Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) Standards Review

CSWG Standards Review Report

Zigbee Smart Energy Profile 2.0 Public Application Protocol Specification, 11167 Version 0.7

May 10, 2011

Security Assessment of Zigbee Smart Energy Profile 2.0 Public Application Protocol Specification, 11167 Version 0.7

1. Introduction

1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different "layers" in the communications "stack" or "profile," one example of such a profile is the GridWise Architecture Council (GWAC) Stack. Some standards address the lower layers of the communications stack, such as wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cybersecurity technologies cannot be linked to them until they are translated into "bits and bytes" by mapping them to one of the semantic structures. Above the communications standards are other security standards that address business processes and the policies of the organization and regulatory authorities.

Secondly, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may just be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to: cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Thirdly, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself: how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance.

Fourthly, some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may," and/or "could" statements, "normative," or "informative" language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of policy, procedural, and communication standards designed to provide specific services. Ultimately, cybersecurity as applied to the information exchange standards should be described as profiles of

technologies and procedures which can include both “power system” methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if TCP/IP is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then TLS (transport layer security) should most likely (but not absolutely) be used.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be taken into account.

1.2 Correlation of Cybersecurity Requirements with Physical Security Requirements

Correlating cybersecurity requirements with specific physical security requirements is very complex since they generally address very different aspects of a system. Although both cyber and physical security requirements seek to prevent or deter deliberate or inadvertent attackers from accessing a protected facility, resource, or information, physical security solutions and procedures are vastly different from cybersecurity solutions and procedures, and involve very different expertise. Each may, in fact, be used to help protect the other, while compromises of one can definitely compromise the other.

Physical and environmental security that encompasses protection of physical assets from damage is addressed by the NISTIR 7628 only at a high level. Therefore, assessments of standards that cover these non-cyber issues must necessarily also be at a general level.

1.3 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as “appropriate security technologies and procedures should be implemented.”

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

1.4 References and Terminology

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

References to "government-approved cryptography" refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees[1]:

- Requirements are expressed by "…shall…," which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).
- Recommendations are expressed by "…should…," which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).
- Permitted or allowed items are expressed by "…may…," which is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).
- Ability to carry out an action is expressed by "…can …," which is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).
- The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. "All traffic in this lane must turn right at the next intersection.")

2. Zigbee Smart Energy Profile 2.0 Public Application Protocol Specification, 11167

2.1 Description of Document

As stated in the document, "*the purpose of this document is to define the application protocol used by the Zigbee Smart Energy Profile release 2.0. The Zigbee Smart Energy Profile Public Application Protocol is designed to meet the requirements stated in the Zigbee Smart Energy Profile 2.0 Marketing Requirements Document and the Smart Energy Profile 2.0 Technical Requirements Document. Per Req[DataModel-1], this application protocol is built to map directly to IEC 61968, the common information model, and is expected to follow a RESTful architecture.*"

According to the specification, "*the Zigbee Smart Energy Profile 2.0 Application Protocol is primarily a layer seven protocol, built on top of an Internet Protocol (IP) stack…* with IP providing functions in the 'TRANSPORT' and 'NETWORK' layers." Therefore, the purpose of SEP 2.0 Application Profile Specification is to define "the mechanisms for exchanging application messages, the exact messages exchanged including error messages, and the security features used to protect the application messages" on Internet Protocol (IP) Home Area Networks (HANs).

[1] The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after "which") comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

2.2 Assumptions

Smart Energy Profile 2.0 Application Protocol is primarily a layer seven protocol, built on top of an IP stack. It further assumes that all interactions will be common information model (CIM)-based, which constrains the types of interactions, particularly impacting those interactions already using other protocols and object models.

It also assumes that all HAN devices will be IPv6 based, which is also an incorrect assumption. It, therefore utilizes the IP addressing scheme to bind names to HAN nodes and meters, ignoring the fact that these devices use network independent (and IP independent) node-naming conventions and registration services that represent end-to-end Smart Grid level entity associations based on other Standards.

The SEP 2.0 Technical Requirements (TRD) (reviewed separately), recognizes the need for pass-through messaging (i.e., tunneling of non-SEP protocols), (see TRD section 1.6.1, "*Ensure coexistence with incumbent technologies that have significant installed bases on shared media*" covering the needs of Security, Authentication and Audit. This capability is supported in Zigbee/SEP 1.0, but seems to be lacking in SEP 2.0 Application Profile, so that authentication and auditing capabilities may be compromised for the non-SEP protocols.

The protocol does not implement multicast services, claiming that "*LD and FS shall support point to point distribution of files. Multicast distribution of files is not recommended due to potential security vulnerabilities*", which is an incorrect statement, since the vulnerability of multicast depends upon the type of information, the security requirements, and the policy, procedures, and technologies used for security.

This document expands the scope of SEP 2.0 as defined in the SEP 2.0 Technical Requirements Document, which limits the scope to the HAN. In this Application Profile, it states, "As such, this document may be useful for anyone developing a Smart Grid solution," which extends beyond the HAN and may lead to cybersecurity and interface authority ambiguities.

2.3 Assessment of Cybersecurity Content

2.3.1 Does the standard address cybersecurity? If not, should it?

The document does address cybersecurity by identifying some specific security requirements and cipher suites. However, many cybersecurity issues are not addressed either in this document or the Zigbee SEP 2.0 Technical Requirements document.

2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

The correlations between this document and the security requirements described in NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, Chapter 3, families and requirements, are shown in Table 1.

Table 1: Correlations between Standard being Assessed and the NISTIR Security Requirements

Reference in Standard[2]	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
12.2 Application Authentication and Authorization context	SG.CA-1: Security Assessment and Authorization Policy and Procedures	Acknowledges that authentication and authorization should be used, but does not mandate it. In addition, the need for authentication is based on the ACL in the ESI: use of Port 80 (authentication is not needed); use Port 443 (authentication is needed). This may be a vulnerability, depending upon further checks. For instance, what if the ESI ACL is compromised?
12.3 Registration	SG.AC-1: Access Control Policy and Procedures	Application authentication only applies using HTTPS and Port 443.
12.7 Cipher suites	SG.SC-12: Use of Validated Cryptography	The following cipher suites are included. • TLS_ECDHE_ECDSA_WITH _AES_128_CCM_8 • TLS_DHE_RSA_WITH _AES_128_CCM_8
12.8.1 Device Certificate	SG.SC-15 Public Key Infrastructure Certificates	Certificates are supposed to come with the devices – however, no methods are mentioned on how to trust manufacturer-supplied certificates.
13.2 Time Function Set	SG.AU-8: Time Stamps	Time synchronization is optional. However, it should not be optional for any device that requires security and does/should contain audit logs.

2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

- All responses in interactions require the use of a Uniform Resource Identifier (URI) to contain the response. The security of this approach should be assessed.
- In clause 12.1, network authentication and authorization is stated to be out-of-scope. Although this is reasonable, network authentication and authorization must be addressed through a normative reference for SEP 2.0 networks.
- No methods are described or referenced on how to trust manufacturer-supplied certificates.
- No methods are described or referenced on key management.
- SEP 2.0 should not prevent the use of IPv4. In addition, IPv6 security issues must be addressed, including the fact that IPv6 exposes the IP address of the private end device to the larger network.
- Since SEP 2.0 does not provide multicasting services, other protocols will need to provide these services, which could lead to significant cybersecurity gaps. For instance, the SEP 2.0

[2] The references may be just the section numbers or could include the title of the section, depending upon what fits easily.

requirement for point-to-point may lead to an inadvertent denial of services attack in bandwidth-constrained networks. The lack of report-by-exception could also lead to inadvertent denial of service attacks. This is a general concern with the security approach of SEP 2.0 because the security requirements of functions that require real-time interactions taking place in a timely manner and the reality of constrained networks are not taken into account.

- In the HAN, there is a need for gateways and protocol converters between SEP 2.0 and other protocols. The assumption is made that all such interactions will occur in the ESI. However, this is not likely to be correct for all situations since many appliances and DER systems may utilize their own protocols, and interchanges through the public Internet directly to these home devices may also occur. There are no discussions on how to handle the security of these gateways, protocol conversions, and non-SEP devices.

2.3.4 What work, if any, is being done currently or is planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

The draft SEP 2.0 documents are being reviewed and commented on by many stakeholders, including the CSWG. As an output of the public comment and this review, it is anticipated that many of the existing security issues will be addressed in future versions.

2.3.5 Recommendations

This document does not meet the cybersecurity requirements of the NISTIR at this time. The CSWG recommends that the SGIP not accept this SEP 2.0 document until the following recommendations are acted upon:

- Remediate the security issues identified in section 2.3.3, either by direct inclusion in the document or as normative references to existing documents, or by planning future documents to address the security issues.
- Address the security of pass-through messaging of other protocols.
- Address the security of non-CIM-based object models that either are directly used over the 7-layer SEP 2.0 stack, or use gateways for protocol conversions. These object models could include ANSI C12.19, IEC 61850, BACnet, Modbus, and many appliance-specific models.
- Address the security of interactions with non-SEP protocols that either are directly tunneled over the 7-layer SEP 2.0 stack or use gateways for protocol conversions. These protocols could include ANSI C12.22, IEC 61850/MMS, DNP3, BACnet, Modbus, and many appliance-specific protocols.
- Clarify which references are normative and which are informative.

2.3.6 List any references to other standards and whether they are normative or informative

2.3.6.1 Normative and/or Informative (no distinction made)

Smart Energy 2.0 Documents

[ZBHP MRD]	Zigbee+HomePlug Joint Working Group Smart Energy Profile Market Requirements Document (http://www.zigbee.org/imwp/download.asp?ContentID=16081) Public download available at: http://www.zigbee.org/Standards/ZigbeeSmartEnergy/HomePlugMarketingRequirementDocument.aspx
[ZB 095449]	Smart Energy Profile Technical Requirements Document (095449) Public download available at: http://www.zigbee.org/Standards/ZigbeeSmartEnergy/20TechnicalRequirementsDoc.aspx
[ZB 105571]	Smart Energy 2.0 UML Model (105571)
[ZB 105629]	Smart Energy 2.0 XSD Package (105629)
[ZB 105636]	Reading Type Codes (105636)

Zigbee Alliance Documents

[ZB 053474]	Zigbee Specification (053474r17) Public download available at http://www.zigbee.org/Specifications/Zigbee/download.aspx
[ZB 075123]	Zigbee Cluster Library Specification (ZCL) (075123r02) Public download available at http://www.zigbee.org/Products/ZigbeeClusterLibraryDownload.aspx
[ZB 075356]	Smart Energy Profile 1.0 (075356r15) Public download available at http://zigbee.org/Standards/ZigbeeSmartEnergy/PublicApplicationProfile.aspx
[ZB 094940]	SEP Intermediate Release 1 MRD (094940)
[ZB 095021]	SEP Intermediate Release 1 TRD (095021)
[ZB 095023]	Zigbee IP 2009 Specification (095023)
[ZB 095310]	SEP Intermediate Release 1 Profile Specification (095310) Draft Application Protocol Specification
[ZB 095165]	Prepay requirements for the Intermediate release (095165)
[ZB 095208]	SE PM Additional Incremental Release Features (095208)
[ZB 095288]	Smart Water Meter MRD (095288r00)
[ZB 095264]	Zigbee OTA Upgrade Cluster Specification (095264)
[ZB 095328]	Smart Energy Profile UML Model (095328)
[ZB 095446]	Zigbee IP Application Support Specification (095446)

IEC Documents

All IEC documents are available at: http://webstore.iec.ch, unless otherwise specified.

[61850]	Communication networks and systems in substations - ALL PARTS
[61850-1]	Communication networks and systems in substations - Part 1: Introduction and overview
[61850-7-420]	Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes
[61968-1]	Application integration at electric utilities - System interfaces for distribution management - Part 1: Interface architecture and general requirements
[61968-2]	Application integration at electric utilities - System interfaces for distribution management - Part 2: Glossary
[61968-3]	Application integration at electric utilities - System interfaces for distribution management - Part 3: Interface for network operations
[61968-4]	Application integration at electric utilities - System interfaces for distribution management - PartInterfaces for records and asset management
[61968-9]	Application integration at electric utilities - System interfaces for distribution management - Part 9: Interfaces for meter reading and control
[61968-13]	Application integration at electric utilities - System interfaces for distribution management - Part 13: CIM RDF Model exchange format for distribution
[61968 UML]	CIM Users Group Unified Modeling Language (UML) Model http://cimug.ucaiug.org/CIM%20Model%20Releases/Forms/AllItems.aspx)
[61970-301]	Energy management system application program interface (EMS-API) - Part 301: Common information model (CIM)
[62055-21]	Electricity Payment Meters – A Framework for Standardization

IETF Documents

[COAP]	Constrained Application Protocol (CoAP), Z. Shelby, B. Frank. Constrained RESTful Environments WG. (http://tools.ietf.org/wg/core/)
[RFC 768]	User Datagram Protocol (http://tools.ietf.org/html/rfc768)
[RFC 792]	Internet Control Message Protocol (http://tools.ietf.org/html/rfc792)
[RFC 793]	Transmission Control Protocol (http://tools.ietf.org/html/rfc793)
[RFC 1042]	A Standard for the Transmission of IP Datagrams over IEEE 802 Networks (http://tools.ietf.org/html/rfc1042)
[RFC 1350]	The TFTP Protocol (Revision 2) (http://tools.ietf.org/html/rfc1350)
[RFC 2119]	Key words for use in RFCs to Indicate Requirement Levels (http://tools.ietf.org/html/rfc2119)
[RFC 2616]	Hypertext Transfer Protocol -- HTTP/1.1 (http://tools.ietf.org/html/rfc2616)
[RFC 2818]	HTTP Over TLS (http://tools.ietf.org/html/rfc2818)
[RFC 3117]	IETF RFC 3117, On the Design of Application Protocols (http://tools.ietf.org/html/rfc3117)
[RFC 3617]	Uniform Resource Identifier (URI) Scheme and Applicability Statement for the Trivial File Transfer Protocol (TFTP) (http://tools.ietf.org/html/rfc3617)
[RFC 3744]	Web Distributed Authoring and Versioning (WebDAV) Access Control Protocol, G. Clemm, J. F. Reschke, E. Sedlar, J. Whitehead, May 2004. (http://tools.ietf.org/html/rfc3744)

Other References

[S3API]	Amazon Simple Storage Service API Reference (API Version 2006-03-01), Amazon Web Services (http://docs.amazonwebservices.com/AmazonS3/latest/API/)
[EXI]	Efficient XML Interchange (EXI) Format 1.0(http://www.w3.org/TR/2008/WD-exi-523 20080919/)
[NIST 1108]	NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

	(http://collaborate.nist.gov/twiki-526 sggrid/pub/SmartGrid/IKBFramework/NISTFrameworkAndRoadmapForSmartG527 ridInteroperability_Release1final.pdf)
[REST]	Representational State Transfer (http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm)
[RESTWEB]	*RESTful Web Services* by Leonard Richardson and Sam Ruby. Copyright 2007 O'Reilly Media, Inc., ISBN 978-0-596-52926-0. (http://oreilly.com/catalog/9780596529260/)
[XEP-0134]	Protocol Design Guidelines (http://xmpp.org/extensions/xep-0134.html)

UCA References

[OpenHAN]	UtilityAMI 2008 Home Area Network System Requirements Specification (http://www.utilityami.org/docs/UtilityAMI%20HAN%20SRS%20-537 %20v1.04%20-%20080819-1.pdf)