Keywords: security, authentication, encryption, asymmetric encryption, symmetric encryption, secure manufacturing, secure installation, smart meter, smart grid, metrology, AMI, AMR, RF, PLC, powerline communication

APPLICATION NOTE 5631

Ensuring the Complete Life-Cycle Security of Smart Meters

By: David Andeen, Strategic Segment Manager for Energy

Mar 05, 2014

Abstract: This application note explores the various potential points of attack in the life cycle of smart meters: during manufacturing, installation, operation, and post-installation. The application note then discusses real solutions to these security vulnerabilities, such as the use of secure bootloaders during manufacturing, metrology boards during installation, asymmetric encryption in the hardware rather than the software during operation, and possibly a cumulative attestation kernel (CAK) for forward-looking security. Maxim's ZEUS™ system-on-chip (SoC) is presented as a robust design solution for smart meter security.

A similar version of this article was published June 26, 2013 *Elektronik Journal*.

Introduction

The newest generation of smart meters performs far more in electrical networks than these devices did in their original communications role just a few years earlier. Today's smart meters are endpoints in large-scale, machine-to-machine networks—endpoints that extend to both smart grid infrastructure and to the vast array of future machines and devices that connect to the smart grid. In addition to protecting business and consumer data on an electricity grid, smart meters and their associated infrastructure monitor, control, and even protect the critical power infrastructure. Given this expanded role, smart meters introduce new and unprecedented security challenges for network administration. It is no surprise that basic encryption and passwords can no longer ensure the highest level of protection. Instead, smart meters now require complete life-cycle security from cradle to grave.

This application note explores the security threats faced by smart meters through their entire life cycle. It tracks a smart meter from manufacture, to installation and initial operation, and through its service life. Along the way, we identify security risks and solutions to those threats.

Urgent Need for Secure Smart Meters

Sound the alarm! Smart grid security has finally emerged as a critical social issue.

Just a few years ago, discussions of smart grid security focused on setting standards for privacy and the prevention of data theft. Today, conversations center on the real threat to society's power systems. Issues of cyber security, infrastructure threats such as Stuxnet, and organized hacks on electricity meters such as that in Puerto Rico[1, 2] frequently appear on the news wires and in mainstream television news media.[3] To provide requisite system security, many respected international organizations are working to establish guidelines and criteria, especially for automated metering infrastructure (AMI). In Europe, the German organization for the security of information technology, Bundesamt für Sicherheit in der Informationstechnik (BSI), released the protection profile for gateways in smart metering systems.[4] Similarly in North America, the National Institute of Standards and Technology (NIST) released the NISTIR 7268 specification, which provides guidelines for securing an AMI.[5]

To date, media attention has underscored issues involving smart meters and reflected widespread concerns. Nonetheless, the media do not provide solutions. BSI and NISTIR offer descriptions and guidelines on how a secure implementation should or could be architected, yet minimal implementations exist. In fact, industry today lacks many critical protective mechanisms that are essential for a secure system-wide smart meter implementation.

The threats to secure smart meters are varied and evolving. Consequently, there is no single, ultimate solution to security concerns involving electricity networks. Any robust smart meter security strategy must be equipped to deal with threats as they evolve. Potential issues start during the manufacture, assembly, and calibration of the meter's hardware, and continue through the meter's operational life, which most utilities expect to be 10 to 20 years. Hardware and software offer possible solutions at each step. Hardware is computationally faster and more physically secure, while software is more flexible. An optimal balance blends hardware and software security measures to protect the system's infrastructure. One such optimized smart meter solution already exists. Maxim's ZEUS™ smart meter system-on-chip (SoC) represents a state-of-the-art combination of hardware and software security for smart meter infrastructure. The ZEUS SoC serves as the primary design example in this article.

Securing Manufacturing

Smart grid security discussions often focus on encryption algorithms during operation. Encryption is admittedly an extremely valuable tool, yet it is only part of the solution.[6] Encryption protects data during operation, but it does not solve challenges faced during manufacturing and installation. In fact, the manufacturing supply chain is the first point of a potential attack.

As with most electronics companies, smart meter vendors primarily manufacture through contract partners, often in countries different from where design occurs. While safe and productive for most manufacturers, this process does expose manufacturers of secure devices to distinct external threats. Contract third parties gain deep access into system architecture, hardware, and software. Not surprising, therefore, the first tenet of secure manufacturing is a secure supply chain. Secure products like semiconductors must be purchased through trusted supply channels where authentication between the trusted supplier and the trusted OEM occurs. Authentication in the form of a secure hash challenge-and-response algorithm is the

most effective means of validating the supply chain.

The manufacturing process must allow system access and control only to trusted parties. This is where digital signatures and cryptographic algorithms come into play. The meter security breach reported in Puerto Rico occurred from tampering, possibly during the manufacturing process.[8] One very effective method of protecting a system during manufacturing is a secure bootloader. Let's take a closer look at this.

Using a secure bootloader, an OEM controls access to the smart meter controller during manufacturing. Code loaded during manufacturing is checked during boot up. Furthermore, that code is not executed unless it has been identified through an asymmetric cryptographic algorithm combined with a secure hash function. This process verifies that the code comes from a trusted source.[9] An industrial analogy is granting access to a company's computer network—only authorized personnel are allowed on the system (i.e., after authentication) and only those personnel can execute specific commands within the system (i.e., execute code that is cryptographically verified).

The benefits of a secure bootloader are invaluable. As described above, the secure bootloader integrates multiple layers of security. Without a secure bootloader in hardware, hackers might find a single weakness, such as an exposed key, and then penetrate the system. This is why operating a smart meter with the ZEUS SoC and its secure bootloader is so important today. Using this configuration for the smart meter, only authorized parties with the correct private keys and appropriate chain of trust can send messages, which ZEUS, and hence the smart meter, actually loads and executes.

Securing Installation

Depending on the quantity of meters, most utilities do not employ enough people to rapidly install the meters within an adequate period. Consequently, AMI installations typically require third-party contractors, which means that third parties, again, are handling the critical meter infrastructure. Physical hacking of optical ports, or simply rewiring meters, can occur during the installation process. Here is where secure metrology can validate an installation.

Many of today's meters feature a two-board architecture: a metrology board and a communications board (**Figure 1**).

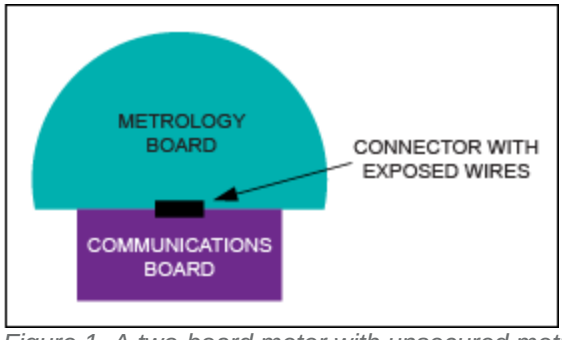

Figure 1. A two-board meter with unsecured metrology has data passing over exposed connector wires.

This architecture potentially runs the metrology data across open wires prior to encryption for communication, unless the metrology function provides security. An alternate approach is to use a single-board meter with secure functions, like a security envelope, on the metrology chip itself. Through on-chip

encryption in a separate metrology area, meter data can be encrypted immediately following measurement. This step closes any potential security gap from metrology to communication. Data received following the installation process can be trusted as valid. A utility can then compare post-installation data with meter reads from the old meter to ensure correctness. By placing encryption on the metrology chip, the ZEUS SoC closes the gap between metrology and communication (**Figure 2**); it does not offer a window for hackers to enter the network. Beyond installation, the security envelope ensures the integrity of meter data during the entire operational life of the meter.

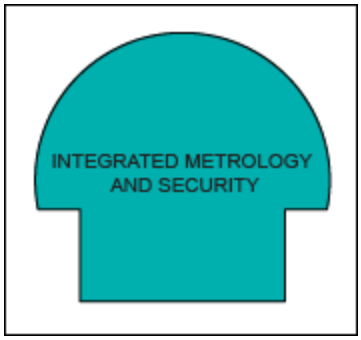

Figure 2. A single-board meter embeds secure functions on the metrology chip itself.

Securing Operation

Electricity meters, and soon smart meters, reside outside every business and residence, and often in physically insecure locations where hackers have ample time to study and explore them. Given the expanse of networks and the long operational life of meters, AMI smart meters are vulnerable to threats both in space and time.

Large Attack Surface

AMI installations have a large attack surface, meaning that there are multiple points for a potential attack on a smart meter. **Figure 3** shows a graphic representation of such a network, which generally consists of hundreds to thousands of meters communicating over powerline communication (PLC) or RF to concentrators. Concentrators communicate to the utilities through some form of backhaul, either over cellular or fiber infrastructures. In the link from meters to concentrators, meshing and/or forwarding of messages to and from meters enables the meters themselves to expand the network. This architecture keeps infrastructure costs down by reducing the number of concentrators relative to the number of meters. Mesh networking, however, increases the vulnerability of a network by creating an opportunity for the interception and alteration of communication between smart meters. This disruption is referred to as a “man in the middle” attack.

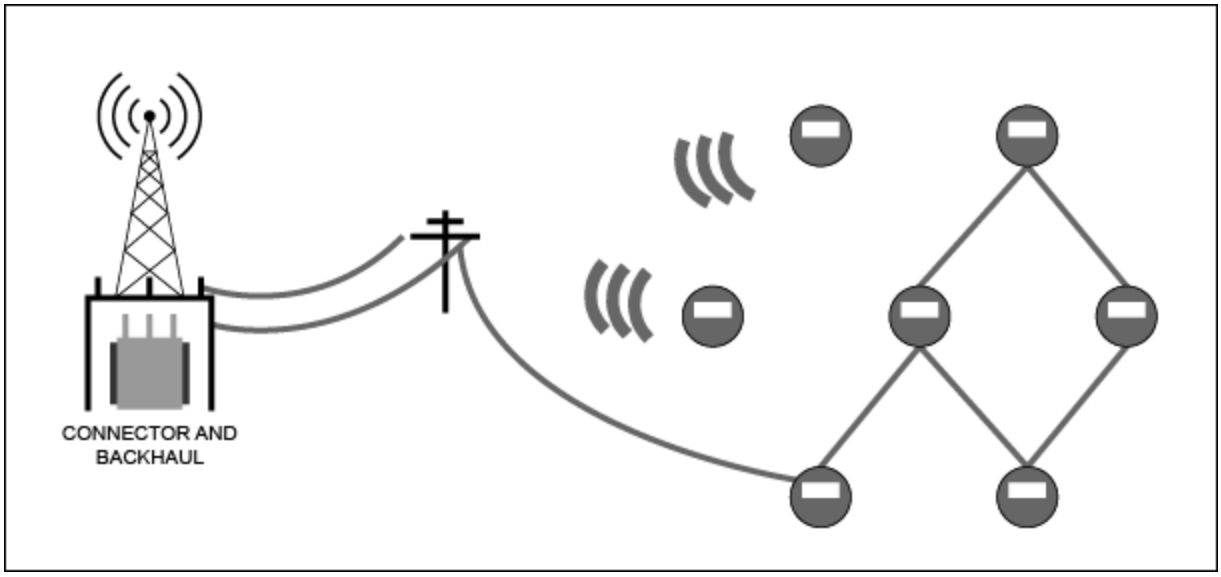

Figure 3. An AMI architecture has meters communicating by PLC or RF to a concentrator. Backhaul from the concentrator often occurs over the cellular network. Note that the ratio of meters to concentrators is greatly reduced in this graphic.

The smart meters themselves do not integrate the security features or computational power of the concentrators and other large networking equipment. This makes it theoretically easier to attack the meters than the concentrators or the network backhaul. Moreover, attacks on a mesh network can be leveraged over a large area, depending on the size of the mesh. Given that multiple communications occur meter to meter and outside the supervision of any additional network infrastructure, each single meter needs a strong level of individual security.

Equipping individual meters with security features means defining specifications that uniquely protect each one. AES and other symmetric encryption algorithms provide excellent security, but their drawback is that all meters share the same key. Consequently, any attacker who discovers the private key is able to attack all those meters. Instead, asymmetric encryption provides the best method to uniquely encrypt data because each meter uses a unique set of secure keys for encryption and decryption of data. Keys used for multiple secure events, such as authentication, should be generated on chip, stored on secure memory, and embedded in the secure product itself, thereby protecting the private key and never requiring that it leave the meter. By requiring unique key combinations for each meter, discovery of a private key allows access only to an individual meter. Thus, asymmetric encryption drastically reduces the “attack surface” of an AMI installation and significantly reduces the potential return on investment for an attacker. Simply put, it may no longer be worth an attacker’s time and effort.

But computation takes time and no one wants to slow down a time-sensitive system. Thus, the critical challenge with asymmetric encryption is the computation required for each individual meter. In this situation, hardware offers a significant benefit. Performing encryption and decryption functions in hardware, with the use of hardware accelerators, reduces the necessary computation time when compared to similar functions in software. Now system software resources spent encrypting and decrypting messages can be minimized, freeing up the system for other functions.

The ZEUS SoC integrates multiple layers of hardware asymmetric encryption along with secure key

generation and storage. To further bolster the asymmetric encryption, a true random number generator creates secure keys to prevent key generation from replay attacks. Multiple symmetric encryption algorithms like AES also provide layering of encryption with the above described asymmetric methods as well as compliance with any security standards that require such encryption.

Flexibility for Future Threats

Secure smart meters must be flexible enough to handle any security threats that evolve over the years following AMI installation. Consequently, the detection and disposition of threats during long-term operation is the next, difficult step to ensure the viability and security of the meter and the electricity network.

Utilities argue that costs and lack of mature solutions are major reasons why many current AMI installations do not feature intrusion-detection systems.[10] The issues for smart meter manufacturers distill down to a straightforward, but not-at-all-simple question: how much computational power must be embedded into a meter for threat detection? Various academic papers propose solutions that integrate meter-based and network-based threat detection solutions.[11, 12] One promising solution consists of a cumulative attestation kernel (CAK),[13] a meter-based algorithm that audits firmware revisions to provide another layer of detection when threats have breached the encryption and authentication process. A CAK can run on an 8-bit or 32-bit microcontroller and requires minimal memory. Experts, such as the Electric Power Research Institute,[14] agree that smart meters should contain some advanced functionality to provide security and accommodate future solutions.

It is a given today that security breaches require costly intervention. Consequently, the ongoing operation of a secure smart meter network involves more than threat detection and disposition. The issue is response. How a meter reacts to current and future threats affects the robustness, the effectiveness, and likely the financial success of an AMI installation.

Consider secure systems. Many secure systems, such as financial terminals, immediately shut down when hacked, thereby preventing the attacker from gaining any further access to the network. While inconvenient to be sure, the benefits of a shutdown outweigh the threat of losing secure financial information. In contrast, smart meters, which gate the only supply of electricity to a respective customer, must weigh the pros and cons of any response to a threat. An immediate shutdown to a perceived threat is not the optimal response. Instead, these networks must immediately assess the potential threat prior to issuing any response. In fact, the entire AMI must continue to operate in the environment of threats, while effectively gauging the severity of each respective threat. Most would agree that service interruption to a single customer would be considered less severe than large-scale disruption or pervasive abuse of the entire communication infrastructure. Given that large-scale cyber attacks pose the greatest threat to AMI, smart meters need the ability to prioritize defensive responses during any time of operation.

A smart meter must also provide this robust hardware security, defuse threats, and accommodate future software solutions without extensive system upgrades. The ZEUS SoC architecture includes a 32-bit ARM® core. Any communication that does not properly decrypt or authenticate can be ignored, logged, or reported at the discretion of the meter and network architects. Separation of metrology from the ARM core ensures that meter functions continue uninterrupted during various software routines. This operation is in solid compliance with WELMEC[15] and other standards that require separation of metrology and/or metrology software from nonmetrology software and applications. Furthermore, the hardware security

described earlier ensures the quickest handling of communication while freeing the ARM core to perform system tasks. The ARM core may also be equipped with tomorrow's solutions, such as a CAK, which would layer on top of the already secure system. Computational power and hardware security, combined with appropriate software upgrades to improve system security against evolving threats, provide a highly effective system security solution that maintains a proper balance of hardware and software features.

A Future of Opportunity

The smart grid represents an amazing transformation of the twentieth-century electricity grid. But when we added network and control functionality to such a vast system, we greatly increased its exposure and vulnerability to security attacks and, most importantly, cyber threats. International organizations are defining performance standards and the news media is reporting grid advances and security breaches. But it lies with the manufacturers of smart meters to defend against the security attacks. A proactive approach for smart meters is separating the hardware and software functions; it is securing the entire life cycle of the smart meter, from purchase of third-party components to manufacturing, installation, and long-term operation. With this understanding of smart meters and the evolving electricity industry, Maxim Integrated designed the ZEUS SoC to be the advanced, elegant solution for today's and tomorrow's smart meters.

References

1. "FBI: Smart Meter Hacks Likely to Spread," Krebs on Security, April 2012, http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/.
2. Tutorial 5445, "Stuxnet and Other Things that Go Bump in the Night."
3. "Senators Aim To Protect Electric Grid From Hackers," CBS News, April 30, 2012, www.cbsnews.com/8301-503544_162-4981641-503544.html.
4. "Protection Profile for the Gateway of a Smart Metering System," Bundesamt für Sicherheit in der Informationstechnik, Gateway PP v01.01.01 (final draft), 2011.
5. "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security" and "Guidelines for Smart Grid Cyber Security," volumes 1-3, The Smart Grid Interoperability Panel—Cyber Security Working Group, National Institute of Standards and Technology, U.S. Department of Commerce, September and August 2010, http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf.
6. Tutorial 5486, "Securing the Life Cycle of the Smart Grid."
7. Tutorial 3675, "Protecting R&D Investment with Secure Authentication."
8. See notes 1 and 2.
9. See note 7.
10. "Intrusion Detection System for Advanced Metering Infrastructure," Electric Power Research Institute, December 31, 2012, www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001026553.
11. Michael LeMay and Carl A. Gunter, "Cumulative Attestation Kernels for Embedded Systems," IEEE Transactions on Smart Grid, vol. 3, no. 2, June 2012, http://seclab.web.cs.illinois.edu/wp-content/uploads/2011/03/LeMayG09-esorics.pdf.
12. Stephen McLaughlin, Brett Holbert, Saman Zonouz, and Robin Berthier, "AMIDS: A Multi-Sensor Energy Theft Detection Framework for Advanced Metering Infrastructure," paper presented at the

IEEE Third International Conference on Smart Grid Communications (SmartGridComm), in Tainan City, Taiwan, Nov. 5-8, 2012, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6486009&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel7%2F6479749%2F6485945%2F06486009.pdf%3Farnumber%3D6486009.

13. See note 11.
14. See note 10.
15. "Software Guide (Measuring Instruments Directive 2004/22/EC)," WELMEC Working Group 7, March 2012, Issue 5, www.welmec.org/fileadmin/user_files/publications/WELMEC_07.02_Issue5_SW_2012-03-19.pdf.

The author would like to thank his colleagues Ben Smith, Christophe Tremlet, and Gregory Guez for their technical contributions to this article.

Related Parts		
MAX32590	DeepCover Secure Microcontroller with ARM926EJ-S Processor Core	Free Samples
MAX71637	Single-Phase and Three-Phase Secure Energy Metering Microcontrollers	
MAXQ1050	DeepCover Secure Microcontroller with USB and Hardware Cryptography	

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

Application Note 5631: http://www.maximintegrated.com/an5631
APPLICATION NOTE 5631, AN5631, AN 5631, APP5631, Appnote5631, Appnote 5631