Keywords: smart, grid, meter, attacks, electricity, utilities, cyber, terrorists, hackers, chip, SoC, manufacturer

APPLICATION NOTE 5926

BATTLING THREATS IN THE SMART GRID SUPPLY CHAIN

By: Kris Ardis, Executive Director for Energy Products

Abstract: Security in the smart grid gets a lot of attention, but usually the discussion focuses on encryption of data. To truly secure the grid, we need to consider threats that are present even before a smart meter or other device is deployed. This article shares many examples of potential threats in the smart grid space, in particular threats that can appear when we consider the life cycle and supply chain of a smart meter. We also discuss tools available today to help combat those threats.

Security in the smart grid. This topic is getting a lot of attention from governments, utilities, and even consumers. The attention is warranted. Besides air, water, food, and shelter, electricity has become one of mankind's most fundamental necessities. The reliable flow of electricity is certainly crucial to life in the industrialized world, and is a key factor in facilitating the development of emerging countries.

The prevalent discussion on security in the smart grid tends to focus on cyber security, in this case, the ability of embedded devices to join networks and transact data over networks in an authenticated way. While this is a critical step in securing the supply of power to the world in a smart grid environment, this approach is too narrow. It ignores the threats to the smart grid from throughout the life cycle and supply chain of smart grid equipment.

In this article we will explore some threats to the smart grid that are ever present in the supply chain of a smart meter. We will explain why those threats must be considered and remedied to ensure the cyber security of the grid. Finally, we will assess the technologies available to combat these threats.

Why Threaten the Grid?

Why would anyone want to attack a smart meter? The answers vary.

In perhaps the simplest scenario, an attacker might want to lower their own electricity bill. This objective is selfish—attackers want to change the behavior of their smart meter to protect their own interests. In some cases, it could be organized criminal activity that wants to hide true consumption data (a common case is drug laboratories trying to disguise their consumption). But what about attackers who deal at a more ideological level?

It is no secret that many countries must handle the threat of terrorist attacks, perhaps even daily. While threats like bombs or airplane attacks are certainly scary, attacks against the electrical delivery grid could, in fact, be far more effective at disrupting the quality of life for a large number of people. An attacker who takes control of a few million meters could launch a very substantial public assault by disrupting the flow of electricity to a huge population.

Physical Threats During the Smart Meter's Life Cycle

Figure 1 shows at a conceptual level the various stages in the life cycle of a smart meter. For simplicity, this model has been limited to four steps: the procurement of silicon, the manufacturing of the smart meter, the deployment of the smart meter, and the smart meter in mission mode. This simple model lets us create a threat analysis. For each stage (including the transition or shipment between stages) we ask ourselves, what are the ways that an attacker might try to take control of a smart metering network?

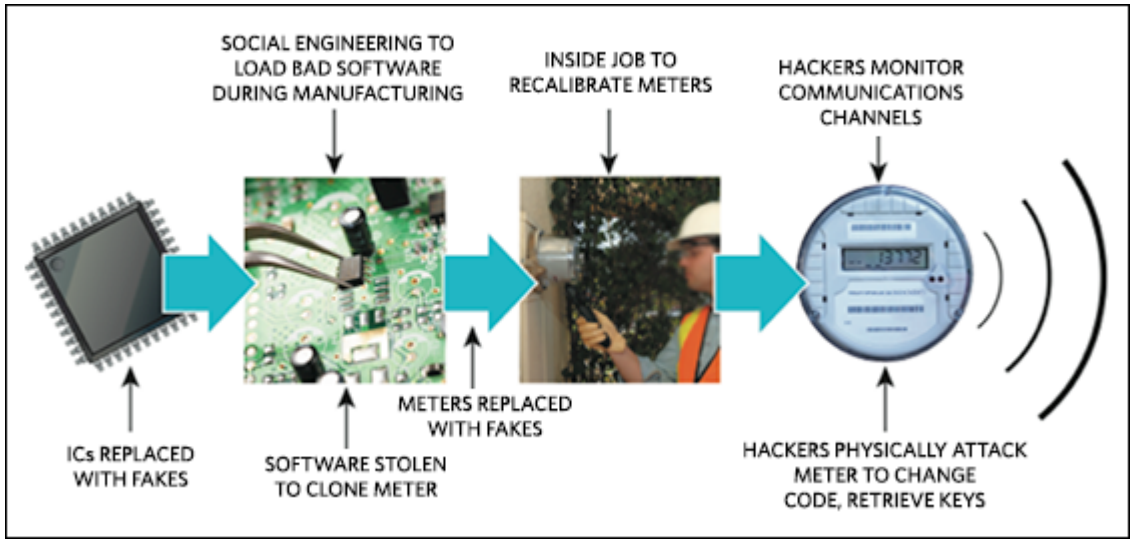

Figure 1. A simplified model of threats to the life cycle of smart meters. As you can see, encryption of communication alone will not protect us.

Replace Legitimate ICs with Fakes

Transit between a silicon manufacturer and equipment manufacturers presents an excellent opportunity for attackers to inject problems into the smart meter supply chain. Microcontrollers are the "juiciest" targets for attackers. In normal supply-chain models, a silicon manufacturer will ship a flash-based microcontroller to a manufacturing house, whether a contract manufacturer (CM) or the end customer. At the manufacturing site, the smart meter firmware is loaded into the microcontroller. Some system-level configuration occurs before the meter manufacturing is complete and a smart meter is boxed. This is how the process is supposed to proceed.

Now imagine a sophisticated attacker who designs and manufactures a microcontroller that looks and acts very much like a genuine metering system on a chip (SoC). There are multiple scenarios possible now. This IC could be altered to allow a cyber terrorist to remotely assume control of a meter over a network connection. Or, the fake SoC could be designed to dump its memory contents to any request, thereby divulging secret communications keys loaded during manufacturing. Or, the fake SoC could allow its software to be inspected by anyone, thereby threatening the IP of the legitimate meter manufacturer.

There are other less sophisticated attackers. A "fake IC " does not need to be manufactured. Imagine an authentic flash microcontroller being shipped to a CM. An attacker intercepts the shipment and loads a program in the flash that looks very much like the normal boot loader built into the system. When the IC arrives at the CM, the deception (i.e., the fake bootloader) might be difficult to detect. The CM then downloads the normal firmware, but the “insecure” bootloader has created a resident virus in the meter. Later this virus could cause the meter to function incorrectly and share secret encryption keys with an attacker.

Without appropriate protections, an attacker who fakes or tampers with an IC shipment can control the entire life cycle of a smart meter, opening up any imaginable problem on the smart grid.

Use Social Engineering to Load Bad Software During Manufacturing

Threats exist on the manufacturing floor as well, with the most tangible threat in the workforce running the manufacturing operations. Typically, these workers earn far lower wages than the engineering teams or managers. Imagine a poor economy where a $100 bribe will convince a manufacturing line worker to load special firmware into a batch of smart meters. In more wealthy nations, if $100 does not work perhaps $1,000 or $10,000 will?

If an attacker gains access to the manufacturing flow, they can potentially steal the binary code images intended to be loaded onto the smart meter. It would not be too difficult to take that image and alter the firmware to cause unintended behavior. For example, an attacker alters an interrupt vector so that it causes undesirable behavior in rare, carefully defined situations. The interrupt vector could be programmed to monitor a real-time clock, waiting until a specific time in the summer when it will open the meter’s disconnect relay and stall the processor to take the meter off the network. Under such an attack millions of meters might stop the flow of electricity to residential consumers. The economic costs would be staggering if the utility were forced to manually replace the smart meters. The cost in human life could be higher, considering the threats from a disruption of service during the heat of summer.

Steal Software to Clone a Meter

Let's consider an attack based on economics and not terrorism. In normal manufacturing flows, the binary image loaded into a smart meter is readily available to the workers on the line. With a modest bribe (i.e., a social engineering expense) the attacker gains access to raw PCBs for reverse engineering. Now this attacker has the complete BOM with identified IC part numbers and the software needed to run the smart meter. This is everything needed to clone a meter. The attacker can sell the meter design without the R&D costs for that meter.

Once an attacker can clone a meter, they are also a potential threat to alter the software deployed in a meter, as described above.

Replace Legitimate Meters with Fakes

The plastics and markings on meters are far easier to duplicate than the functionality of a piece of silicon. In this scenario, an attacker manufactures a meter that visually resembles a legitimate meter, but the firmware contains a hidden attack. The planned attack could be economic, for the meter might be calibrated to incorrectly report on the amount of energy consumed. It might even be catastrophic if the meter allows an attacker to take control of its disconnect or to control the data reported back to the utility. An attack on a single meter is an inconvenience, but not a disaster. However, any attack against a quantity of meters can be infinitely more damaging. Imagine six million meters reporting the incorrect amount of electricity consumed. The utility would be working from incorrect data, hampering its ability to respond to changes in demand and generate the correct amount of power. Widespread grid instability and a massive loss of productivity are inevitable.

Recalibrate Meters with Insider Access

Once a legitimate meter is deployed in the field, the attack threats do not cease. Imagine an attacker who works for the meter manufacturer and knows how to build an IR device that can communicate with a meter and change its calibration data. Such a device would be easy to manufacture and could alter any meter to underreport the amount of electricity consumed. While this might not cause a widespread failure of the grid, it could cause severe economic damage to the utility.

The attack described here is not theoretical. In fact, it was done already.[1]

Monitor and Hack Communication Channels

This is the attack that the smart community is worried about! The fundamental issue is that the communication network around a smart meter could be hijacked to emulate commands to open its disconnect relay and, thus, disrupt service to a consumer. Alternatively, meter communication might be faked to report erroneous usage data. Utilities then might use this flawed smart-meter consumption data to make decisions about the amount of generation capacity needed or about volt/var optimization. If the data and commands here are not properly encrypted (hidden) and authenticated (validated), it provides an avenue for an attacker to influence or even control the smart grid.

Physically Attack a Meter to Change Code, Retrieve Keys

Once a meter is deployed, how secure is it really? The physical security of a meter is a critical consideration. The embedded endpoints of the smart grid (e.g., smart meters, grid sensors, distribution automation control points) are necessarily distributed and not protected by any physical means. Consequently, the endpoints of the smart grid are susceptible because they can easily be stolen, taken to a lab, and inspected at the leisure of an attacker.

In this scenario an attacker opens the meter, accesses the programming pins of the meter microcontroller, and loads new firmware to report incorrect usage data. Another attacker physically accesses the meter, then takes control of the internal memory of the meter microcontroller, and eventually dumps the secret communication keys. In these dangerous situations the attacker can decipher the smart grid's network communications and initiate a wide range of disruptive actions.

How the Life Cycle Threatens Cyber Security

We have been talking about physical threats to the smart meter life cycle. Let's turn now and talk about cryptographic threats to grid communications.

The smart-grid community is working very hard to ensure that the communications in the smart grid (i.e.,

data and commands) are secured and authenticated. Modern smart-meter standards are asking for AES encryption, if not elliptic curve techniques as well. These powerful algorithms can protect and validate data for decades, and are far more complex than the abilities of computing power to decipher within the next few decades.

In this case what is the threat? The commands and data in the smart grid network are cryptographically protected, and the algorithms used cannot be broken with raw processing power for a number of years, or well after we all plan to be in different careers or retired! Now the concern is not with the cryptographic protection on the data and commands. Instead, the potential weak, vulnerable entré for an attacker is the protection of the key material, the cryptographic secrets.

An attacker will take every opportunity to access key material (encryption keys), and target the lowest risk/cost options. Sniffing communication traffic and brute-force decryption could take decades, so the cost is high. But what about the cost of infiltrating a contract manufacturer in a foreign country to intercept secret keys loaded during the manufacturing cycle? Would this be a lower cost or lower risk option?

Looking back at each of the threat scenarios discussed above, an attacker could take advantage of each situation to compromise secret encryption keys. That would most definitely break the cyber security so carefully designed and implemented in the smart meter network:

Replace Legitimate ICs with Fakes

In this case, an attacker programs the fake or intercepted ICs to share memory contents with any other attacker. Secret keys loaded during the manufacturing cycle would be easily compromised since the fake (or intercepted) ICs could be programmed to share such data.

Succumb to Social Engineering and Load Bad Software During Manufacturing

If secret keys are programmed in the manufacturing environment, then social engineering approaches (e.g., bribes or other gifts) could be used to convince line workers to share the secret keys loaded during the process.

Steal Software to Clone a Meter

If an attacker could rebuild the software that was to be loaded on a smart meter, they could structure the software to share—instead of protect—secret encryption keys.

Replace Legitimate Meters with Fakes

Fake meters could be programmed to share secret encryption keys with any adversary. If a backdoor was programmed into the fake meter, it could compromise any secrets loaded on a legitimate meter during the manufacturing process.

Recalibrate Meters with Insider Access

To date publicized attacks to recalibrate meters have been for individual gain, i.e., lowering an individual's electricity bill. A savvy insider could also program a backdoor into the production meter that would enable mass recalibration of meters. The resulting massive data inaccuracies across the grid could lead to bad decisions at the utility and to grid instability.

Monitor and Hack Communication Channels

Hacking communication channels is the traditional attack that cyber security analysts consider. Modern cryptographic techniques can sufficiently stifle any assault, as long as the attacker has no opportunity to access cryptographic keying material.

Launch Physical Attacks on a Meter to Change Code, Retrieve Keys

Many microcontrollers contain a means to dump the program code or data memory in a bootloader situation. Many products also support test mode. While these modes might be hidden, access to them can be discovered by a determined attacker who then gains access to any internal memory in the meter microcontroller. If the keying material is stored in on-chip memories, then it is vulnerable, and physical access to the meter is only a small step away from physically accessing the memory contents inside the meter microcontroller.

Combating Threats to the Smart Meter Life Cycle

So far we have outlined security threats to the smart meter and to its security software. While the above examples cannot be considered exhaustive, these threats are real indeed. They prove that anyone or any agency deploying an embedded smart grid device must analyze and anticipate any potential threats to the grid itself. Therefore, it is important for us to consider the technology available to combat these identified threats.

Ensure Legitimate ICs with No Fakes

We must be certain that silicon delivered to a manufacturing plant is legitimate, unaltered, and not substituted with fake materials. Procedural controls are our first line of defense. We must enforce legitimate supply chains. Only purchase components directly from the original supplier or from authorized supply chains. The risk here is procuring materials from third parties or brokers who are not subject to rigorous tracking procedures that verify legitimate, untampered material.

While these procedural controls can be effective, they will not stop a truly determined attacker with the considerable resources to replace legitimate material with convincing fakes. In this case, a secure bootloader can deter the attack. A secure bootloader, loaded into the appropriate silicon during manufacturing, can be locked through advanced encryption techniques like a shared AES key or with the private key of the silicon manufacturer. When the meter manufacturer receives the silicon, they can then use those same advanced cryptographic tools to ensure that the silicon was securely locked by the silicon manufacturer.

Thwart Social Engineering and Load Only Authentic Software During Manufacturing

Once again, procedural controls can help here. For example, requiring two or more random line workers to “validate” the firmware that is being loaded can help deter attacks.

Procedural controls can help, but advanced security techniques built into the silicon provide the most robust solution. The secure bootloader highlighted above can let a meter manufacturer deliver encrypted, digitally signed code into the meter. In fact, the contract manufacturer or manufacturing site might only have access to the encrypted version of the application software. The secure bootloader on the metering IC safely decrypts and stores the plain version of the software internally. This process prevents attackers from stealing the firmware for cloning or reverse engineering a meter since it is never available in plaintext between the meter designer and the meter itself. It also can stop an attacker from introducing new firmware into the manufacturing chain, because any firmware loaded onto the metering IC would need to be signed

and encrypted by an authorized person.

Safeguard Software to Prevent Cloning Meters

Using this same secure bootloader, the manufacturing site only needs to store an encrypted version of the application software. Now any attacker who steals the encrypted software cannot reverse engineer it. Meanwhile, the secret key programmed into the secure bootloader is specific to meters produced by each authorized end-meter manufacturer. Consequently, encrypted software has little value to an attacker attempting to clone meters. To clone a meter, an attacker would need to steal ICs destined for a particular end customer, since no other silicon would be preprogrammed with the appropriate secret key.

Validate Legitimate Meters and Prevent Fakes

Recall the attack that tried to create a convincing fake meter to be programmed with bad software designed to disrupt the smart grid. Again a secure bootloader will assure the end customer (i.e., the utility) that the meter is loaded with the correct, validated firmware. In addition, the bootloader can “lock” the meter, disabling its ability to function until received by the intended utility.

Prevent Insider Access to All Entry Points in a Meter

To prevent knowledgeable insiders from reprogramming or recalibrating meters, the meter designers need to “lock down” (cryptographically speaking) all possible entry points to the meter. The entry points receiving the most attention are the home and utility networks, although there are other access points that get less attention (yet need to be considered) including serial ports, infrared interfaces, and JTAG or other debugging ports.

These latter entry points must have secure protection to guarantee that anyone attempting to take control through these peripherals is authenticated cryptographically. For example, most meters have infrared access points so utility workers can read local meter information. Sometimes the utility worker can issue commands through those ports. If this communication is not encrypted and authenticated, the smart meter is vulnerable to attack. It is not enough to have a secret or unpublished command set. A determined attacker can initiate random commands, monitor the meter’s behavior, and eventually map out the command set understood through the IR port. A less technologically savvy attacker might bribe a utility worker to get the command set, or access to the tools used to communicate with the IR port.

Secure Communication Channels with Data Encryption

Monitoring and hacking communication channels are the threats receiving the most attention today from utilities, government, and industry. This is a primary focus for anyone responsible for cyber security. Here we are concerned with two topics: hiding data to protect sensitive/private information, and authenticating data/commands to assure validity. Cryptographic tools can be used for both tasks.

Data and command authentication is typically implemented with signatures. Note that for authentication, we might not be concerned about data secrecy. It might actually be acceptable for the data or command to be publicly readable. But it is essential that you have strong assurance that the data or command is valid.

Hiding data is typically implemented through symmetric encryption (i.e., a shared secret key) schemes such as AES. This algorithm is relatively fast when implemented in software, but often requires hardware acceleration if a large stream of data needs to be encrypted. An example would be a firmware update, where a long stream of data must be received and potentially encrypted (or hashed) before the processor can proceed to install the new revision. AES key sizes range from 128 to 256, with longer key sizes

stronger and thus harder for an attacker to break. Note that as a symmetric algorithm, AES requires that both the sender and the receiver of data have the same encryption key.

There is increasing interest in using asymmetric schemes where the “signer” has two keys: one shared key (public) and one secret key (private). The keys essentially undo the operation of the other. In simple terms, the signer uses their private key on a piece of data to generate a signature; everyone can validate that the signature came from the signer because they know his/her public key and use it to reverse the operation. Elliptic curve techniques are gaining interest for the smart grid (ECC, ECDSA) because of the small key sizes (256 bits instead of 4096 bits needed for algorithms such as RSA) and high level of security.

Launch Physical Attacks on a Meter to Change Code, Retrieve Keys

While cyber security—the encryption of communication channels in smart metering—gets a lot of attention, it is not the only security concern of a meter while deployed. A smart meter is fundamentally in a high-risk area; it is not physically protected or monitored. A technologically advanced attacker’s best route to analyze a smart meter is to procure one and spend significant time with the meter. Since meters exist on every house, it is very easy and very low risk for an attacker to acquire meters and bring them to a hidden lab for analysis.

The best protection to these threats comes from the financial terminal industry. In that industry, silicon for financial terminals integrate sensors that actively monitor physical threats (such as device intrusions, threatening temperature and voltage conditions, and even chip-level physical inspection) and erase secret keys stored in NVSRAM in the event of any detected attack. This technology can ensure that any physical attack on the meter results both in a permanent disabling of the meter and the erasure of any critically sensitive information, including security keys.

Secure Technology Embedded in the Smart Grid

The scenarios presented here have outlined a host of security threats and the technologies to thwart those threats.

Now this technology is available commercially. For years, Maxim Integrated has provided security solutions to the financial terminal and credit card industries, solutions that are trusted worldwide. The security of financial transactions is extremely high, while the successful growth of that industry is the foundation of the modern growth of electronic commerce. And it is this high level of security that creates the demand for the embedded silicon that we have been discussing.

Threats to the smart grid are potentially far more damaging than threats to the financial terminal industry. Who would argue that the widespread and prolonged loss of electricity would be far more damaging than the inability to process card transactions? Maxim Integrated is responding with secure products, such as the MAX71637 energy-measurement SoC, that integrate the highest level of security technology. Now you can secure the entire life cycle of smart-grid equipment, from design to manufacturing, to mission mode, to the end of the device’s useful life. This is really the only way that utilities and consumers will capitalize on the many benefits of the smart grid.

Reference

1. You can read about this attack and other assaults on the grid in application note 5537, “Smart Grid Security: Recent History Demonstrates the Dire Need,” February 11, 2013.

Related Parts		
MAX36025	DeepCover Security Manager for Tamper-Reactive Cryptographic-Node Control with AES Encryption	
MAX71617	Energy Measurement SoCs	Free Samples
MAX71637	Energy Measurement SoCs	Free Samples
MAXQ1050	DeepCover Secure Microcontroller with USB and Hardware Cryptography	

More Information

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

Application Note 5926: http://www.maximintegrated.com/en/an5926
APPLICATION NOTE 5926, AN5926, AN 5926, APP5926, Appnote5926, Appnote 5926