The Need for Security Testing and Conformance Standards in the Smart Grid

Mike Ahmadi, COO

Granite Key LLC

Email

Abstract

While cyber security is and shall always remain a moving target as we continue to build out the Smart Grid, it is quickly becoming apparent to stakeholders that there is need for the establishment of baseline security standards. The Smart Grid Interoperability Panel [1] (SGIP) Cyber Security Working Group [2] (CSWG) has been working towards establishing guidelines for security testing, and utilities are now beginning to require vendors to achieve third party conformance.

Southern Company [3] was the first utility in the US to require a third party certification [4] for their chosen vendor, and other utilities are currently exploring this, both in the USA and overseas. This led to the establishment of the International Electrotechnical Commision (IEC) 62443-2-4 standard project [5], which is intended to serve as an international standard based on the requirements in the standard. This session will discuss the progress of this work, its relationship to the SGIP, and how industry is using the requirements to drive toward better security.

1. THE CHALLENGE

The Smart Grid is currently in an active state of deployment on a global scale. While stakeholders have invested vast resources to address technological issues at many levels, the incorporation of cyber security safeguards has not kept pace with the emerging threats. This initially resulted in a semi-coordinated effort to address cyber security in the Smart Grid, with little or no standardized approaches. A non-standardized approach to cyber security leads to high costs of implementation and ownership throughout the lifecycle of deployed Smart Grid systems, as well as interoperability issues that can cripple the Smart Grid.

Additionally, the current effort to address cyber security in the Smart Grid has placed an inordinate burden upon utilities, with little focus being placed on security requirements for product and system vendors. This has led to an enormous drain of resources, as both vendors and utilities continue to manage security issues on a case-by-case basis.

2. THE APPROACH

While the issue of cyber security in the Smart Grid has risen to a place of prominence in recent years, one of the first major efforts to address security in the Smart Grid began with the establishment of the working group that led to the creation of the NIST Interagency Report 7628 [6] (NISTIR 7628), which was released in 3 volumes in mid-2010. This large body of work was the result of public and private (voluntary) collaboration involving over 400 individuals over a span of approximately 2 years.

The NISTIR 7628 work did not take place in isolation. Utility industry groups, such as the Utility Communication Architecture International user's group [7] (UCAIug) Open Smart Grid [8] (OpenSG) Smart Grid Security Task Force [9] contributed (and continue to contribute) heavily to the NISTIR 7628 effort. This allowed for input on an international level, and the US and Canada continue to work diligently together in the NIST CSWG follow-on work that continues today.

While the NISTIR 7628 is a very valuable compendium of knowledge relating to Smart Grid security, it does not provide adequate guidance for the implementation of security at the application and lower levels (and it is not intended to do so). Various sub-groups have emerged in NIST under the SGIP CSWG to dive deeper into cyber security specifics. Here are a few examples:

CSWG Testing and Certification [10] – This group exists to develop testing and certification criteria for Smart Grid stakeholders to adopt based on the NISTIR 7628 and other relevant bodies of cyber security work.

CSWG AMI Security [11] – This group exists to explore cyber security issues related to Advanced Metering Infrastructure (AMI) and propose solutions based on use cases.

CSWG Design Principles Group [12] – This group is focused on examining low-level to mid-level technical challenges associated with Smart Grid deployment by taking a "bottom-up" approach to addressing Smart Grid security.

CSWG IEC 62443-2-4 Task Force [13] – This task force was formed as a sub-group of the CSWG High Level Requirements Group. The purpose of this group is to analyze and harmonize the security requirements in the IEC 62443-2-4 draft standard, which is intended to serve as a set of baseline security requirements for vendors of Industrial Automation Control Systems. The IEC 62443-2-4 standard project has recently emerged as a significant milestone in the development of cyber security standards for the Smart Grid.

These are only a few of the CSWG working groups. Additional working groups can be found at the NIST CSWG collaboration site, and participation is open to anyone and everyone who wishes to contribute.

Additionally, the UCAIug OpenSG task forces continue to address Smart Grid security issues, and many of the same participants found in the NIST CSWG working groups also participate in the OpenSG working groups. The NIST and OpenSG working groups currently feed each other information, in a coordinated attempt to harmonize the efforts, and with an eye towards standardization. Here are some examples of OpenSG working groups:

AMI Security Task Force [14] – This currently dormant group focused on the creation of security requirements, guidelines, and recommendations for Advanced Metering Infrastructure (AMI), which resulted in the creation of the AMI Security Profile [15] (now in version 2.0).

Embedded Security Task Force [16] – This task force is focused on developing guidelines and recommendations for embedded security components used in Smart Grid products. The focus is very low level (e.g. microchips).

Security Conformity Task Force – This group is currently focused on establishing guidelines and requirements for assessing the conformity of Smart Grid stakeholders to security requirements established in standards (such as the IEC 62443-2-4 emerging standard).

Advanced Security Acceleration Project for the Smart Grid (ASAP SG) [17] – While the ASAP SG is technically not an OpenSG project, the work on ASAP SG has been accomplished, by and large, by members of OpenSG, as well as the NIST CSWG, and has been adopted by both groups.

It should also be noted that the National Rural Electric Cooperative Association (NRECA), which is comprised of approximately 900 rural electric coops in the USA, has released a comprehensive body of security guidelines based on the NISTIR 7628 and other bodies of work. The NRECA Cooperative Research Network (CRN) headed this project, and the body of work has been publicly released as the "Guide to Developing a Cyber Security and Risk Mitigation Plan" [18]. The documents are publicly available and are arguably the most comprehensive and easy to follow set of guidelines for utilities published to date.

The only requirements that currently exist at the US Federal level related to Smart Grid security are the North American Electric Reliability Corporation Critical Infrastructure Protection requirements [19] (NERC CIP 002-009). This is the only set of requirements to date that utilities in North America are audited against, and utilities that are not compliant with NERC CIP standards are subject to stiff fines. This has led to the development of a cottage industry of NERC CIP compliance experts, and every utility that falls under NERC's purview has invested resources (in many cases vast resources) in managing NERC CIP compliance. While this is considered a good first step by many stakeholders, just as many find the NERC CIP requirements lacking in scope and effectiveness towards the goal of achieving security in the Smart Grid for several reasons.

One reason is the fact that NERC CIP requirements apply to less than 10% of the utilities in North America. Additionally, NERC CIP requirements only apply to bulk generation and transmission, and does not apply to distribution (leaving AMI out of the picture) except in the event of a 300 MW load shed. This very narrow scope does not do much to address the cyber security needs of the Smart Grid, despite the sometimes inordinate number of resources dedicated to addressing NERC CIP requirements.

3. WHERE ARE WE TODAY?

Although a lot of effort has gone into (and continues to go into) the creation of guidelines and standards for deploying and managing secure Smart Grid systems, we are currently left with little visibility of the practical application of security requirements. Utilities, vendors, and regulators alike are left with a grab bag of guidelines and requirements that are often assembled in various ways to create what is suitable for each individual stakeholder. While this can indeed lead to better security, it can also lead to security issues that are sometimes more troublesome than doing nothing at all. Security interoperability remains a significant and currently unsolved issue in the Smart Grid, and the lack of a standardized baseline for security implementation is the major challenge.

Utilities are left hoping that the Smart Grid systems they are deploying are adequately addressing current and emerging cyber security threats, with little more than faith in the security claims their vendors provide as initial evidence. Utilities are then forced to dedicate significant resources to test the security claims their vendors make, and many utilities simply do not have the resources to expend on such testing (regardless of the size of the utility).

One utility in North America, Southern Company, took a very significant approach to addressing this challenge.

Southern Company teamed up with Wurldtech Security Technologies [20] and worked with them to create a modified version of a set of security requirements originally created in Europe for the Industrial Automation Control Systems (IACS) industry known as the WIB [21] Security Requirements [22].

The WIB requirements were created as a set of baseline security requirements for vendors, driven by the security needs of end users. The largest energy company in the world, Royal Dutch Shell [23], has mandated third party certification against the WIB security requirements for all of their vendors of IACS products, and Southern Company followed suit by mandating the same for their vendors.

Wurldtech was the first company to create a certification program for the WIB requirements, and it is known as Achilles Practices Certification [24] (APC). The first AMI vendor (under the mandate from Southern Company) to achieve APC certification was SENSUS[25]. The announcement of APC certification by SENSUS sent some shockwaves through the Smart Grid security community, because it seemed (at the time) to occur outside of the aforementioned working groups. As was soon discovered, the development of the WIB 2.0 requirements (which was developed to address Electric Industry security requirements lacking in version WIB 1.0) was extremely well aligned with the NISTIR 7628 requirements, with absolutely no conflicts whatsoever.

This led to the submission of the WIB 2.0 requirements to IEC as part of the IEC 62443 series of cyber security standards for IACS, and was approved as a project within IEC in the summer of 2011. The current project is well underway, with continual support from NIST, OpenSG, the Department of Homeland Security (DHS), and other working groups both domestically and globally.

While the ratification process for standards in IEC can be a long and arduous process, the WIB work continues in parallel. The WIB working group is currently working on version 3.0 of the WIB security requirements, which will incorporate updated requirements commensurate with the IEC 62443-2-4 standard project, serving as a de-facto standard during the gap between current deployment timelines and deployment after the IEC 62443-2-4 standard becomes ratified. Several large vendors have now become certified to the current WIB requirements under the APC program, and many more are currently in the process of becoming certified.

Additionally, several more utilities, both in North America and abroad are currently in the process of considering mandating the WIB requirements as a stop gap measure (like Southern Company did), and public utility commissions in North America are currently considering the addition of such requirements as part of their Smart Grid deployment plans.

Let's take a moment to review the benefits of this approach:

3.1. Benefit 1: Immediately Leveling the Playing Field

The advantage of having a third party certification program for Smart Grid vendors is that both vendors and utilities can level set on a baseline set of security requirements. This leads to, among other benefits, a significant reduction in costs associated with the procurement process.

3.2. Benefit 2: Establishment of a Path Forward

Security is an ongoing challenge, with destination. Consequently, no standard written can adequately address security challenges ad infinitum. The establishment of a baseline set of security requirements that everyone in the energy industry can adopt does, however, allow us to move forward in unison as security needs continue to develop in the Energy Industry.

3.3. Benefit 3: Security Interoperability

The prescriptive nature of standards naturally leads to interoperability. If everyone is working off of the same set of security requirements, there is a much greater chance that the security will interoperate.

4. THE PATH FORWARD

The development of any standard requires continual support and participation by stakeholders, as well as active implementation. The implementation is the single most important part. Standards that are not adopted and implemented represent enormous bodies of work with limited (or no) purpose. Active adoption and implementation of Smart Grid security standards by all industry stakeholders leads to continuous development and improvement of cyber security in the Smart Grid. By actively implementing security standards, we are forced to learn what is most effective for the entire industry, and consequent changes to requirements affect the entire Smart Grid community consistently. This is important, because a unified effort taken up by all stakeholders has the greatest chance for survival due to the fact that all stakeholders become part of the "fabric".

5. SUMMARY

All efforts must lead to something conclusive at some point in order for the efforts to remain relevant. By planting a stake in the ground and coalescing upon a standardized set of cyber security requirements throughout the Smart Grid industry, all stakeholders can focus on improvements in cyber security that are both interoperable and widespread. By focusing on this now, while the Smart Grid is still in its infancy, we can be assured that as it continues to grow, cyber security will not be an afterthought.

References

[1] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome

[2] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityC TG

[3] http://www.southerncompany.com/

[4] http://www.wurldtech.com/newsandevents/announcements/11-02-14/Southern_Company_Sensus_and_Wurldtech_Cooperation.aspx

[5] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/IEC6244324Tas kForce

[6] http://csrc.nist.gov/publications/PubsNISTI Rs.html

[7] http://www.ucaiug.org/default.aspx

[8] http://osgug.ucaiug.org/default.aspx

[9] http://osgug.ucaiug.org/utilisec/default.aspx

[10] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGTesting

[11] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGA MI

[12] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSWGD esignPrinciples

[13] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/IEC6244324TaskForce

[14] http://osgug.ucaiug.org/utilisec/amisec/defau lt.aspx

[15] http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/AMI%20Security%20Profile%20(ASAP-SG)/AMI%20Security%20Profile%20-%20v2_0.pdf

[16] http://osgug.ucaiug.org/utilisec/embedded/default.aspx

[17] http://www.smartgridipedia.org/ind ex.php/ASAP-SG

[18]https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Pa ges/default.aspx

[19] http://www.nerc.com/page.php?cid=2%7C20

[20] http://www.wurldtech.com/

[21] http://wib.nl

[22] http://www.wib.nl/download.html

[23] http://www.Shell.com

[24] http://www.wurldtech.com/achilles-certification/achilles-certified-practices/program-summary.aspx

[25] http://www.sensus.com