**Forewarned is Forearmed? The State of Smart Grid Security**

Dr Kieran McLaughlin, Prof Sakir Sezer  
Centre for Secure Information Technologies (CSIT)  
QUB, Belfast

**Abstract**

The phrase “Forewarned is forearmed” suggests that if we know the dangers of something beforehand, we can prepare for it. You could think of it as a more useful version of hindsight.

Despite the undeniable success of the Internet, the past decade has seen it face immense problems regarding security. In hindsight, if we were to start again with security in mind, we might design it differently. The historic problem of security on the Internet forewarns the potential problems facing emerging Smart Grid technologies.

The security issues within the IT industry cannot simply be mapped directly to the Smart Grid, as each domain has different purposes, equipment and architectures. However, there exist parallels that provide insights into how we can, and must, forewarn ourselves regarding security and reliability in Smart Grid, by learning from the history of attack methods, motivations and security failings previously experienced with the Internet.

**Ubiquitous Communications Require Ubiquitous Security**

The electricity grid is undergoing a technological revolution that will be as radical for energy distribution over the next 20 years, as the Internet was for information distribution over the last 20 years. The core objective of the Smart Grid is to improve reliability and efficiency in the electrical system.

New communications technologies will be deployed at all levels of the grid, including generation, transmission, distribution, storage, and metering, to provide ubiquitous connectivity that facilitates information sharing for advanced system management. This will enable the integration of distributed renewables and micro generation, promotion of energy conservation, improved control and management of electrical assets, load control, etc.

The electric grid is much older than IT networks, more mature, and relatively secure. In effect with Smart Grid we want to “improve” this well functioning system by blending in some much newer, less mature and potentially less secure technologies. This is possible, but it is a difficult and complex task.

The public face of the Smart Grid is principally Smart Metering, part of the Advanced Metering Infrastructure (AMI). North America is expected to reach over 78m smart meter installations by 2015¹. Asia-Pacific is projected to increase from approximately 53m in 2010 to between 350-380m by 2016¹². An EU directive calls for complete household coverage by 2022³. The UK government

---

plans to install 53 million smart meters in all homes and small businesses in the country by 2019, at an estimated cost of £11.7bn\(^4\) ($18.6bn).

**Standards**

A report for the UK Department of Energy and Climate Change (DECC), which holds responsibility for UK Government energy policy, highlighted the issue that although there is some agreement behind meter standardisation, there is not in the rest of the grid \([1]\). The situation is more complex in the US, where around 3,100 utilities are involved. Indeed, although meters provided by Silver Spring Networks, for example, use standard TCP/IP communications, some other companies have chosen to develop their own propriety protocols.

Such protocols not only provide the languages and rules for communicating in Supervisory Control and Data Acquisition (SCADA) systems, they also provide a bridge linking cyber space with the power system domain. For example, the electrical substation automation standard IEC 61850 not only defines the interoperability of devices from different vendors but also describes the communication topology, configuration and data structure in terms of substations and other Smart Grid equipment. Therefore in determining the functionality and interoperability of the Smart Grid system as a whole, decisions made regarding communications protocols and standards have a very significant impact.

Some admirable progress has been made under the National Institute of Standards and Technology (NIST), in particular the published volumes of NISTR 7628 - Guidelines for Smart Grid Cyber Security. NIST via its Smart Grid Interoperability Panel (SGIP) is also working on a number of Priority Action Plans, and they have recently begun to publish a Catalog of Standards \([2]\).

Alongside NIST, the IEEE is also working on approving numerous Smart Grid standards \([3]\). For example, IEEE 1686-2007 defines access, operation, configuration, firmware revision, and data retrieval from substation intelligent electronic devices (IEDs) with regards to cyber security.

Moreover, despite this progress, there appears a lack of impetus behind agreeing standards for interoperability, particularly in the core of the Smart Grid beyond the AMI. In particular it is worth noting that even compliance to standards does not necessarily equate to true interoperability between two devices.

The driving force behind getting AMI infrastructure operating can essentially be traced back in large part to reasons of government legislation, economic stimulus money, etc. In the haste to do so, many are of the opinion that security considerations have not received sufficient attention \([4]\), which is compounded by the fact that the functions and definitions of the transmission and distribution Smart Grid core are currently not well defined. The aforementioned DECC report \([1]\) says, “the focus in the smart grid has been to get it working, then later realize that security is an issue”. The report suggested security providers have ignored the requirements in distribution and SCADA control systems.

A recent statement by the US Federal Energy Regulatory Commission (FERC), which governs NIST and SGIP, indicates a halt to the process of agreeing smart grid interoperability standards, due to

\[4\] \text{http://www.decc.gov.uk/en/content/cms/tackling/smart_meters/smart_meters.aspx}
“concerns with cyber security deficiencies and potential unintended consequences from premature adoption of individual standards” [5]. A report by the US Congressional Research Service further highlighted that FERC was not legally empowered to adopt Smart Grid standards [6]. As a result, the delivery of interoperability and cyber security is essentially optional.

NIST has raised its own concerns in this regard, fearing it could take “years” to adopt standards, while recognising “customised” (non-interoperable) equipment continues to be added to the grid. Meanwhile in a response to an MIT report on the future of the electric grid [7], respected industry figure Joe Weiss highlighted in his “Unfettered” blog that NISTR focuses on meters and does not adequately address control systems, excludes power plants for example, and remarks that NERC CIPs are not technically adequate enough to deal with cyber security. He also recommends FERC be solely empowered with responsibility for cyber security of the Smart Grid.

**We Are Building Our Aqueducts Above Ground**

Aqueducts played a key role in Roman infrastructure and supported the growth of large cities, and ultimately Roman civilization. This infrastructure took much time and effort to construct. Early aqueducts were built underground for security, but through time newer, more elaborate and impressive structures were built above ground. It has been theorised that poor physical security of this infrastructure contributed to the downfall of Rome when it and its aqueducts came under attack from barbarians. After the fall of Rome, the only water supply to the city came from a single aqueduct – one that had been built underground. It has been suggested that there are parallels between the risks to the Roman aqueduct infrastructure and today’s critical infrastructure, such as the Smart Grid [8].

SCADA plays a significant role in providing a control system for many industrial processes. In recent years, in an effort to provide improved functionality, these previously closed systems have been connected to open, networked environments. This has lead to a number of cyber security challenges in SCADA systems, and is particularly relevant to Smart Grid technology.

First generation SCADA architectures involved mainframe systems in charge of all functions, such as data polling, processing, display and running application programs. Communications used vendor-proprietary equipment and protocols. In the 1980s, a distributed architecture emerged, with multiple computers in a network handling different specific functions and roles. Third generation SCADA moved from a proprietary environment to an open, networked architecture, where communication protocols such as TCP/IP are used to distribute SCADA functionality across Wide Area Networks (WAN). Fig. 1 illustrates the development of SCADA across recent decades [9].
Figure 1: Evolution of SCADA concepts, protocols and standards

Until the 1990s industrial systems utilising SCADA were generally secure from cyber attacks because of proprietary hardware, software, communications protocols and their isolation from the outside world. However, the current upsurge of interconnectivity in modern SCADA systems, such as Smart Grid, brings huge challenges in order to make the systems secure from cyber attacks. In many ways this mirrors the earlier development of the limited and specialized ARPANET, and emergence of the Internet as we know it today.

In other words, now that we are building our aqueducts above ground, we ought to make sure they are properly protected.

Significant Cyber Incidents

Smart Grid is just one domain of critical infrastructure that is being revolutionised by IT technologies. So when we think about cyber security of the Smart Grid, it worth examining a few pertinent cyber incidents that have already affected critical infrastructure.

In 2000, an attacker was able to access and control sewerage infrastructure at Maroochy Water Services, Australia, with radio equipment stolen from his former employer, that had installed their SCADA systems [10]. On at least 46 occasions he was able to cause a total of 800,000 litres of raw sewage to spill into local parks and rivers, due to lack of protection, detection and traceability.

In 2003, the Slammer worm disabled the computerised safety monitoring system at the Davis-Besse nuclear power plant in Ohio, USA, although at the time it was shut for maintenance [11]. The plant’s network connection was protected by a firewall, however, the worm entered the network from an infected computer by a legitimate third party contractor connected via telephone dial-up directly to the plant network.

In 2008, a software update on a single computer caused the Hatch nuclear power plant in Georgia, USA, to enter emergency shutdown [12]. When the computer rebooted it caused data on a control system to reset, which was interpreted as a fall in the water reservoirs cooling the plant’s nuclear fuel rods. As a result this triggered safety alarms which caused the plant to shutdown.

Finally, possibly the most famous SCADA based cyber incident is Stuxnet [13]. This was a complex piece of malware that is thought to have specifically targeted a uranium enrichment facility in Iran in
Infection was caused via USB sticks, so no outside network connection was necessary. The malware infected Windows PCs and spread using zero-day attacks to elevate administrator privileges. It targeted specific Siemens SCADA control software to upload rogue code to specific types of Siemens Programmable Logic Controllers (PLC). Its ultimate objective was to alter the PLC code to cause the centrifuges they controlled to spin so fast that they were physically damaged.

The evidence suggests Stuxnet was an extremely specific and targeted attack. However, concern remains that the SCADA and Microsoft Windows vulnerabilities it used to propagate remain exposed in other industrial systems. In January this year, researchers at DigitalBond released Metasploit modules capable of attacking vulnerabilities they discovered in a number of manufacturers’ PLCs[14]. While Metasploit can be used for valid penetration testing by security engineers, it can equally be used by hackers. The researchers say they hope this will be a “Firesheep moment” for the SCADA community.

Forewarned
These incidents highlight potential deliberate cyber attacks, but they also show that vulnerabilities can lead to cyber incidents occurring due to mistakes and unforeseen consequences, as well as resulting from deliberate attacks.

The 2008 Hatch incident helps highlight a number of issues. Operating system patches are often not applied in control systems because, due to time or cost issues, they have not, or cannot, be verified as stable, or they conflict with existing hardware. This is worth highlighting as a key disparity between the world of Smart Grid/SCADA and IT, where regular patching for security is assumed possible and indeed expected for cyber security.

Now linking this back to Stuxnet; the zero-day attacks it used against Windows have since had patches released, but many control systems are likely never to receive these patches, for the aforementioned reasons. Tools like Metasploit make these kinds of “attack templates” relatively simple to re-apply and execute against live systems. Numerous other well known specific vulnerabilities have been published, for example, various Siemens PLCs, the Aurora generator vulnerability, etc. These highlight, not only that newly integrated IT style communications infrastructure can itself be attacked, but more significantly that this IT infrastructure in fact provides a never before available route to attack the core devices themselves.

Furthermore, the Hatch and Davis-Besse incidents highlight the potentially large scale impact of relatively small scale oversights when communications technologies are integrated into the grid. Such mistakes are easily made in control systems when communications technology is added as a “bolt on” feature. With piecemeal improvements and the danger of a disorderly approach to Smart Grid interoperability, security becomes hard to coordinate, and all too easy to overlook.

The Challenge
Despite the previous sections that have highlighted a number of problems, the point of this article is not to collect a list of negatives against the Smart Grid, rather it is to focus on the issue of what we
can do to address the challenges these problems present – by learning from experience where possible.

The Internet teaches us that implementing security is not a one-off effort. It is an ongoing process. Smart Grid is an evolution of the current electrical grid, so the current infrastructure will not be unplugged one weekend and replaced with another. The transformation will take place over many years, with improvements being made in incremental steps. This makes security a constantly moving target. Thus the first challenge is to ensure we adopt a rigorous ongoing audit of threats and routes of attack, in order to provide comprehensive Smart Grid security coverage.

In the dynamic environment of the Internet, security has to be adaptable and updatable in order to deal with new threats. In IT, the base technologies change quite rapidly. In Smart Grid the base technologies will not change so rapidly, and will certainly not be replaced or upgraded as rapidly, but it is vital we are not fooled into believing new threats will not emerge just as rapidly as in IT.

Ongoing security audits should include “red-team” type self assessments using tools such as Metasploit where possible (though it may not be practical on some live systems). A systematic approach of mapping motivations and potential paths of attack execution can help detect unknown vulnerabilities as part of a comprehensive audit process. In this respect, information sharing across the energy sector regarding newly encountered attacks and vulnerabilities would contribute significantly to the greater good, although we recognise this would take a 180 degree reversal in philosophy for much of the industry.

Another key challenge will be sharing expertise and nurturing collaboration between specialists in Operational Technology (OT) and IT security, because between them they share a combined body of knowledge covering all of the issues outlined in this discussion. However they can only act successfully upon this expertise if they act together. Thankfully many forward thinking utilities are already acting in this regard.

In order for security to be verifiably robust, it must include benchmarking against best practice and enforced compliance to worthwhile standards. Much groundwork has already been laid, however, with so many separate parties involved, there appears an urgent need for a centralised and coordinated initiative to deliver true interoperability. This means there is a big onus on government and regulatory bodies to work with utilities, vendors, and existing competing consortia to make sure this happens.

Smart Grid is a long term investment and requires longer term thinking. Interoperability that will support a robust open market is in the long term public interest. Yet as previously highlighted, it is essentially government targets that are driving current timetables for infrastructure deployment. Thus we suggest that where possible, governments and their agencies should incentivise and support coalescence around open platforms and interoperability, rather than incentivising utilities and vendors to prioritize roll out to arbitrary targets.

Wi-Fi devices initially suffered from poor interoperability because there was no way to test for compliance with IEEE standards. The Wi-Fi Alliance played a leading role in the success of this
technology by verifying interoperability. A similar model would be an ideal outcome in Smart Grid, although at present many big players are competing for position in the market. Therefore we envisage a number of potential scenarios: (1) it may be possible that they come together in a Wi-Fi style alliance, (2) perhaps a number of vendor-aligned islands of interoperability will emerge, (3) or maybe a de facto set of standards will rise to dominate the pack – let’s call this the Blu-ray outcome.

At the start of 2012 Cisco released their vision of a Smart Grid reference model, called GridBlocks, which focuses on open standards [15]. This includes implementation recommendations and some component reference designs. Cisco appears to be adopting the approach of licensing these reference designs to partner companies, and it clearly hopes to create an ecosystem of devices around its GridBlocks concept. Needless to say the likes of IBM, Silver Spring, etc, are probably not so keen to buy into open standards “as defined by Cisco”. This story clearly has some way to run.

What Now?

Looking back at the way the Internet evolved, it has been extremely difficult to successfully redesign security back into the system. If we were to start again, likely we would not want to start from here. With Smart Grid however we are at the start. This is perhaps our one opportunity to make effective, enduring decisions about security. Smart devices being deployed now may be in place for decades to come.

In reality there is inherent security risk in absolutely every IT system, and Smart Grid is no different. As security engineers we must minimise the risk to an acceptable practical level. Currently, the evidence shows we are simply not minimising the risk.

So what should we do?

1. IT security cannot be separated from supply security. It needs to be a genuine core priority and not an issue of simply meeting “compliance”. This includes eliminating any silo mentality between OT and IT departments.
2. It seems self evident that “security as a priority” is not compatible with current government driven timetables (and the always dubious incentive of government pots of gold). It is always easy to have a go at government, but Smart Grid is an expensive long term investment and it needs clear long term thinking.
3. Interoperability through verifiable open standards and protocols is essential. Government projects and investments should actively incentivise utilities and vendors towards universal interoperability as a priority. Whether the style of outcome is Blu-ray or Wi-Fi Alliance, the sooner the better.
4. Governments should empower a single authority responsible for oversight and enforcement for cyber security standards. As already highlighted, FERC does not have legal powers to enforce standards in the US. It should, and other countries should likewise empower a single authority with responsibility for oversight of Smart Grid cyber security.
5. Establish national mechanisms or bodies where utilities/vendors can confidentially share information of emerging Smart Grid attacks and vulnerabilities, to facilitate industry as a whole to react in a more coordinated and robust fashion to cyber threats. This may be
coordinated by the oversight authority recommended above. This is a tricky area, as companies are understandably reluctant to share such information.

6. Security is a constantly moving target that requires a rigorous ongoing audit of cyber vulnerabilities, red team self assessment, Metasploit tests, etc. In other words, be sure you test yourself before script kiddies (or worse) test you. This is where good practice reaches the parts that compliance alone can’t.

7. Finally, there is a clear shortage of specialised engineers specifically trained in critical infrastructure cyber-security. This requires immediate action, coordination and funding from industry, universities and government to create sustained, career focused education and training programmes. All the best technologies, legislation and standards in the world are useless unless we have good people.

A fundamental motivation for Smart Grid deployment is the future security of the energy supply. Vitally, it must be recognised that without robust cyber security, the security of supply is actually threatened. In many parts of government and industry, the lack of connection between these two principles is currently significant.

We must learn from IT’s successes and failures to ensure security and to avoid preventable mistakes. We have been forewarned.

References