# Smart Grid Security: Recent History Demonstrates the Dire Need

White Paper

maxim integrated™

Keywords: smart grid security, smart meter, energy measurement, authentication, symmetric encryption, asymmetric encryption, distribution automation

# Smart Grid Security: Recent History Demonstrates the Dire Need

**By: David Andeen, End Segment Manager, Smart Grid**
**Feb 11, 2013**

*Abstract: The rapid build out of today's smart grid raises a number of security questions. In this article, we review two recent well-documented security breaches and a report of a security gap. These situations include a 2009 smart-meter hack in Puerto Rico; a 2012 password discovery in grid distribution equipment; and insecure storage of a private key in distribution automation equipment. For each of these attacks, we examine the breach, the potential threat, and secure silicon methods that, as part of a complete security strategy, can help thwart the attacks.*

A similar version of this article appeared in the December 2012 issue of *Power Systems Design Europe* magazine.

## The Smart Grid Evolution Increases Its Security Risks

The smart grid surrounds us these days. In the U.S. approximately 36 million smart electricity meters have been deployed since 2007.[1] In Europe, both Italy[2] and Sweden[3] have each achieved complete smart meter installations. Spain is actively deploying,[4] while the rest of Europe and Asia are all on the verge of massive deployments. Utilities in North America, Europe, and China are aggressively upgrading their distribution automation (DA) infrastructure with smart-enabled devices, including line sensors and distribution controllers enabled with communication. In a relatively poor global economy, smart grid projects shine with bright success and infrastructure renewal.

Success often makes us comfortable, even complacent about the day-to-day operation of our systems. Looking forward to even more deployment, we tend to avoid hard, worrisome questions about the long-

term effects of the movement. A particular thorny question for the evolving smart grid is security. Where? How much is enough? A former utility employee recently asked me, “If we network all of the electricity meters and grid infrastructure, can someone write a computer virus and take down the entire grid?” Unfortunately, my answer was yes.

To answer these smart grid security questions, we will review two recent well-documented security breaches and a report of a security gap. These situations include a 2009 smart-meter hack in Puerto Rico; a 2012 password discovery in grid distribution equipment; and insecure storage of a private key in distribution automation equipment. For each of these attacks, we’ll examine the breach, the potential threat, and secure silicon methods that, as part of a complete security strategy, can help thwart the attacks.

## The Security Risks Are Increasing

Whether a computer virus can take down an entire electricity grid is entirely up for debate, and beyond the scope of this article. Furthermore, the security world abounds with threats and worst-case scenarios. As of now, most smart meter communication occurs in a query-and-respond manner; the data exchange is simple and with minimal control functionality. Critical switching on the distribution grid occurs over different networks, protected by high voltage.

But the grid is evolving right in front of us. In fact, the widespread deployment of the smart grid is increasing the opportunities for hardware and cyber attacks. As with all communication networks, connectivity enables functions and applications that consume more bandwidth; connectivity makes access to the system functionality simpler. The drive toward using Internet protocol (IP) to achieve interoperability will create robust networks that operate at low cost, but ones that are just as vulnerable to attack as in the Internet. As with corporate data, now critical grid functions, such as switching, remote disconnect, and volt/VAR optimization, will migrate to these networks. Wonderful technical advances for the grid, yes, but along with them come new vulnerabilities.

With smart meters and grid distribution communication becoming more pervasive, we must anticipate critical threats. We must also assess the security breaches that have already occurred in the smart grid. What can we learn from them? What protections can be proactively designed into smart grids to thwart those attacks and others to come? Let’s try to answer these questions.

## Securing Manufacturing

In 2009, employees at an electricity meter manufacturer in Puerto Rico hacked smart meters by accessing the meters through their optical ports. The U.S. FBI reported that the meter manufacturer’s employees and utility employees were both altering meters and training others to alter meters; their payoff was $300 to $1000 in cash per meter. U.S. federal authorities estimate that the Puerto Rican utility losses could amount to $400 million and that future attacks are likely.[5] Although the exact security mechanisms, or lack thereof, at the manufacturing site are unclear, one fact is undeniable: manufacturing employees could gain access to a meter. Most companies use third-party manufacturers for some or all of their product manufacturing. While wealthier, established companies put tight controls on these manufacturers, smaller equipment makers often do not, or cannot, closely control their supply chain. As a result, their products are at higher risk of a security breach.

Strong authentication protocols are one highly effective method for avoiding the type of attack witnessed

in Puerto Rico. In authentication, two communicating parties verify their identity and, thus, trust their communication. Individual passwords serve as the most basic forms of authentication. Any communication from an unauthenticated party, such as a hacker, is ignored. But what happens when a perpetrator uses a discovered password to gain system access?

In a typical password-protected *static* system, the same password is used every time. A *dynamic* system, in contrast, achieves higher levels of authentication. As described by Jones,[6] here the host generates a random number as a security challenge whenever a party requests access. The requestor must then respond with an answer generated from that random number, the message that it is trying to send, and a secret key. The host compares the response to its random number challenge with an internally generated response. The two responses must be equal, but every subsequent response will be different, because each is based on the random number generated by the host.

The mathematics of this challenge and response are designed so that a party intercepting the response has virtually no possibility of decoding the secret key from that information. The dynamic nature of the system ensures that the communications are unique each time. The SHA-1, SHA-2, and SHA-256 algorithms are all excellent examples of this type of dynamic authentication.

The most valuable information in the challenge-and-response authentication process is the secret key. Additional techniques to further strengthen the authentication process include generating secret keys on a physically secure chip like the MAXQ1050 DeepCover® secure microcontroller and generating keys in stages. These methods ensure that no single party retains access to all the building blocks of the keys. A combination of the integrated and staged key generation provides even better security.

## Single or Multiple Keys and Asymmetric Schemes

In August of 2012, Justin Clarke reported a security flaw in the operating system of RuggedCom's Rugged Operating System (ROS).[7] RuggedCom products provide ruggedized network timing and communications infrastructure for electricity transmission and distribution, as well as other industrial applications. Clarke's report asserted that a single key could be used to penetrate the inner workings of the ROS. Once inside, an attacker could easily view communication traffic without additional security barriers. Furthermore, a key could be obtained from any piece of RuggedCom equipment and used to access any other piece of their equipment.

The issue at hand relates to a single secret key. Systems employing a symmetric encryption algorithm will use a single private key for encryption and decryption of data. Any device with the private key may join the network, similar to a conference call in which participants use the same code to enter the discussion. Because of their sheer volume, smart grid devices, and smart meters specifically, create a challenge with symmetric encryption schemes. The millions of smart meters and pieces of distribution automation equipment installed on the grid mean that the holder of that single secret key can potentially access each piece of equipment. The security threat is obvious. Shutting off power and causing massive outages in areas of critical infrastructure or high population represents the worst potential outcome. Furthermore, this is a minimal effort attack with potentially dire consequences.

An *asymmetric* certificate-based security scheme provides a solution to this type of attack. Asymmetric schemes consist of a public/private key combination for each end device. Each key works to mathematically encode or decode a message. All network devices know each other's public key and may use it to encode a message directed to a specific device. That specific device then uses its private key to decode the message. Secure integrated circuits (ICs) generate private keys completely on chip, store

them in secure memory, and never reveal them. Managing entities, such as utilities, then also give each device a certificate that establishes a chain of trust within a network. In this way the meter becomes associated with an access point, is thus authorized, and can join the network. Each certificate should be unique, based on an individual identification number or other unique identifying characteristic. This scheme, therefore, provides the benefit of asymmetric encryption, never revealing either private keys for the many devices on the grid or network or the individual identification of each device.

## Protecting Keys

On September 19, 2012, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported another security gap in distribution automation equipment. In this incident the private key, used for signing certificates, was insecurely stored on a programmable logic controller (PLC).[8] The private key was the certificate authority's private key, so anyone obtaining the private key could certify itself/themselves as a valid device in the network. The attacker could then execute a "man in the middle" attack; the attacker intercepts communications, certifies itself as a valid system device, and proceeds to gain network access. Initial resolution of the issue required uninstalling certificate authority signing keys and manually confirming the identity of each device on the network. This resolution works in a smaller network, but would be a massive expense and effort for a multimillion device network.

Key management is the most difficult aspect of security because key access means key exposure, to systems and/or people. Exposing keys greatly increases risk of theft. The first line of defense in protecting keys is, therefore, to generate them once, in a physically secure IC, and never let them off the chip. A device on the smart grid can effectively use keys stored in such a way and never reveal them.

In addition to on-board key generation, encryption, and software security, there is also physical device security, which provides many effective techniques for securing keys. When tamper-detection pins on a secure IC sense interruptions of specific signals between pins electronically connected to equipment access points, the IC reports a physical tamper event. Systems respond to tamper events as programmed. Actions range from logging the event to erasing secret keys, hence rendering the system inoperable, which is common in financial terminals, but generally not acceptable in smart grid. Protective meshes and temperature monitoring are other mechanisms for detecting efforts to decap a secure silicon device to retrieve secure keys. Meshes physically protect the top of a secure device from a probing attack. Temperature sensors detect events such as pouring of liquid nitrogen on a device to force the retrieval of a key from memory. Secure memory design also includes mechanisms for eliminating retention and imprinting of key data because of material stress over time.

Overall, storing keys in a secure IC instead of the general-purpose RAM of a connected device like a PLC provides the ultimate level of security for those keys.

## Cyber Attacks on the Rise

The real scenarios in this article represent the tip of the proverbial iceberg. In July 2012, the top U.S. military official responsible for defense against cyber attacks, General Keith B. Alexander, reported a 17-fold increase in cyber attacks against American infrastructure from 2009 to 2011.[9] GlobalData reported in September 2012 that the cyber security market in China will increase from $1.8 billion in 2011 to $50 billion in 2020.[10]

The smart grid is an undeniable trend. Countries and utilities are working to establish better control over

their electricity resources, shave peak demand, operate more efficiently, and accommodate massive amounts of distributed resources. The smart grid also becomes the major litmus test for future Internet networking of things, a proving ground for a network of millions of smart meters. Knowing all this, equipment and meter manufacturers must consider security as a critical, system-level requirement when developing smart grid devices. There is really no doubt that multilayered, life-cycle hardware and software security is the best solution for keeping smart grids operational.

## References


1. "Utility-Scale Smart Meter Deployments, Plans, & Proposals," **IEE Report**, May 2012, The Edison Foundation, The Institute for Electric Efficiency, www.edisonfoundation.net/iee/Documents/IEE_SmartMeterRollouts_0512.pdf.
2. Tweed, Katherine. "Smart Grid Italy: What to Watch," **GreenTechGrid**, August 10, 2011, www.greentechmedia.com/articles/read/smart-grid-italy-what-to-watch.
3. King, Chris. "Sweden at forefront of demand response in Europe," **eMeter**, August 17, 2010, www.emeter.com/smart-grid-watch/2010/sweden-at-forefront-of-demand-response-in-europe/.
4. "Iberdrola to deploy an additional one million smart meters in Spain," **Telecom Engine**, March 20,2012, www.telecomengine.com/article/iberdrola-deploy-additional-one-million-smart-meters-spain.
5. "FBI: Smart Meter Hacks Likely to Spread," **Krebs on Security**, http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/.
6. Tutorial 3675, "Protecting R&D Investment with Secure Authentication."
7. "Siemens software which control power plants vulnerable to hackers," **Homeland Security News Wire**, August 27, 2012, www.homelandsecuritynewswire.com/dr20120826-siemens-software-which-controls-power-plants-vulnerable-to-hackers.
8. "SIEMENS S7-1200 INSECURE STORAGE OF HTTPS CA CERTIFICATE," ICS-CERT ADVISORY, ICSA-12-263-0, September 19, 2012, http://ics-cert.us-cert.gov/pdf/ICSA-12-263-01-a.pdf.
9. Sanger, David E. and Schmitt, Eric. "Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure," **New York Times**, July 26, 2012, www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html?_r=3ref=fb&.
10. "China's Cyber-Attack Fears to Spark Massive Defense Spending," **GlobalData**, September 19, 2012, www.globaldata.com/PressReleaseDetails.aspx?PRID=368&Type=Industry&Title=Smart%20Grid.




| Related Parts | |
|---|---|
| MAX36025 | DeepCover Security Manager for Tamper-Reactive Cryptographic-Node Control with AES Encryption |
| MAX71637 | Single-Phase and Three-Phase Secure Energy Metering Microcontrollers |
| MAXQ1050 | DeepCover Secure Microcontroller with USB and |

**More Information**
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact