STRATEGY AND GUIDING PRINCIPLES

Prepared for:

The SG Security Working Group (UCAIug)

Prepared by:

The Advanced Security Acceleration Project (ASAP-SG)

Managed by:

EnerNex Corporation
620 Mabry Hood Road
Knoxville, TN 37923
USA
(865) 218-4600
www.enernex.com

Version 0.42
October 21, 2009

Table of Contents

1 Acknowledgements

SG Security Working Group (WG) and AMI-SEC Task Force (TF) would like to acknowledge the work of the primary authors, contributing authors, editors, reviewers, and supporting organizations. Specifically, we would like to thank:

- ASAP-SG (Advanced Security Acceleration Project – Smart Grid)
    - The Security Team including resources from Consumers Energy, EnerNex Corporation, InGuardians, the Software Engineering Institute at Carnegie Mellon University, Oak Ridge National Laboratory, and Southern California Edison
    - Supporting organizations including the United States Department of Energy
    - Participating utilities, including Consumers Energy, Florida Power & Light, and Southern California Edison
- The utilities, vendors, consultants, national laboratories, higher education institutions, governmental entities, and other organizations that have actively contributed to and participated in the activities of the SG Security WG and AMI-SEC Task Force

The SG Security WG and AMI-SEC TF would also like to thank the Department of Homeland Security (DHS) Cyber Security Division, National Institute of Standards and Technology (NIST) Computer Security Division, North American Reliability Corporation (NERC) and The Common Criteria for the works that they have produced that served as reference material for ASAP-SG activities.

2 Authors

Len Bass

Patrick Donohoe

Darren Highfill

James Ivers

Howard Lipson

James Stevens

Edited by: James Ivers

3 Introduction

This document summarizes the documents produced by the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) in an effort to provide security guidelines for smart grid applications and the strategies and guiding principles used in their creation. This material is suitable for any party interested in how the documents fit together to improve smart grid security and the thinking that guided their creation. This document is appropriate for a wide audience, including policy makers, project funders and sponsors, and C-level executives (e.g., CEO, CIO, or CTO).

The vision for the smart grid is broad, expressing many necessary properties of a modern power grid. This scope of the work described in this document, however, is focused more narrowly on security issues involved in the migration to a smart grid. Increasing deployment of networks (such as those used in advanced metering infrastructure (AMI)) that enable communication between broad ranges of systems and devices, from home appliances to utility enterprise systems to elements of critical infrastructure, presents an urgent need for security guidance that is specialized for the smart grid.

The introduction of two-way digital communications between networked consumers and producers, among other applications, results in the kind of complexity and infrastructure that has been in place for the Internet for decades. However, this also opens up the kinds of security issues that are the bane of today's Internet: vulnerabilities that leave consumers and utilities exposed to theft or denial of service, compromise of confidential information, and malicious attacks on the infrastructure with intent to cause damage or financial loss. The consequences of a successful cyber attack against a resource like the electrical grid are potentially catastrophic.

Hence the vision for the Smart Grid also includes the goal of making the grid more secure—giving it the ability to withstand both physical and cyber attacks without suffering significant damage or disruptions to service, and without incurring major recovery costs.

ASAP-SG was created by the SG Security Working Group of the UCA International Users Group (UCAIug) to be a utility-driven, public-private collaborative effort to develop recommendations, and best practices for building, acquiring, integrating, and operating smart grid systems, components, and devices. The current focus is on the development of security requirements that

- utilities can use in their Request For Proposal (RFP) processes,
- vendors can use as reference material in their development processes,
- government can use to understand the measures being taken to secure critical infrastructure, and
- utility commissions can use to verify the protection of public interests.

The documents produced by ASAP-SG will serve as raw material for the SG Security Working Group within the UCAIug, as well as the National Institute of Standards and Technology's Cyber Security Coordination Task Group (CSCTG). Each of these organizations is expected to review, comment, edit, and select material as it sees fit for production of its respective guidance documentation.

The remainder of this document provides more details about the ASAP-SG efforts to provide actionable guidance for securing the Smart Grid. It describes the high-level strategies used to generate the best security guidelines feasible in a short period of time and the guiding principles used in their creation.

4 Strategy

While the smart grid as a whole is a massive, long-term endeavor (comprising many different business applications), many utilities are already deploying pilot applications in targeted areas and are formulating plans to proceed with large-scale deployments soon after their pilots are complete. An accelerating pace of deployment imposes the need for the rapid development of security guidance for today's procurement activities, e.g., to avoid costly mistakes in capital expenditures for new equipment like smart meters.

The ASAP-SG group, in consultation with members of the SG Security community, developed an approach to address such critical, short term needs with an eye towards longer term needs. Several key factors driving this approach are

- a need to deliver security guidelines before it's too late (e.g., before costly investments have already been made in infrastructure that cannot be inexpensively updated)
- a need to supply security guidance that is as broadly applicable as possible, regardless of the size of a utility or the particular technologies used by a vendor
- a need to supply actionable guidance for procurement activities in a form that is easily put to use by utility and vendor communities

Security profiles are a key element to the solutions provided by ASAP-SG. A security profile is a document that contains a baseline set of security controls for a given smart grid application. By segmenting security guidance based on smart grid applications (and associated components), guidance can be developed incrementally. This allows, for example, an AMI security profile to be developed without simultaneously grappling with other smart grid applications, such as automated data exchange. Guidance from different security profiles can be combined when utilities field multiple smart grid applications, or can be considered independently should a utility incrementally deploy their applications.

The following documents are being created to provide security guidance for smart grid applications

- *Strategy and Guiding Principles*: (this document) explains the approach taken, the structure of and relationships between ASAP-SG documents, how the documents should be used, what problems the documents do and do not address, and the guiding principles in their creation and application.

  This document is a good starting point for any individual wanting to understand how the ASAP-SG artifacts fit together and which is most suitable for use in a given situation.

- *Security Profiles*: several documents for different smart grid applications will be developed in the first year (e.g., advanced metering infrastructure or automated demand-response). A security profile is a self-contained document that includes a baseline set of security controls for a given smart grid application. A smart grid application is identified by the set of use cases it supports. A security profile also includes a domain analysis that describes the logical architecture of the application (where security controls are associated with the components of the logical architecture). The logical architecture is kept relatively abstract to ensure applicability across a wide range of products.

  Profiles are primarily oriented towards procurement activities, with both utility and vendor perspectives in mind. Organization of security controls against logical components provides a utility with a picture of security requirements across a range of discrete products. Controls for individual components can also be quickly accessed, allowing vendors to understand the requirements for specific products.

- *Smart Grid Security Profile Blueprint*: identifies the process for creating a security profile, including the required information and the activities to be performed at each step in the process.

  This document is useful for any individual wanting to understand how a profile was created, creating a new profile, or adapting an existing profile to a different context (e.g., to accommodate a more stringent risk tolerance).

- *Usability Analysis*: community feedback and suggestions for improvement of ASAP-SG documents, principally the security profiles. To ensure that artifacts meet utility and vendor needs, an independent usability analysis team has been commissioned by SG Security to analyze the documents produced by ASAP-SG, with an emphasis on usability for procurement activities. The usability analysis team includes representatives of utility and vendor organizations, but no members of the ASAP-SG team.

  These documents are primarily for communication with the ASAP-SG team, which will respond to the feedback before delivering artifacts to the broader SG Security community.

ASAP-SG is leading the creation of these documents, including the initial set of security profiles, with a community-oriented process. ASAP-SG creates an initial version of each document (e.g., the AMI Security Profile), hands it to the usability analysis team, reviews the usability analysis report, reworks the document as needed, and delivers it to SG Security for additional technical feedback and approval. This process was structured to ensure timely creation and delivery of documents to the SG Security community while involving experts from a variety of fields and

different roles in the community (e.g., utilities and vendors) at points where their perspectives are most needed.

The result is a set of documents providing security guidance for the smart grid that has been subject to community review and adoption. The deliverables are structured to facilitate scaling to future needs by segmenting the problem into individual security profiles that can be individually prioritized, created, and updated.

5 Guiding Principles

This section describes the high level guiding principles used by ASAP-SG in its work. These principles are broken into three areas—stakeholder related, security related, and general principles.

5.1 Stakeholder Related Principles

No effort should begin without careful consideration of the intended users and impacts on other stakeholders. In this case, the primary users of the security guidance are utility and vendor organizations. Both utilities and vendors come in various shapes and sizes. That is, utilities are large and small, public and private. Vendors also vary in size and in specializations. The diversity of these organizations affects how they might use the output of ASAP-SG and how costly this use would be.

Secondary stakeholders for ASAP-SG include standards development organizations, government agencies, and consumers. Secondary stakeholders should see a great deal of utility in ASAP-SG documents, but ASAP-SG documents are not written explicitly for these stakeholders.

Ideally, stakeholders could use ASAP-SG documents (particularly the security profiles) to support (to greater or lesser extent) the following activities.

- Utilities can use security profiles as
    - a source of detailed security requirements for RFPs
    - a source of validation criteria, e.g., when checking security compliance of procured products or system integration activities

    - a resource that informs ongoing security/risk management activities (e.g., auditing)
    - documentation of measures taken to address security concerns
- Vendors and service providers can use a security profile as
    - a source of applicable security requirements and validation criteria
    - a common frame of reference against which to identify common offerings, allowing more cost effective product development
    - a benchmark against which compliance can be used as a product differentiator
- Standards development organizations can use a security profile
    - to identify needs that are not satisfied by existing standards
    - as a mature draft or significant input into new standards development
- Government agencies can use a security profile as
    - a resource in assessing measures being taken to secure the smart grid
    - evidence in answering public concerns over what is being done to secure the smart grid
    - a basis for potential regulation or auditing activities
- Consumers can use a security profile as a resource in understanding measures being taken to secure the electric grid.

In addition to taking these stakeholder needs into consideration, ASAP-SG documents should be

- usable by utilities and vendors of varying size and sophistication.
- tested by representatives of various stakeholder groups to ensure coverage, ease of application, and clarity.

5.2 Security Related Principles

ASAP-SG's overarching efforts to ensure smart grid security are guided by a desire to satisfy the seven high-level security objectives listed below. Any security and survivability control found in a security profile should help achieve one or more of these objectives. While any individual device, component, or subsystem may not contribute to all of these security objectives, the system as a whole must fulfill all of them with appropriate assurance.

Smart grid systems, components, and devices shall

1. Ensure the availability, integrity, and (where appropriate) the confidentiality/privacy of all mission-critical elements of a smart grid application and its associated data in the face of malicious attacks or unintended adverse cyber and physical events (i.e., *security events*).

2. Protect the electrical system, utility personnel, the general public, and all other stakeholders (including service providers and their own services and assets) from harm caused by any security event associated with any smart grid application.

3. Ensure that sufficient information about a security event is available when and where it is needed to support the decision making necessary to protect (or minimize the disruption to) the mission of the affected smart grid application.

4. Support survivability and resiliency by continuing to fulfill critical functions (perhaps in a degraded mode that still provides essential services) during and after an attack, accident, or other adverse event.

5. Never allow any smart grid application or its associated technology to be used as a stepping stone or conduit for attacks on other smart grid applications, end users, external service providers, or any other interconnected entity. The weakest link of the smart grid could provide an attack vector and, consequently, the controls associated with the least important element link should be as carefully considered as those of the most important elements.

6. Ensure that smart grid applications will not amplify the adverse effects of any attack, accident, natural disaster, or human error.

7. Ensure that the security and survivability services and controls used to protect the smart grid do not provide an attack vector or incorrectly respond to malicious or benign stimuli in a manner that would create or worsen a security event.

5.3 Other guiding principles

This section describes additional principles used by ASAP-SG, largely derived from good engineering practices. Fundamentally these are to leverage existing work wherever possible, use the community input to guide the work, and keep the security guidance at an appropriate level.

1. Leverage existing work wherever possible. In particular, a great deal of valuable work has been done in two areas of particular importance

    - Security controls: Developing security controls from scratch is both a brutal and error prone activity, particularly when several catalogs of useful controls exist. ASAP-SG efforts should focus on *adapting* such sets of controls to the particular needs of the smart grid. Candidate sets of controls include UtiliSec's AMI System Security Requirements, the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (based in turn on NIST 800-53), and the Security Standards Council's Data Security Standard for the Payment Card Industry (PCI).

    - Domain understanding: To secure a smart grid application, one must first understand it. The community has been working to create a common understanding of the requirements (often expressed in use cases) and logical architecture of smart grid

applications, particularly in areas like AMI. To provide guidance that has broad applicability, ASAP-SG efforts should build on community consensus efforts like this wherever possible.

2. Use community input to ensure the work is relevant and to help set priorities. Security profiles should be vetted by the same communities expected to use them. Decisions regarding which security profiles should be created first should be driven by community need.
3. Keep the security guidance at an appropriate level. Security guidance that is to be widely applicable needs to be utility and vendor neutral. Largely, this requires assigning security controls to a logical architecture, rather than to a concrete, physical architecture. There is a trade-off here in specificity of guidance vs. range of applicability. ASAP-SG guidance should be as specific as possible, to the extent that it *does not* infringe on broad applicability.

6 Future Work

Current ASAP-SG efforts are an important step in providing security guidance for the smart grid, but are an incomplete step. Much work remains, some of which is summarized here.

The current scope of ASAP-SG activities calls for the establishment of a process for creating security profiles and the delivery of a few for high impact, near term smart grid applications. However, there are other smart grid applications that fall outside of the current scope of activities, and consequently a need to continue developing new security profiles. Likewise, as technologies and business needs change, there will be a need to revisit existing security profiles.

The security guidance found in these security profiles provide effective baselines for different smart grid applications, but are not a panacea. Individual security profiles can be further improved in several ways, largely based on availability of specific contexts. Several areas in which the current work could be improved are

- expanding the work beyond a technical focus. Current security guidance does not include organizational or operational recommendations.
- incorporating formal risk or vulnerability analyses. Formal risk and vulnerability analyses are valuable activities, but impractical without a specific system and organizational context. Future work should include guidance on how utilities can refine the provided security guidance by incorporating input from their own risk or vulnerability analyses.
- providing more tools to reason about the interactions between security and other key system properties, such as usability, performance, or reliability. Current guidance emphasizes security over other properties (though common sense and experience are used to temper decisions).

- providing a choice among controls that could be used to satisfy different risk tolerances. Current security guidance establishes a baseline. Organizations wishing to implement stronger controls would benefit from more control options and guidance on when to choose each level of control.
- developing abuse/misuse case scenarios as a method to help validate that the security controls specified in a given security profile would mitigate or prevent any adverse impacts associated with those scenarios.
- providing more explicit support for product and system conformance. Current ASAP-SG work focuses more on the identification of required security controls than on criteria (e.g., testing procedures) that could be used to verify conformant implementations.