Landis+Gyr
manage energy better

Landis+Gyr Security Architecture

June 2021

Contents

1 | Summary

This document provides the architecture of the Landis+Gyr Gridstream Security offering for North America.

AUTHORS
STEPHEN CHASKO

CONTIBUTORS
DAMIEN HUGOO

2 | Smart Grid Security Landscape

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. 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.

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]

Not only must utilities fend off ever-present attacks from cybercriminals, but also 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.

3 | 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 need to rely on strong cryptographic mechanisms to ensure the integrity of meter readings, command and control data.

AVAILABILITY

Availability of data and equipment are the primary operational concerns for smart grid technology. Utilities must have the utmost confidence in 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 free of corruption or conflict. Additionally, 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.

4 | Security best practices utilities should follow

Meeting security needs with confidence

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

Confidentiality, integrity, availability, and authentication 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) written by National Institute for Science and Technology (NIST), to ensure CIA of customer information. These security best practices ensure that proper access controls are implemented in the partner's solutions and that utilities feel safe knowing the confidential data of the utility and its customers is handled with best-in-industry security.

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, preventing the spread of unauthorized or malicious code.

People and process

One key area of risk is an insider 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 (RBAC) 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 process for network security configuration, device management, and network management.

Data protection

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 prevent unauthorized access to 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 breaches, and maintaining regulatory compliance.

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.

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:

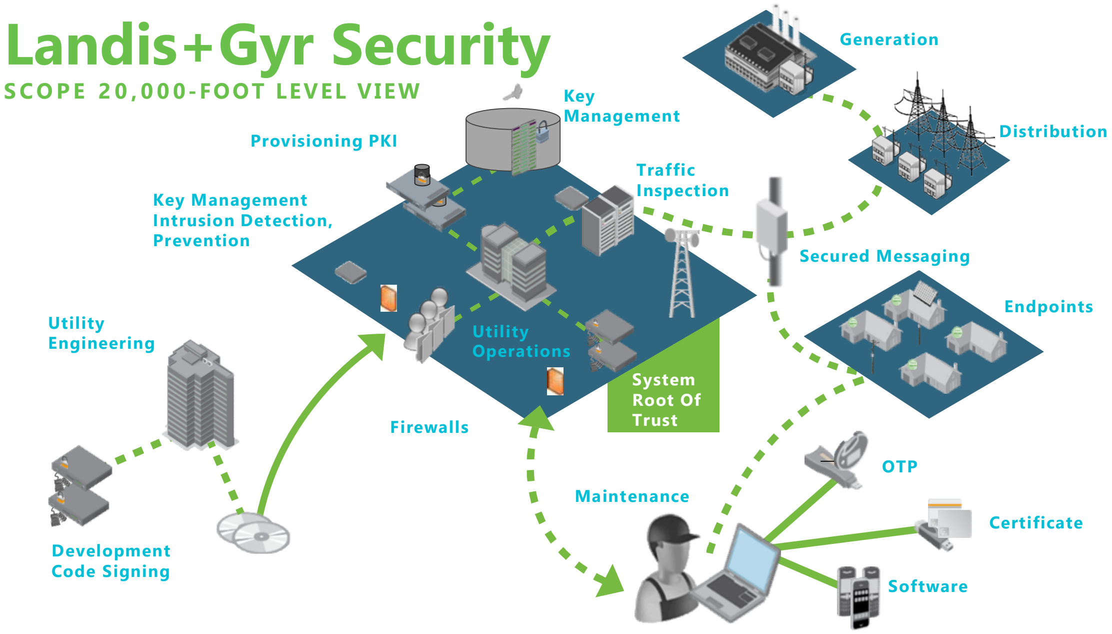
- Implement security controls in all phases of the development cycle, from design through implementation, maintenance, and device/product decommissioning
- Develop and perform ongoing risk assessments and penetration tests to identify assets, vulnerabilities, threats, and impacts that can be used to prioritize and implement necessary mitigating security features
- Create a robust, future-ready, systemic feature set leveraging the requirements documented in NISTIR 7628 Volume 1
- Implement appropriate privacy controls based on information provided in NISTIR 7628 Volume 2
- Leverage the vulnerability classes listed in NISTIR 7628 Volume 3 to ensure your security solution has the necessary controls to mitigate the vulnerabilities listed

Utilities should use the NIST guidelines and requirements when researching prospective smart grid solution vendors.

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.

5 | Landis+Gyr Gridstream Connect Security Overview

Smart grid networks introduce a variety of new and attractive ways to increase communication across the distribution system. However, the growing number of network entry points may also increase exposure to potential attackers. If left unsecured, potential vulnerabilities might allow an attacker to penetrate the network, gain access to control software, and alter load conditions to destabilize the distribution grid.



Landis+Gyr's Gridstream Connect solution provides utilities with a highly flexible, interoperable, open standards-based, and adaptable platform capable of supporting an ever-increasing list of utility applications and connected devices. To help utilities safely realize the potential of this connected network platform, Landis+Gyr has developed a comprehensive security architecture providing end-to-end protection across the entire network.

Designed to provide security controls and mechanisms at a system level, the Gridstream Connect security solution incorporates FIPS 140-2 validated components and utilizes open standards and cryptographic protocols for RF communication end-to-end with the head end system. The network solution protects endpoints, applications, systems, networks from unauthorized access, exploitation, modification, or denial of any network resources. This allows for addressing exposure risk at each area of the RF network to be addressed, including:

- Command Center head-end system (HES)
- Backhaul communication over the Wide Area Network (WAN)
- Network layer communication (LAN)
- Physical protection of the network devices
- Mobile Administration tool security
- Home Area Network (HAN) security

The Gridstream Connect security solution meets or exceeds both US government and international industry security standards, including NISTIR 7628, Wi-SUN, AMI-SEC, NERC CIP, DOE and others.

Landis+Gyr's proactive involvement with standards organizations such as the NIST Cyber Security Working Group (CSWG), the Wi-SUN Alliance, and the IEEE 802 committees is helping drive the development and adoption of future industry standards and best practices, ensuring that utility investments made today will continue to provide operational and economic benefits for years to come.

Gridstream Connect Security Features:

- Upstream and downstream message confidentiality and integrity
- Firmware signing and authentication
- Strong auditing control and reports
- Role-based access control
- Security configuration capabilities
- Device tamper detection
- Integration with Active Directory

Gridstream Connect Security Provisions to Prevent and Mitigate Unauthorized Access:

Role Based Access Control

The HES enforces access controls through a Role-Based Access Control (RBAC) functionality. RBAC allows the security administrator within a utility to manage user credentials and privileges assignment. In this way, the utility can manage which employees have access to commands and features related to the devices in the network.

RBAC effectively controls access to various network functions based on the credentials provided by the user. The designated security administrator uses the RBAC controls to delegate the ability to remotely access meter data or meter control functions.

Audit Logs

The HES logs all activity engaged by users and makes it available to privileged users like administrators through reports or dashboards (i.e. Security Dashboard). In addition, every device in the network has an event log and transmits new events periodically to the HES.

Meter Tamper Alarms

Landis+Gyr meters offer tamper alarms such as reverse energy flow, tilt/tamper and outage notifications in case a meter is removed from the socket. The alarms are transmitted to the HES upon occurrence and logged by the head end, displayed on the GUI, and optionally emailed to appropriate users.

Network Gateway and Network Bridge Tamper Alarm

In the event that the cover of the network gateway or network bridge is removed, an alarm will be immediately sent to the head end, displayed on the GUI, and optionally emailed to the appropriate users.

Firmware Integrity

All firmware images released by Landis+Gyr are digitally signed utilizing the Landis+Gyr asymmetric private key (ECC). Each endpoint within the network will validate the digital signature using the Landis+Gyr public key. If the key doesn’t match the Landis+Gyr signature, the device will not upgrade that firmware version. This is a strong prevention mechanism to avoid injection of rogue code into the network.

Field Tools

Field Tools used to manage and troubleshoot, enforce usage of network access defined at the HES level and enforced at the device level.

Third Party Penetration Testing

To validate the Gridstream Connect security solution set initially, security partner Lockheed Martin performed a risk assessment using NISTIR-7628 guidelines and the NERC-CIP standard. Additionally, on an ongoing basis, Landis+Gyr performs risk assessments and penetration tests to identify vulnerable assets and implements mitigating security features for discovered security threats. World-class penetration testing partners include Lockheed Martin, IBM, Wurldtech and IOActive among others on a rotating basis. These assessments provide perspective that Landis+Gyr directly incorporates into our research and development process to consistently improve smart grid security.

Landis+Gyr has performed, and will continue to perform, internal and external penetration tests with security industry experts, such as Lockheed Martin and IBM in an effort to stay on top of the increasing number of threats and new attack vectors.

6 | Advanced Security

6.1 | Certified Root of Trust

In the same line, we have partnered with Thales to integrate their LUNA Hardware Security Modules (HSM) into the Gridstream Connect architecture. The HSM serves as the root of trust where the utility ECC private key is vaulted. The private key is used to generate digital signatures to downstream commands sent by the HES. The HSM also features FIPS 140-2 and Common Criteria Level 4 certifications, providing a strong protection for one of the critical elements in the advanced security architecture.

6.2 | Individual and Segment Keys

The Gridstream Connect security solution provides for encryption key segmentations at the individual and group levels. First, each endpoint is required to generate its own AES 256-bit encryption key to encrypt upstream and downstream messages sent to and from each endpoint. All endpoint individual keys are further vaulted in a Key Manager.

Second, the HES system assigns a segment key to one or more mesh pockets (a mesh pocket is comprised of a collector and associated endpoints). The segment key is used to protect the transmission of broadcast downstream commands to all endpoints associated to a specific collector.

6.3 | Secure Key Storage and Lifecycle Management

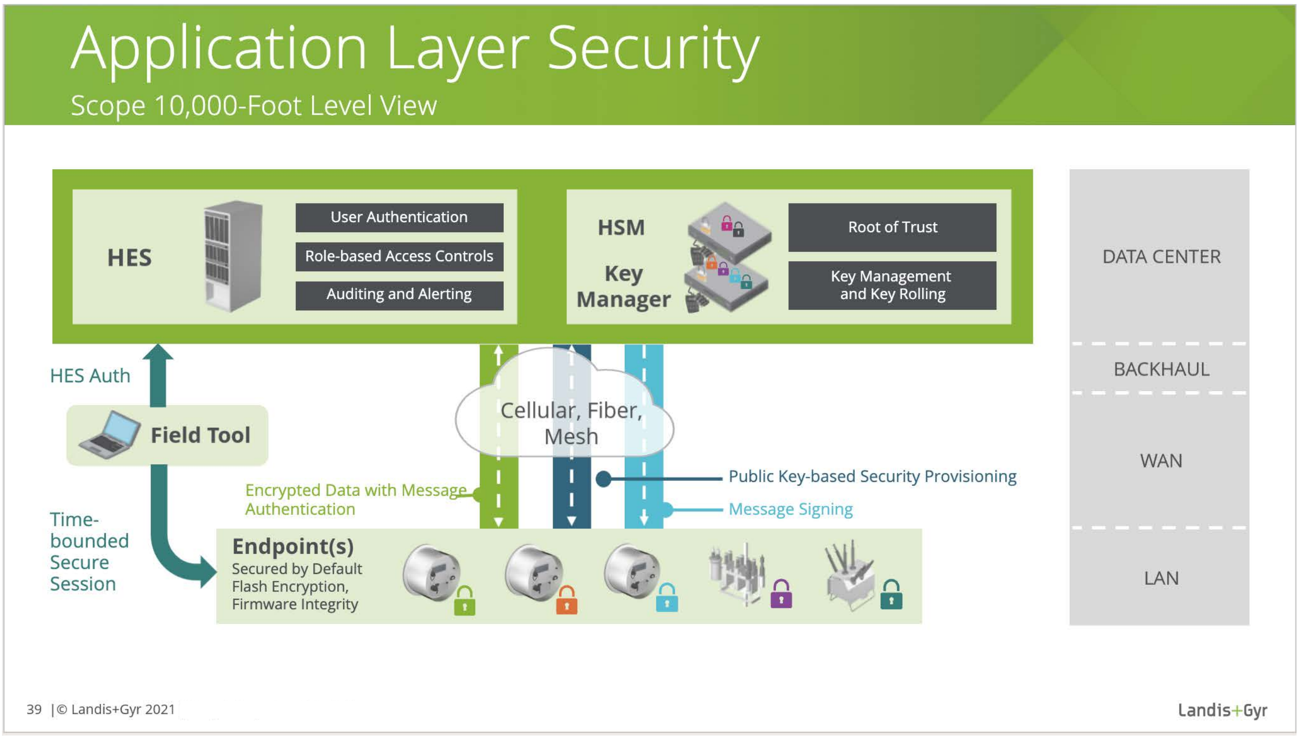
Secure storage of device-specific keys protected via encryption to protect key storage at rest and during system use. Further, device-specific keys and network-specific keys have configurable and mature key rolling and lifecycle management processes. These tools enable the customer to use Gridstream Connect technology along with customer-specific security procedures to follow NISTIR-7628 guidelines for key lifecycle management.

6.4 | Message Authentication

All commands are signed using ECDSA standard based on the utility ECC private key. Endpoints will enforce signature validation before acting on any command, thus providing a control mechanism to prevent rogue commands or man-in-the-middle vulnerability.

6.5 | Mobile Administration Tool Authentication

During a communication request with a network AMI endpoint, field tools must present a digitally signed certificate as a means of validating and authenticating the field tool is authorized to perform a command or action on that device that would allow them access to meter data or meter control functions.



Application Layer Security

Scope 10,000-Foot Level View

HES

User Authentication

Role-based Access Controls

Auditing and Alerting

HSM

Key Manager

Root of Trust

Key Management and Key Rolling

DATA CENTER

BACKHAUL

WAN

LAN

HES Auth

Field Tool

Time-bounded Secure Session

Cellular, Fiber, Mesh

Encrypted Data with Message Authentication

Public Key-based Security Provisioning

Message Signing

Endpoint(s)

Secured by Default

Flash Encryption,

Firmware Integrity

39 |© Landis+Gyr 2021

Landis+Gyr

7 | 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 FIPS-validated cryptography, Landis+Gyr is able to provide the necessary confidence that data security and critical infrastructure are secure, electric service is protected, and the utility's reputation is protected.

Bibliography

Periodicals:

S. Mauw and M. Oostdijk, "Foundations of Attack Trees" International Conference on Information Security and Cryptology – ICISC 2005, LNCS 3935, pages 186-198, December 2005.

Technical Reports:

SGIP CSWG, "Guidelines for Smart Grid Cyber Security, Vol.1, Vol.2, Vol. 3," NIST IR 7628,August 2010.

M. Carpenter, et al, "Advanced Metering Infrastructure Attack Methodology", January 2009

B. Lawlor and L Vu, "A Survey of Techniques for Security Architecture Analysis", Information Networks Division, ISL, DSTO-TR-1438, May 2003

Papers Presented at Conferences (Unpublished):

R. Anderson and S. Fuloria, "On the Security Economics of Electricity Metering," Cambridge University Computer Laboratory, 2010.

Papers from Conference Proceedings (Published):

R. Anderson and S. Fuloria, "Who Controls the Off Switch," in *Proc. 2010, IEEE Smart Grid Communications*.

Y. Liu, P. Ning and M. Reiter, "False Data Injection Attacks Against State Estimation in Electric Power Grids", CCS'09, November 9-13, 2009

J. Newsome, E. Shih, D. Song, A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses", ISPN'04, April 26-27, 2004

C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasure", IEEE International workshop on sensor network protocols and applications, May 11, 2003.

Thesis:

Jung, Sang, Shin, "Attacking and Securing Beacon Enabled 802.15.4 Networks"Computer Science Thesis Georgia State University,2011