ORIGINAL

Re Docket # E-00000C-11-0328

Email Proof of Criminal Conspiracy at the Arizona Corporation Commission
Information & Perspective by Warren Woodward
Sedona, Arizona ~ June 7, 2015

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated ...." ~ 4th Amendment, U.S. Constitution

As part of my recent complaint to the Arizona Ombudsman that the Arizona Corporation Commission (ACC) is in violation of Public Records Law, I had to revisit the 2,899 pages of emails and documents that I received from the ACC last January as a result of my Public Records Request.

Going through the emails, I came across one I had noticed before but had not realized its true significance at the time. Perhaps I was scanning and not really reading.

Reading the email again I was both shocked and angered to find that certain individuals at the ACC knew full well, and as early as August of 2013, that "smart" meters are surveillance devices.

These individuals knew "smart" meters invaded the privacy of ratepayers, and they knew it – not from anything the public had sent them – but from Elster itself, the company that manufactures the "smart" meters that APS and some other Arizona utilities use.

That these individuals, these regulators, kept silent and did nothing to stop invasion of privacy is nothing short of a criminal conspiracy.

That these individuals, these regulators, kept silent and did nothing to stop APS and other utilities from lying and misleading the public about the surveillance capability of their "smart" meters is nothing short of a criminal conspiracy also.

Those of us who have complained about "smart" meter surveillance have been called "the Black Helicopter Crowd" by a previous ACC commissioner. We have been called "Kooks." Our complaints that "smart" meters are an invasion of privacy have been ignored by the ACC and we have been made to feel as though we are "conspiracy theorists" when in actual fact the real conspiracy has been a criminal one of silence, dereliction of duty and willful negligence at the lawless ACC.

On August 15, 2013, Laurie Woodall, a lawyer who is the "Policy Advisor" for ACC commissioner Susan Smith, sent an article (reproduced in full below) to ACC Utilities Division Director Steven Olea, ACC Utilities Division Assistant Director (and lawyer) John LeSueur, and ACC Utilities Division Engineers Del Smith, Ed Stoneburg, Margaret Little, and Ray Williamson.

The article appeared at Energy Central, an online electric power industry information clearing house, and was written by Michael John. John's bio is posted at the Energy Central website and I have reproduced it below in full to show that he holds an important position at Elster. His words should not be taken lightly.

Michael John is Solution Manager at Elster. He is committed to ensuring Elster's Smart

> Grid and Smart Metering applications are secure by design and fully compliant with the latest EU standards for security and privacy. He has played a key role in developing Privacy Enhancing Technologies (PETs) for Smart Grids at Elster.
>
> In addition to his role at Elster he is also actively involved in the European Commission's Smart Grids Task Force Expert Group 2, which focuses on the regulatory recommendations for privacy, data protection and cyber security in the Smart Grid environment. He is also involved in ESMIG's Security and Privacy Group. Michael is furthermore engaged in several related groups at member state level in Europe.
>
> Michael John has a strong telecommunications and information security background. Prior to joining Elster in 2010, he was a Network Engineer at Nortel. He also holds an MSc in Computer Science.

Woodall copied and pasted the Michael John article into her email and sent it to the other ACC conspirators along with the article's URL. Woodall wrote nothing of her own in her email but she did highlight various parts of the article. Among the highlighted bits:

> Other potential security threats include tampering with meter data in order to manipulate the outcome of billing, or the leakage of personal information and utility-related data that could provide attackers with insight into a householder's behavior. Known as a `consumption signature', this type of information can be used to work out the times of day the householder is absent from a property, as well as the types of electronic appliances they own.

Contrast that highlighted bit with the following from APS's "Myth vs Fact" sheet, which is a compilation of APS "smart" meter lies and propaganda that APS has posted at its website and has sent to customers since at least 2011 when I got my copy:

> Myth: APS will use automated meters to monitor the actions of its customers.
>
> Fact: Automated meters do not have this capability. Like the old mechanical meters, automated meters measure how much energy customers use, not how they use energy. The automated meter does not store or transmit any personal identification information. The automated meters give APS no indication of who our customers are, what they are doing, nor can they determine what appliances customers are using.

Not only is APS lying about not being able to determine appliance usage, APS is lying about this as well: "The automated meter does not store or transmit any personal identification information." Here's a sentence from the Michael John article Woodall did not highlight but it is worth calling attention to now since it proves APS is also lying about "smart" meter storage of personal information,

and that the ACC conspirators knew it.

> "Finally, at end-of-life, the smart meter must be decommissioned to ensure remaining sensitive data such as security credentials and personal information is disposed of securely."

In conclusion, I could not be more furious that the ACC has played dumb all these years when in fact the ACC knew all along that "smart" meters are a very real invasion of privacy. The current corruption scandal investigation of the ACC by the Arizona Attorney General's office needs to be broadened considerably. Some people at the ACC belong in jail.

Here is the full article Woodall emailed, highlighted exactly as it appeared in Woodall's email. In her email, two sentences were also put in **bold** and underlined in addition to being highlighted.

http://www.energycentral.com/gridtandd/metering/articles/2694/Securing-the-smart-meter-supply-chain

Securing the smart meter supply chain

Posted on July 30, 2013

Posted By: Michael John

Topic: Metering

Security issues have attracted more attention as smart meter rollouts have progressed. Consumers have expressed concerns about the privacy of their data, which has led to delays in smart metering programs in the US and the Netherlands. As this was not an area of focus before and therefore without specifications, there have in Europe been instances of smart metering implementations where the necessary features have not been enabled or older forms of encryption are used.

The industry is currently working closely with governments and consumer groups to address the issue of security. Technical specifications continue to evolve, while new or revised security and data privacy mandates may still be introduced. The European Commission's Smart Grids Task Force now requires that security and privacy be addressed even at the pilot stage of a smart metering program. There are also more governments taking the lead on smart metering programs, which often means more involvement from the regulator or national ministry.

This is why information security has to be a core part of smart metering rollouts from the start. Utilities can avoid scenarios where infrastructure must be upgraded or replaced to meet new requirements if end-to-end security is embedded within system design. With several utilities in Europe nearing an installed base of a million smart meters or more, it is important they recognize that security is not just about enabling the technical features on the smart meter, but ensuring the underlying processes are managed in a secure and trusted way across the supply chain.

Smart metering lifecycle

The lifecycle of the smart meter begins at the design and engineering phase. It is then manufactured and delivered to the party responsible for installing it at the premises of the consumer, at which point, it moves into the operational phase and becomes part of the smart metering network. Finally, at end-of-life, the smart meter must be decommissioned to ensure remaining sensitive data such as security credentials and personal information is disposed of securely.

At each phase of the smart meter lifecycle, an unauthorized third party might attempt to gain access to sensitive data and use it to launch a malicious attack on either a consumer or an organization. For example, if architecture design is not robust, an attacker could potentially manipulate the smart meter, data concentrator, or gateways in order to disconnect the supply of electricity. A large scale disconnect across multiple households would not only cause inconvenience to the residents in those locations, but may also lead to issues with the grid itself - such as a power outage.

Other potential security threats include tampering with meter data in order to manipulate the outcome of billing, or the leakage of personal information and utility-related data that could provide attackers with insight into a householder's behavior. Known as a `consumption signature', this type of information can be used to work out the times of day the householder is absent from a property, as well as the types of electronic appliances they own.
The attacker would need to be highly sophisticated and have significant resources at their disposal. However, given that data concentrators might not be located within secure premises, there is the potential for unauthorized parties to gain access to the sensitive data they hold by physically breaking into them.

Security by design

From the outset, the smart meter engineering process must be suitably robust. If a meter crashes (or is made to crash), attackers could potentially exploit this possibility either by injecting code or executing existing code that would allow them to manipulate the meter. Likewise, the engineering of firmware - i.e. software closely tied to the hardware components of the device - must be robust. Here, functional testing is necessary to ensure it is resistant to malware disguised as standardized communications protocols.

Secure firmware engineering will be essential for meter manufacturers moving forward. As recent history has shown, attackers are more likely to target the means of production, and there have been several cases of USB sticks shipping direct from offshore factories that contained malware. **As such, even if a product is certified as being functionally compliant to the relevant standards, it doesn't necessarily mean it is secure, or indeed that there is authentic firmware on it.**

This is why a `security and data protection by design' approach is recommended whereby data protection and security features are built into smart metering systems before they are rolled out. In the world of IT, robust security design is based on end-to-end communications where the receiver can prove the identity of the sender and knows that the message has not been tampered with in transit.

Building a Trust Provisioning model

Manufacturers for example, are trusted for engineering and producing secure and reliable products. To assure all stakeholders (utilities, meter network operators, consumers) that engineering and production processes of manufacturers are secure, manufacturers can express conformity by obtaining a dedicated certification, for example ISO 27001, the international standard for information security management.

In Europe, Elster, who was recently awarded ISO 27001 certification, has created what is effectively a secured cell within its factory. As shown in Figure 1, the meter enters one end of the cell as an un-trusted and unsecured device and emerges at the other end fully sealed and provisioned with unique key material and its `trust anchors'. The smart meter is therefore supplied to the utility as a `trusted' device - i.e. loaded and pre-configured with the correct, authentic firmware and credentials. Elster has also developed a secure process for exchanging the provisioned information with its customers.

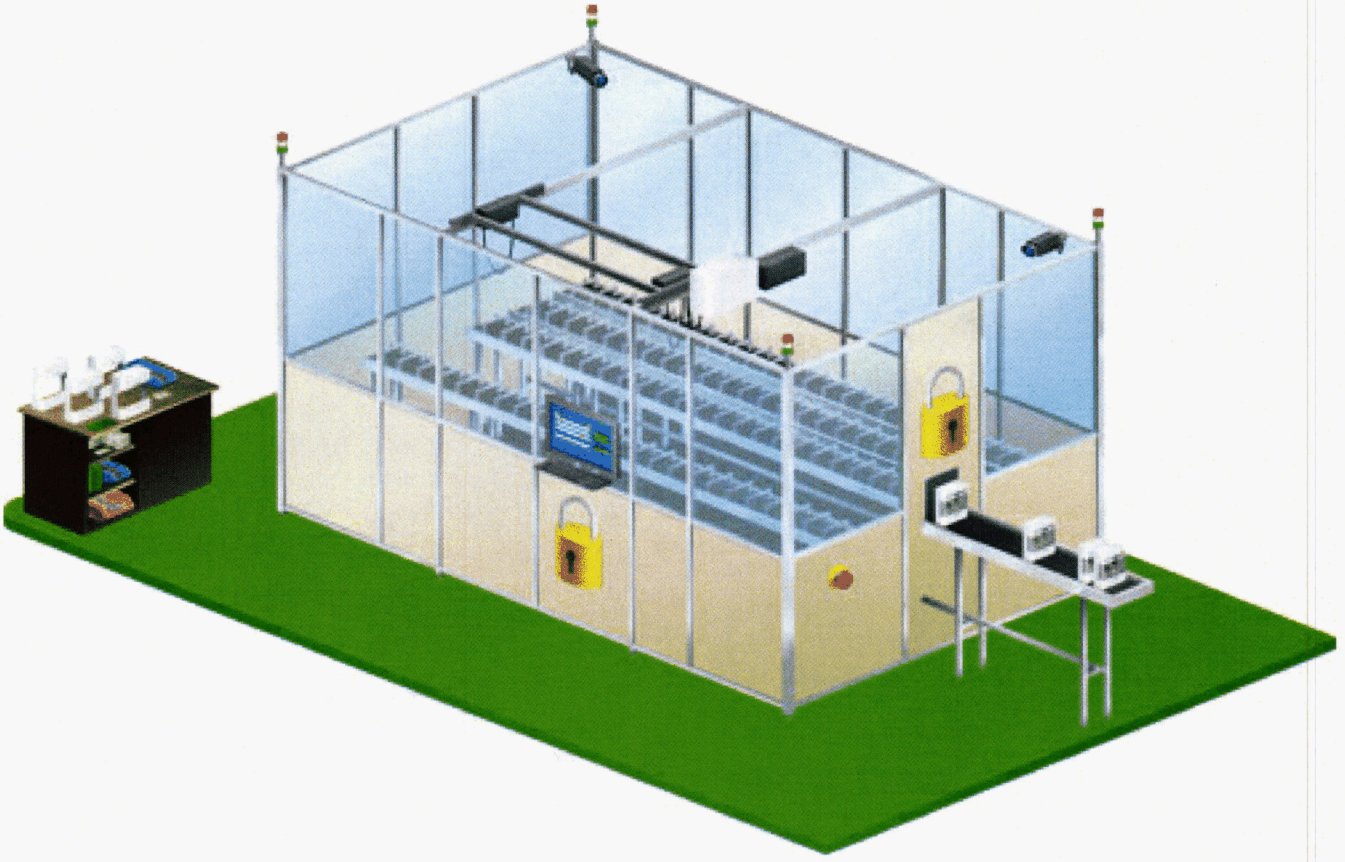

Figure 1: A secured cell for the factory environment
Source: Elster

A key benefit of the trust provisioning approach is that it is agnostic of market design and the smart metering infrastructure, given that every Member State chooses its own model of smart metering implementation and will be at a different stage of liberalization.

Once the meter is installed, ownership transfers to the utility or the party responsible for operating the meter. **At this point, it is critical that the appropriate data security protocols and privacy protection are already enabled.** Further down the line, the decommissioning is just as important, as there may still be security relevant data stored on the meter that, if obtained, could allow unauthorized parties to observe or decrypt previous communication or any personally identifiable information left on the meter.

Similarly, a secure process is required for re-provisioning devices. Utilities will need to ensure they have unique keys for all of their smart meters, and have a management process to update them, and to alter access controls should a smart meter be re-provisioned for a new tenant.

Roadmap and ramp-up plan

Although there are no standards designed to address the smart metering and smart grid supply chain specifically, there are existing standards that provide a baseline and others that are being enhanced to meet the requirements of smart metering and smart grid programs.

In the UK, the central data and communications company (DCC), the function established to manage the data that travels to and from gas and electricity smart meters in households over the wide area network (WAN), will rely on external assurance and certification. This will be achieved via the CESG - the UK Government's National Technical Authority for Information Assurance (IA).

CESG is developing Commercial Product Assurance (CPA-Foundation) security characteristics for smart metering equipment. Once approved by DECC and CESG, they will be published to enable equipment manufacturers to have their equipment tested against the characteristics.

Meanwhile, in Germany the Federal Office of Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) has specified the smart meter protection profile (PP for the Gateway of a Smart Metering System). It is based on the international Common Criteria (CC) and secures the communication between the smart meter in each household and the smart grid, as well as addressing German privacy laws. In meeting these rigorous requirements and being focused around a `single device' however, there is the possibility for further delays to roll-out.

Certainly, it is clear that all stakeholders must have confidence in the standardization and specification process, that the markets be better educated about the tools and technologies available to them, and that government and industry agree a sufficient rather than minimum set of security design requirements. Otherwise, the commercial introduction of certified devices can prove challenging.

With a current understanding of threats, and a current understanding of the required architecture, it is possible to agree on a roadmap that gets rollouts underway and a ramp-up plan to assure manufacturers achieve volume. Utilities that have yet to commence commercial smart meter rollouts now have the opportunity to address security from the outset, specify options that are well aligned with the recommendations made by the EC and relevant industry bodies, and avoid the complexity and expense of implementing security in retrospect.