Keywords: smart grid, smart meters, ansi, ieec, power meter, concentrator, grid security, electric utility, stuxnet, cyber security, grid attack, power company

APPLICATION NOTE 5337

Securing the Smart Meter

By: Kris Ardis
Feb 24, 2012

Abstract: This article will discuss various techniques to increase the security of the endpoints in the smart grid—meters and sensors that are dispersed far away from the watchful eyes of the utilities. Conventional attacks such as physical and logical attacks on the smart meter will be considered, as well as more coordinated attacks that might infiltrate the supply chain, causing utilities to deploy compromised meters. The technology to address these attacks exists today, has been used successfully for years in the financial payment-processing industry, and can readily be applied to the smart grid.

As the nations of the world race to implement smarter electricity-delivery systems, how to secure those systems is an important topic. Despite the fact that few standards exist for smart grid security, many utilities have proceeded with their rollouts—deploying IT systems to collect and analyze data, communication infrastructure to deliver data, and endpoints like smart meters and grid health monitoring systems to produce the raw data. While security has been a concern for the last several years, there is still much work to be done, especially to protect the "endpoints" like meters and grid sensors. This article gives an overview of some threats against those endpoints and the technology that can be used to mitigate those threats.

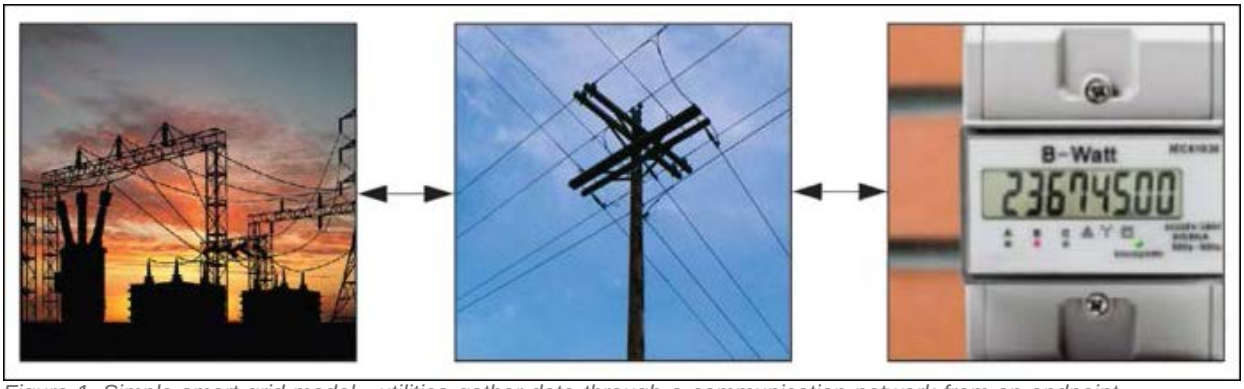

Figure 1. Simple smart grid model—utilities gather data through a communication network from an endpoint.

The Threats

Certainly there are many, but most threats to the smart grid can fall into one of two large categories. The first category is an individual threat. In this case, the attacker aims to manipulate smart grid data for his/her own gain—perhaps to lower an electricity bill, or to hide an illegal drug manufacturing operation. An individual threat does not seek to disrupt the management of the electrical grid for others, but only to improve the position of an individual or group.

The second category is a societal threat, and includes activities that try to harm the operation of the electrical grid. This might be an attack on the utility itself (massive underreporting of energy consumption by the whole grid could

cause financial strain on the utility) or at society in general, the extreme example of which is a terrorist attack that leaves the electrical grid inoperable and customers without power. Without electricity, productivity and financial losses would be staggering, and in environments of extreme heat and cold there is a very real threat to human life.

The Weakest Link

An attacker would look at the entire grid and try to determine the best place to attack: where an attack yields the desired result with the least amount of investment and risk to the attacker. Let us return to our simple "utility-to-endpoint" model for both threat scenarios to see how an attacker might achieve his goals.

1. Individual threat: Using the example of the hacker who wants to lower his electricity bill, the attacker could achieve his goal by infiltrating the utility control room and changing the records collected from his meter. He could also intercept the communication that relays consumption information to the utility. Or, he could alter the firmware on his meter to underreport the amount of power consumed.
2. Societal threat: Using the example of a terrorist who wants to disrupt the flow of electricity to the maximum number of users, the attacker could infiltrate the utility control room and order the remote disconnect of a number of meters or shut down the supply of electricity at certain substations. The attacker could also inject instructions onto the communication bus to issue commands to do the same. Or, the attacker could take control of meters and program them directly to activate their remote disconnect relays, or take control of sensors to feed false data to the utility, leading them to believe they need to shut down certain segments of the grid.

We can see that with our simple model, there is a path where both types of threat can be realized against any of the major portions of the grid (Utility Control, Communication Network, Endpoint). While it may be true that security improvements could benefit all three segments, a practical process demands that we identify and address the weakest link. This is what our adversaries will do—look for the easiest entry point to achieve their goals, the weakest link in the smart grid.

Consider how an attacker is likely to see the three major segments today. A successful attack against a utility control room would yield the highest amount of control over the grid; however, it is a high-risk attack. Utility control rooms are sure to be well protected, with good access control and concurrent authentication procedures in place. It will also be extremely difficult to hide the attack—if control room personnel do not catch the offender, security cameras will record it. While it is true that an inside threat could be effective in a utility control room, there are procedures that many utilities use to prevent any one person from having authority to make changes that could threaten the operation of the electrical grid. Multiple people would be required to consent to any such action, meaning that the attacker must have multiple people "inside."

So where does the attacker look next? The communication channel. To date, most of the dialog on smart grid security has focused on the communication channel, and most systems deployed today use strong cryptographic technology to protect the data and commands while in transit between smart grid endpoints and the utility command centers. To successfully attack the communication channel, one needs to discover the secret encryption or authentication keys. Reliable, publicly known communication protocols will not share the secret keys, meaning an attacker needs to either (1) discover the secret keys from the utility or from the endpoint or (2) brute force attack the encryption/authentication scheme of the channel. Note that option 1 is actually not an attack on the channel itself, but an attack on the other major components of the grid. A brute force attack (option 2) is not likely to yield results either. Common encryption algorithms like AES-128 are computationally infeasible to attack in a brute force manner, meaning it would take years (or decades) for super-fast computers to guess the correct secret key data, long after the useful life of the data.

The attackers then turn to the smart grid endpoints themselves: devices like smart meters or grid health sensors. This type of equipment is immediately more appealing because the endpoints are not well guarded, they are widely dispersed on the sides of houses, or they are attached to remote transmission wires. We can include devices like data concentrators in this category since they are often unprotected as well. This vulnerability gives an attacker more opportunity to study and try different attacks. It is true that these endpoints will be energized, possibly difficult to reach (on a tall transmission line for example), and potentially harmful. However, attackers can exercise some level of caution to prevent personal injury. On the surface, endpoints like meters seem to be the most accessible to attackers. But how would an adversary carry out his attack?

Attacking a Deployed Meter

The following arguments apply for any endpoint in the smart grid with communication capability, but for the purposes of discussion, let us consider the smart meter.

With the individual threats, the attacker would do best to attack the meter directly. His goal might be to change the current-sensing mechanism to make it appear that less power is being consumed, or to reverse-engineer the software in the meter and alter the reported power usage.

The societal attack might start in a similar way: an attacker studying a meter to try to understand how it functions. His goal would be more advanced. He might want to extract cryptographic keys, reverse-engineer the communication protocol, and reprogram the meter. If an attack was repeatable, he could reprogram a large number of meters to underreport power consumption or simultaneously disconnect on a given date and time.

In the face of such threats, what can be done to secure the endpoints of the smart grid? Embedded security technology from markets such as financial transactions and government applications can do an excellent job countering these attacks on individual meters. This security technology integrates a means to deter both physical attacks that aim to forcibly control or inspect an embedded system and logical attacks that aim to analyze the memory, applications, or protocols running on an embedded system.

Embedded products with physical attack-detection mechanisms detect when a system becomes compromised. These products make use of physical sensors like case open switches, blind switches, motion detectors, and environmental sensors to detect attacks. When a threat is detected, the meter can take action, such as trying to contact the utility or even deleting secret cryptographic keys (it may be better to delete those keys than expose them to an attacker).

There are also logical techniques that apply to attacks on deployed meters. Secure on-chip memories can be locked and encrypted so that an attacker has difficulty reading or reverse-engineering the software. Secure bootloaders can lock the device at manufacturing time to make sure an attacker cannot load an unauthorized version of software on the meter.

Techniques to secure deployed meters can also mitigate the societal threat to some extent. Meters with unique encryption keys make sure that if an attacker can extract one meter's key, the attacker cannot know the next meter's key. If extraction of a single secret key is difficult enough (with the physical and logical protections just mentioned), it increases the challenge of a societal threat carried out against a large number of deployed meters.

Attacking the Supply Chain

A handful of existing embedded security technologies can be implemented to mitigate the dangerous societal threat against deployed meters and the smart grid. However, we must consider attacks beyond those against deployed meters and focus on the entire life cycle.

The manufacturing environment is one of the most risky places for intellectual property, whether you consider the conventional threat of theft from off-shore manufacturing, or the fact that your on-shore (or even on-site!) manufacturing is operated by low-paid technicians susceptible to social engineering. In this environment, your IP can be stolen for reverse-engineering study, or new and dangerous IP could even be deployed on your products.

A determined attacker could reverse-engineer a meter's software and install a virus to activate the remote disconnect, shut down the meter's communication, and erase all of its internal memory at a set date and time. The attacker then substitutes this IP in the manufacturing flow. The effect would be devastating—a utility rollout of millions of meters, all of which cut off customer electricity at a given time. Meters would need to be individually serviced or replaced over a course of weeks or months, and at great expense.

Embedded security products can mitigate these threats with features like secure bootloaders, secure memory, and life-cycle management. A secure bootloader can be used to load only encrypted versions of meter software, a meter designer or software provider can send the encrypted application to the manufacturing location, and the secure

bootloader in the system microcontroller can decrypt and store the application. Secure memories (internal or external) can also store application code in encrypted form, making it infeasible to read the application contents and reverse engineer or copy it. Secure life-cycle features can be used to validate the actual supply chain. Silicon manufacturers can lock their devices so that only one customer can unlock it and install code, and a meter OEM can lock its meter so that only the intended utility can unlock and deploy it. As more security is added to the supply chain, the threat of societal attacks exploited through the meter is lessened.

The Solution?

There will be no perfect security solution for the smart grid. Perfect security costs an infinite amount of time and money to develop. However, a vast number of techniques and technologies exist from the world of financial transactions and government applications to help enable a higher level of physical and logical security in the embedded endpoints of the smart grid.

The threats, attacks, and mitigations presented here are in no way a complete analysis of security holes in the smart grid, but are intended in this short space to argue that embedded endpoints like meters need serious consideration when looking at smart grid threats. Once meters and other endpoints are protected with multiple layers of secure mechanisms, the attackers will have to focus their efforts elsewhere.

Related Parts		
71M6541D	Energy Meter ICs	Free Samples
71M6541F	Energy Meter ICs	Free Samples
71M6541G	Energy Meter ICs	Free Samples
71M6542F	Energy Meter ICs	Free Samples
71M6542G	Energy Meter ICs	Free Samples
71M6543F	Energy Meter ICs	Free Samples
MAX2991	Power-Line Communications (PLC) Integrated Analog Front-End Transceiver	Free Samples
MAX2992	G3-PLC MAC/PHY Powerline Transceiver	Free Samples
MAX36025	Tamper-Reactive Cryptographic-Node Controller with Nonimprinting Memory	
MAXQ1050	Secure USB Microcontroller with Asymmetric 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 5337: http://www.maximintegrated.com/an5337
APPLICATION NOTE 5337, AN5337, AN 5337, APP5337, Appnote5337, Appnote 5337