"The Smart Grid infrastructure promises to deliver significant benefits for many generations, but first we need to address its inherent security flaws. Based on our research and the ability to easily introduce serious threats, we believe that the relative security immaturity of the Smart Grid and AMI markets warrants the adoption of proven industry best practices, including the requirement of independent third-party security assessments of all Smart Grid technologies that are being proposed for deployment in the Nation's critical infrastructure. We are also recommending that the Smart Grid industry follow a proven formal Security Development Lifecycle, as exemplified by Microsoft's Trustworthy Computing initiative of 2001, to guide and govern the future development of Smart Grid technologies." *Joshua Pennell, President and founder of IOActive in a presentation to the Committee of Homeland Security and DHS on March 16, 2009.*

Energy distribution is finally moving into the new millennium and becoming as technologically sophisticated as the rest of our society. The new face of our utility infrastructure, commonly referred to as the Smart Grid, promises to save money and resources while providing better accounting of energy usage. However, like any new technology, it is critical to fully examine the implications and risks of the Smart Grid and its component parts. If history has taught us anything, it's that early-to-market technologies are often ideal targets for attack.

Understanding the smart grid infrastructure

The Smart Grid connects local power distribution with the national infrastructure, changing the way electricity is delivered around the country. The Smart Grid's energy delivery network is characterized by a two-way flow of electricity and information, capable of monitoring everything from power plants to customers' individual appliances. The grid leverages the benefits of distributed computing and fault-tolerant communications to deliver real-time information and enable the near-instantaneous balance of supply and demand at the device level.

A critical technology component of the Smart Grid is the Advanced Metering Infrastructure (AMI), or smart meter network, which acts as both a distribution point and an endpoint for communication and sensor nodes. These new "smart" meters are more automated and require significantly less human intervention than older meters. Smart meters include a wireless network interface and mesh networking software, which enables utility companies to automatically update the software running the devices and allows them to shut off a customer's electricity over the network, known in the industry as remote disconnect.

While many still think of smart meters as “technology of the future,” they are very much a reality today. They are inexpensive, typically costing less than $50 per device, which makes it economically feasible for utility companies to deploy them in large quantities. The recently-approved $4.5 billion economic stimulus package is driving many utility companies to roll out the devices at a staggering pace. Over two million smart meters are used in the US today, and it is estimated that more than 73 participating utilities have ordered 17 million additional smart meter devices.

The negative side of “smart”

Promising utilities and customers greater control of their electricity usage, more savings and better service, smart meters sound too good to be true. And in some cases, they are. Some privacy activists are upset because they believe that smart meters are an invasion of their privacy and invite “big brother” into their homes. Smart meters will indeed collect extensive data, some of which could be personally identifiable information, so it is critical to develop and enforce strict privacy controls.

As the grid becomes more sophisticated, the information being distributed becomes more granular, and ultimately more powerful. Unfortunately, opportunity goes hand in hand with risk, and by bringing the concept of the internet to the utility grid, we are creating a new frontier for cyber-attackers. As the history of the internet has demonstrated, malicious users will find and exploit vulnerabilities to wreak havoc and make money.

On a large scale, terrorists could target weaknesses in the Smart Grid to shut off power to large areas in demand for ransom from the utility or even as a political statement. The risk to individuals is steep as well. Petty criminals can leverage these weaknesses to disconnect power to individual homes in order to break into the residence, or simply to be a nuisance.

Weaknesses in the smart grid

Smart meters are essentially mini-computers. However, they lack the types of protection that have become standard on today’s computers and networks to ensure security. Similar to computers and software developed in earlier years, smart meters were not designed with security in mind. Evidence of this comes from extensive research on a series of smart meter platforms, which uncovered a range of vulnerabilities and programming errors.

Testing done by researchers revealed that many smart meters are vulnerable to common attack techniques, including buffer overflows, as well as persistent and non-persistent root kits that

could be assembled into self-propagating malicious software.

Most alarming is that “worm-able” code execution on standard smart meters has been achieved. The smart meter’s chipset used for radio communication is publicly available in a developer kit format, and the radio interface’s lack of authentication can be leveraged to produce a worm. If an attacker installed a malicious program on one meter, the internal firmware could issue commands to flash adjacent meters until all devices within an area were infected with the malicious firmware.

Once the worm has spread to the meters, the attacker gains several abilities including:
• Connecting and disconnecting customers at predetermined times.
• Changing metering data and calibration constants.
• Changing the meter's communication frequency.
• Rendering the meter non-functional.

If a truly malicious worm were to infect meters in a given area, there would be a best- and a worst-case scenario. Under the best-case scenario, the utility would simply push a firmware update across the standard wireless network to all the affected meters, overwrite the worm, and return the meters to normal operation. This assumes the attacker had not damaged the remote flashing capabilities, changed the frequency on which the meter operates, or changed the calibration of the meter.

Unfortunately, during malicious attacks the worst-case scenario is more likely to be true. In this case, the normal wireless update mechanisms would no longer be intact, or the calibration of the meters would have been changed. If meters supported remote disconnect capability they could be instructed to simultaneously or individually disconnect service to customers’ homes. To return power to affected homes, the utility would need to take time to understand the vulnerability and develop a patch. Then the utility would need to physically repair or replace each meter to return it to normal operation. Restoring power to homes would likely be an expensive and long process, detrimental to the utility and frustrating to the costumers.

A look inside the research

IOActive performed “black-box”—or zero knowledge—penetration testing on smart meters. This testing emulates an attack mounted by someone with no detailed knowledge about the devices’ electronics or functionality. The objective of the assessment was to breach the devices and obtain code execution at the binary level. This involves a process of modeling and exploring

potential attack vectors; reverse engineering device binaries; deeply inspecting hardware and software functions; and fuzzing protocol segment executions.

The research was conducted in a controlled lab environment; however, modeling was conducted to demonstrate the severity of a worm attack in the real world. Mike Davis, one of IOActive's Senior Security Consultants, developed a video simulation of a 22,000-node smart meter worm propagation scenario using GPS points created from geo-coded home addresses purchased from a bulk mailing list. The simulation takes into account real-life variables that would affect a worm attack including the radio range, signal strength, radio noise, and packet collisions on the Smart Grid network. The simulation period is 24 hours, and illustrates that approximately 85% of homes would be infected with the worm within this time period.

In addition to software and firmware vulnerabilities, the physical security of the meter hardware also needs to be considered. The devices are rapidly becoming ubiquitous, and soon will be seen on the side of houses around the world. Unfortunately they contain no real physical security mechanisms and can be stolen easily. Many smart meters employ an anti-tamper mechanism that prevents the user from accessing the device and modifying their usage information, but this would not stop a determined attacker.

An attacker could easily reverse engineer the device, due to the poor physical tamper resistance, and potentially uncover many exploitable security vulnerabilities. An attacker would not need to invest much money and they would not need a background in power systems to do this—just enough curiosity.

Many still believe that a meter attack is doubtful. Unfortunately, it is far more likely than people would like to imagine. A Department of Energy lab published a statistic showing that there were roughly 250 exploits for control systems on any given day in 2006–2007. It was reported to take roughly 131 days to patch and remedy these vulnerabilities, creating a wide window of opportunity for exploitation.

In addition to the ease of the threat, utilities are generally viewed as recession-proof, making them an attractive target during down economies. Vulnerabilities in the Smart Grid itself could cause utilities to lose system control of their metering infrastructure to unauthorized third parties, exposing them to fraud, extortion attempts, lawsuits, widespread system interruption, and massive blackouts.

A brighter road ahead for a secure smart grid

Despite controversy surrounding the Smart Grid and vulnerabilities discovered in smart meter devices, the reality is that the advanced metering infrastructure is here to stay. So how do we move past these inherent security vulnerabilities to realize the benefits of “smart” power distribution?

Fortunately, one of the stipulations for government stimulus money given to utilities is that they must have a plan to perform due diligence for their cyber security. This puts utilities in a powerful position, because they can apply pressure to meter vendors to produce more secure devices. Utilities can drive competition in the smart meter market by performing security reviews on devices from several different manufacturers. Also, by continuing to test the security, quality, and reliability of the products from the chosen vendor for the duration of the product lifecycle, they can ensure that meter vendors continually improve their security protocols.

It is advocated that Smart Grid AMI vendors adopt a formal Secure Development Lifecycle (SDL) to guide and govern the release of products that are better able to withstand malicious attacks. The SDL takes security and privacy measures into account during each stage of development, and requires that a final review occur before the software is released. By adopting the SDL, smart meter vendors would be making the shift to treating security as an integral feature-set of their product. And the SDL makes good business sense, too. Studies show that overall project costs are 60 times higher when gaps in information security controls are addressed late in the development phase.

Following the SDL protocol also will help meter vendors correct many of the design flaws discovered in smart meter devices and employ the most basic rule of security: layer your defenses. Good information security is like an onion; the more layers of defense the better. Smart meters currently have very few layers of defense and often don’t apply basic security practices, such as authentication and encryption.

Researchers have found that many smart meter devices do not use encryption or ask for authentication before carrying out sensitive functions like running software updates and severing customers from the power grid. Even when meters had encryption in place, the keys were exposed or extremely weak and an attacker could easily take the meter apart, locating and deciphering the key. In addition, some researchers have been able to leverage the radio interface’s lack of authentication to produce a worm that could have devastating consequences. Authenticating early and often is a standard security practice, and smart meters are not exempt from this protocol.

The good news for utility companies, meter vendors, and energy users is that there is still time to repair the Smart Grid infrastructure. With the help of the government—as well as security and privacy experts—utility companies can, and should, embrace their role as watch guards of the energy “ecosystem” by holding their vendors responsible for the security of their products. The benefits of the Smart Grid and AMI technologies are undisputed. By placing an increased focus on necessary security and privacy protocols, utilities can thrive from the benefits of the Smart Grid, while maintaining the safety of this critical infrastructure.

David Baker is Director of Services at IOActive and a subject matter expert on information security, CIPS compliance work, and Smart Grid architectures. Baker specializes in developing security requirements and identifying best practices for critical infrastructure and utility system management, having debriefed the Department of Homeland Security on AMI research.