



by Michael Demeter and Stephen Chasko

December 2017

# Stopping the Next Breach: Why a Non-Proprietary, Standards-Based Solution is the Best Approach

## Is Your Organization Following Best Practices for Today's Rapidly Evolving Threats?

Advances in smart grid technology offer a host of benefits to utilities and consumers and introduce compelling new ways to increase communication across the distribution system. However, they can also create areas of vulnerability and increase exposure to potential attacks.

In fact, the worldwide cybersecurity market is expected to grow to $170 billion by 2020.[1] From bad data injection to spoofing, man-in-the-middle-attacks, decryption attacks, electromagnetic attacks, energy theft attacks and more, security threats are a real concern.

"Cyber threats to the electricity system are increasing in sophistication, magnitude and frequency," according to the U.S. Energy Department in its report, *Transforming the Nation's Electricity System.*[2] "The current cybersecurity landscape is characterized by rapidly evolving threats and vulnerabilities, juxtaposed against the slower-moving deployment of defense measures."
In response to this landscape, best-in-class solutions providers continue to develop and improve security solutions that focus on industry standards and world-class security partners.

by Michael Demeter and Stephen Chasko

December 2017

# Threats from outside — and inside — the utility

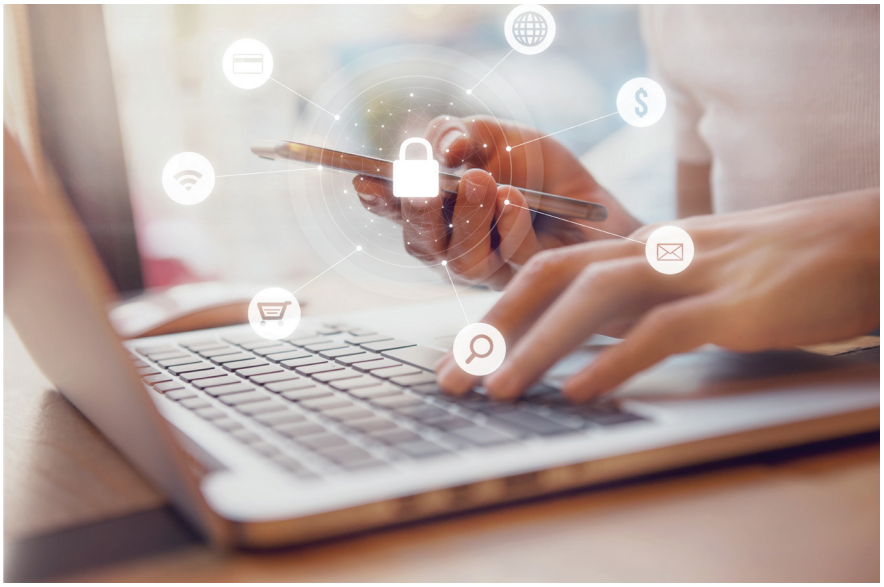
## Unprotected smart grids face potential threats from both external hackers as well as a utility's own employees or business partners.

Within an unprotected smart grid, meters can be hacked by accessing onboard memory, thereby reading diagnostic ports and other network interfaces. RF sniffing is the process of monitoring and capturing all the packets passing through a given network using radio sniffing tools in order to capture a smart meter's consumption data. By sniffing and then breaking network encryption, attackers learn the communication protocol used in a meter.[3]

Utilities must not only fend off ever-present attacks from cybercriminals — employees and vendors can unknowingly release sensitive information. The data firm Recorded Future scoured Internet forums and "paste sites" trying to uncover the vulnerabilities involving employee "credentials" and found that 221 of the nation's top companies had employee credentials exposed. Companies with exposed employee credentials included 49 percent of public utilities.[4] While some utilities have recently experienced highly public breaches to their technology environments, many incidents go unreported. Preventing an attack will require improving the security of the smart grid as well as intelligent constraints on how employees, consumers and partners access applications and data.

A standards-based security solution that relies on a proven, open architecture to address every access point in the network ensures all utility assets are protected at a high level, regardless of which communication technologies are deployed.

Companies with exposed employee credentials included **49 percent** of public utilities.[4]



by Michael Demeter and Stephen Chasko

**Stopping the Next Breach: Why a Non-Proprietary, Standards-Based Solution is the Best Approach**
**Is Your Organization Following Best Practices for Today's Rapidly Evolving Threats?**

# Key security principles

A simple but widely applicable security model is the **Confidentiality, Integrity** and **Availability** (CIA) triad, representing the three key principles that should be guaranteed in any kind of secure system. A fourth category, **Authentication**, is also discussed with regard to security concerns. It is these four principles that are often exploited through varying degrees of attacks.


## CONFIDENTIALITY

Confidentiality is a concern because utilities need to prevent sensitive data from reaching the wrong people, while making sure the right people can still gain access. For example, utilities may want to ensure information such as scheduled customer billing data, meter alarm information and home-area network events are stored in an encrypted format to avoid being intercepted by a consumer's neighbor, another utility or an attacker who could use the data to gain insight about a utility's advanced metering network.

## INTEGRITY

Integrity involves a utility maintaining the consistency, accuracy and trustworthiness of data over its entire network lifecycle. For example, meter data must not be changed in transit, and the utility must ensure that unauthorized personnel cannot alter data. Utilities rely on strong cryptographic mechanisms to ensure the integrity of meter readings, command and control data.

## AVAILABILITY

Availability to data and equipment are the primary operational concerns for smart grid technology. Utilities must have the utmost confidence with their access to meter and billing data. Utilities can best ensure availability by rigorously maintaining hardware, performing repairs immediately when needed and maintaining a functioning software system environment free of corruption or conflict. Additionally, extra security measures, such as firewalls and proxy servers, can help prevent downtime and mitigate malicious actions such as denial-of-service (DoS) attacks.

## AUTHENTICATION

A utility must be aware of who is accessing its data. Unauthorized access could be the result of unmodified default access policies or lack of clearly defined access policy documentation. Utilities need to ensure only authorized utility personnel can view information or perform certain actions. It is vital that the head-end system, field tools and network devices are deployed with a proper "root of trust." Without the ability to confidently authenticate a message or command originated from a trusted source, a malicious attacker could attempt to "spoof" themselves as the head-end system, field tool or as a legitimate network device in attempt to send an illicit command to a meter or inject malicious code into the network.

by Michael Demeter and Stephen Chasko

**Stopping the Next Breach: Why a Non-Proprietary, Standards-Based Solution is the Best Approach**
**Is Your Organization Following Best Practices for Today's Rapidly Evolving Threats?**

# Meeting security needs with confidence

A utility's systems partner should follow best security practices throughout the entire utility network and incorporate standards and software to ensure all security concerns are addressed.

Confidentiality, availability, authentication and integrity of data should be top priorities. Accordingly, communications methods/protocols should have fully integrated non-proprietary security standards validated by top federal and industry standards organizations, including Federal Information Processing Standards (FIPS) and the National Institute for Science and Technology (NIST), to ensure CIA of customer information. These security best practices ensure proper access controls are implemented in the partner's solutions and that utilities feel safe knowing that the confidential data of the utility and its customers is handled with best-in-industry security.

State-of-the-art security best practices within and across each solution component are imperative for data transfer to or from the customer premise and the utility. Data transport security provides privacy and authentication of data as it travels from a multi-energy meter point to the next system instance.

## Six security best practices utilities should follow:

### 1 ENSURING AVAILABILITY

Systems used should be highly compatible with standard IT infrastructure so utilities can employ the best enterprise-level information technologies to solve availability challenges. Data availability concerns can potentially be overlooked in a large utility environment. Every part of your infrastructure needs to be continually backed up and reinforced. Engaging in services that proactively monitor your data ensures that you remain protected and accessible. Lastly, hosting and cloud computing solutions have become an instrumental part of ensuring data availability.

### 2 PROTECTING CONFIDENTIALITY

Utility systems should protect confidential information through the use of non-proprietary security standards integrated within interoperable endpoint/sensor and communications solutions. Additionally, the meter metrology level must ensure data security via protected methods for programming the meter and obtaining customer data.

by Michael Demeter and Stephen Chasko

December 2017

**Stopping the Next Breach: Why a Non-Proprietary, Standards-Based Solution is the Best Approach**
**Is Your Organization Following Best Practices for Today's Rapidly Evolving Threats?**

## 3 DATA INTEGRITY

Data integrity is a fundamental component of utility security. As a process, data integrity verifies data has remained unaltered in transit throughout the utility network. As a function related to security, a data integrity service maintains information exactly as inputted and is auditable to affirm its reliability. Data must be kept free from corruption, modification or unauthorized disclosure to outside threats.

## 4 DATA ENCRYPTION

Encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing the necessary encryption key(s). Encryption is just one tool to keep prying eyes off your confidential data. Identifying critical data, such as meter data and customer billing information, is another step toward determining what data needs to be encrypted and confidential. End-to-end encryption maximizes data protection regardless of whether the data is in a public or private cloud, on a device or in transit. It can be invaluable in combatting advanced threats, protecting against IoT-enabled cyber breach and maintaining regulatory compliance.

## 5 USER AUTHENTICATION

A user authentication system should allocate access permits to users. Because different users such as supplier staff, utility staff, the grid operator or the multi-energy utility have different interests, they should also have different rights to the data on the system and metering point. Access permits can ensure users have rights only to the information they require. In addition, all users of external connections should be authenticated inside a secure data connection protocol. This is especially critical for protecting against signals from an unauthorized meter or a computer that emulates a meter.

## 6 INTENTIONAL THIRD-PARTY PENETRATION TESTING

Utilities that engage penetration testers receive value from revealing vulnerabilities in their end-to-end implementation of smart grid solutions and can focus technology investments in mitigating security measures wisely. Penetration testers attempt to exploit the identified vulnerabilities to show the utility what could occur in the case of a real attack. The target utility's security team should be able to detect multiple attacks and respond in a timely manner. These attacks should be automatically detected, with alerts generated and acted on according to the utility's internal procedures. An independent third party that identifies vulnerabilities can help guide utility leadership to allocate additional funds for cyber-security before a real breach occurs. These tests may also be essential to comply with regulations and pass future audits to obtain necessary certifications.

by Michael Demeter and Stephen Chasko

**Stopping the Next Breach: Why a Non-Proprietary, Standards-Based Solution is the Best Approach**
**Is Your Organization Following Best Practices for Today's Rapidly Evolving Threats?**

## Top Security Solution Features

| | |
|---|---|
| **Device-Specific Encryption Key** | Protect the privacy and integrity of data and commands sent to and from devices |
| **Secure Command Broadcast** | Commands broadcast to groups of devices are also secured with unique keys that provide confidentiality, integrity and authentication |
| **Downstream Message Authentication** | Verify messages using a digital signature to ensure commands originated from a trusted source |
| **Bi-Directional Message Integrity** | Use additional key mechanisms and hashed message authentication code to ensure message integrity |
| **Field Tool Authentication** | Authenticate and secure communication between network devices and field tools |
| **Certified Root of Trust** | Store and maintain a Utility Signing Key within certified security appliances in a high-availability environment |
| **Vaulted Key Management** | Store and manage encryption keys with a dedicated, high-availability key manager |

## Advanced security solutions — what to look for

### People and process

The security solution should be configurable in a way that allows utilities to deploy their specific desired level of protection. One key area of risk is an inside attack, whether malicious or accidental. External attackers can attempt to breach head-end security in many ways, but ensuring employees' legitimate access to systems is just as crucial. Consider head-end operating software and field tools that guard against unauthorized access to functionality and monitor and alert utilities about unusual or improper actions as they happen. To protect against activity by authorized employees, implement strong auditing and reporting processes and capabilities that capture user activity. By following these processes, utilities can quickly identify suspicious activity and pinpoint who performed the action, the date and time in which the action was performed and the results of the transaction.

Head-end software with Role-Based Access Control provides the capabilities necessary for the Security Administrator to assign appropriate permissions to each user of the system. The AMI head-end software can streamline user administration by integrating with enterprise single sign-on solutions. Once the appropriate security settings have been established, the solution ensures a smooth and easy process for network security configuration, device management and network management.

by Michael Demeter and Stephen Chasko

**Stopping the Next Breach: Why a Non-Proprietary, Standards-Based Solution is the Best Approach**

**Is Your Organization Following Best Practices for Today's Rapidly Evolving Threats?**

## Systematic protection

Look for a security solution that takes a holistic approach to people, technology and process security for the smart grid network. Some security approaches focus on protecting the transportation of data messages, but the better solutions go beyond message transportation and offer protocols to validate the trust level of the originator of a data message, and prevent the spread of unauthorized or malicious code.

## Valued partnerships

An ideal security solution offers features and functionality that are configurable to match each utility's organizational security approach and risk posture. These features can be provided by linking users to third-party appliances made available through strategic partnerships with reputable security vendors.

## Operationally secure

Enabling advanced security does not affect the endpoint installation process. In fact, there are no additional steps required by the installer to deploy endpoints in the field, as all the security parameters and keys are exchanged between the endpoint and the head-end server via the endpoint with a "no touch" auto-registration process.

## Data protection

Securing stored data involves preventing unauthorized people from accessing it as well as preventing accidental or intentional destruction, infection or corruption of information. Back up your data with confidence using flexible deployment options and rapid recovery — across your environment. Prevent unauthorized access, disclosure and modification of data stored across your utility onsite or in the cloud. Additionally, make sure you apply retention policies for government-regulated data, legal or temporary events and internally defined retention standards.

## Resistance and local security

Tamper resistance protects devices from being modified and monitored. This includes mechanisms such as keyed connectors, locks and encrypted device-to-device mechanisms. Advanced security solutions should include signed and verified firmware, disabled JTAG/debug communications interface, encrypted flash memory, locked optical ports (configurable), meter tamper detection, backhaul protection and other physical and system-level security features.

Utilities should use the

**NIST guidelines and requirements**

when researching prospective smart grid solution vendors.

## Compliance and auditability

The NIST-produced NISTIR-7628 is a set of guidelines, or "a reference document," for implementing smart grid security. The information and requirements within NISTIR-7628 provide valuable direction for developing effective cyber security strategies. Utilities should use the NIST guidelines and requirements when researching prospective smart grid solution vendors. The vendor you choose should take a proactive approach to following the guidelines:

- Implement security controls in all phases of the development cycle, from design through implementation, maintenance and device/product decommissioning
- Develop and perform ongoing risk assessments and penetration tests to identify assets, vulnerabilities, threats and impacts that can be used to prioritize and implement necessary mitigating security features
- Create a robust, future ready, systemic feature set leveraging the requirements documented in Volume 1
- Implement appropriate privacy controls based on information provided in Volume 2
- Leverage the vulnerability classes listed in Volume 3 to ensure your security solution has the necessary controls to mitigate the vulnerabilities listed

by Michael Demeter and Stephen Chasko

December 2017

# Conclusion

## Security solutions must protect the utility today, while anticipating evolving threats in order to meet the needs of tomorrow.

Industry standards that are challenged and fully vetted in open standards organizations as well as in industry alliances must be used to set a high standard for consistent and interoperable solution performance.

By developing a best-in-class security solution that focuses on industry-driven standards, open non-proprietary standards and NSA Suite B recommended cryptography, Landis+Gyr is able to offer a robust feature set and proven appliances provided by world-class partners. Our solutions provide the necessary confidence that data security and critical infrastructure are secure, electric service is protected and the utility's reputation is protected.

[1] Morgan, S. 2015. "The Business of Cybersecurity: 2015 Market Size, Cyber Crime, Employment, and Industry Statistics". Forbes.com. Accessed from **https://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#6ded0f675d0d.**

[2] U.S. Department of Energy. "Transforming the Nation's Electricity System: The Second Installment of the Quadrennial Energy Review." Energy.gov. Accessed from **https://energy.gov/sites/prod/files/2017/01/f34/Transforming%20the%20Nation%27s%20Electricity%20System-The%20Second%20Installment%20of%20the%20Quadrennial%20Energy%20Review--%20Full%20Report.pdf.**

[3] Skopik, F. 2012. "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures." *International Journal of Smart Grid and Clean Energy*. Accessed from **https://pdfs.semanticscholar.org/c824/ed2e7d12bca030e0c16684842a4e3fb36c37.pdf**

[4] Brunker, M. 2014. "Unwitting Workers Give Hackers Keys to Fortune 500 Firms' Networks: Study". NBCnews.com. Accessed from **https://www.nbcnews.com/news/investigations/unwitting-workers-give-hackers-keys-fortune-500-firms-networks-study-n236076**

by Michael Demeter and Stephen Chasko

December 2017