

Sandy Bacik

From: Sandy Bacik
Sent: Friday, January 06, 2012 8:36 AM
To: csctgarchi@nist.gov
Subject: CSWG Architecture minutes from 20120105

Welcome back Architecture subgroup. This is the first week that we are returning to weekly meeting.

This is also an extra long email, as I included our security services and messages lists at the bottom.

CSWG Architecture twiki: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGArchi>

Chair: Sandy Bacik (sandy.bacik@enernex.com)

20120105 Minutes

1. Current tasks.

- a. Updating the NISTIR 7628 architecture chapter.
 - i. The SGAC and NERC actor harmonization is completed and the spaghetti drawing is being updated with the new actors.
 - ii. We will be adding new interfaces in the next month and the group will need to assist in agreeing to the new / changed interfaces.
 - iii. We have started harmonizing the actor definitions for updating the NISTIR 7628.
 - iv. Once the actors, spaghetti drawing, and interfaces have consensus, we will need to start updating the rest of the chapter to ensure all chapter information, including the logical interface categories, are current.
- b. Conceptual security architecture.
 - i. We are defining a conceptual security architecture with the flexibility to allow a utility to select the technology that will fit into their environment and map to the needed security controls.
 - ii. We reviewed an initial presentation (<http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/20120105-SecurityArchitecture.ppt>).
 1. Slides 2-4 list the security services that we have come to consensus on. See listing at the bottom of this email.
 2. Slide 5 lists the message types that will be mapped to security services. See listing at the bottom of this email.
 3. Slide 6 is a rough drawing to show that messages can cross smart grid domains as well as information classifications.
 4. Slides 8-14 list the NISTIR 7628 (2010) GRC requirements that will be applied to the whole conceptual security architecture. The application level (high, moderate, low, and C-I-A) will be based on business criticality and these are the minimum to be applied at the enterprise level. Additional details for the GRC requirements may be required at the system and application levels.
 5. Slides 17-19 list the NISTIR 7628 (2010) technical requirements. These were the security requirements that were applied to the logical interface categories and will be applied to the conceptual security architecture security services and messages.
 6. Slide 22 lists an initial set of enterprise level security services that need to be applied to the conceptual security architecture. In the list at the bottom of the minutes, the initial set of enterprise level security services are marked with an asterisk (*). We will also change the term "entity" to "enterprise" throughout all the conceptual security architecture so there is no mis-interpretation of NERC's term for entity.
 7. Slide 25 lists an initial set of security services that will be applied to all message types. In the list at the bottom of the minutes, the initial set of security services that will be applied to all message types are marked with a the cross-hatch or pound sign (#).

- iii. We will continue to refine the enterprise application of security services and security services to all message types over the next few meetings.
- iv. Security Services and Messages spreadsheet(http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/Security_Services-And-MessageList-v0p5.xls).
 - 1. The initial mappings of the security services to message types can be found in the "General Security Services" tab.
 - 2. The "General Security Services" tab also has three new columns to map the security services to the enterprise, system, and application levels for a higher application of the conceptual security architecture.
 - 3. The initial mappings of the NISTIR 7628 (2010) technical requirements to the security services can be found in the "Technical HLRs" tab.
 - 4. The "HLR to LICs" tab contains the table from the NISTIR 7628 (2010) mapping the high level security requirements to the logical interface categories.

2. Open floor.

- a. We have started back to weekly meetings.
- b. Stan Klein revisited the notion of incorporating the NERC functional actors with the NISTIR 7628 actors. This was completed in a previous set of meetings and the outcome can be found in the following document on the twiki: <http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/NERC-Actors.doc>
- c. Future F2Fs
 - i. NIST Cybersecurity for Cyber-Physical Systems Workshop in Gaithersburg, MD on April 23-24, 2012. Details to follow as we get closer.
 - ii. CSWG F2F in Sterling, VA on April 25-26, 2012. Details to follow as we get closer.
 - iii. SGIP F2F in Charlotte, NC on March 20-22, 2012. Details to follow as we get close.

3. Attendees

- a. Brad Rumery
- b. Elizabeth Sisley
- c. Neil Greenfield
- d. Sandy Bacik
- e. Stan Klein
- f. Tom Scott
- g. Win Gaulding

Regards,

Sandy Bacik, CISSP, CISM, ISSMP, CGEIT
Principal Consultant

EnerNeX

p: 865.696.4470

e: sandy.bacik@enernex.com // www.enernex.com

Additional information:

- List of the current message types:

Acknowledgement	Alarm	Alert	Audit
Command	Contract	Error	Forecast
Identification	Notification	Plan	Policies
Product	Qualification	Query	Resources
Response	Schedule	Setting	Status
Time	Usage Information	Work Order	

- List of security services (note: * services to be applied at the enterprise level and # services to be applied to all message types):

Access Control (logical and physical) #	Audit Trails * #
Authentication - Enterprise * #	Authentication - Message Origin #

Authentication - Session #
Availability / Reliability #
Certification - Enterprise Public Key *
Confidentiality - Message Contents
Confidentiality - Traffic Flow
Crisis Management *
Disaster Recovery * #
Enterprise Unique Naming *
Incident Response * #
Integrity Protection - Hardware
Integrity Protection - Software
Intrusion Detection *
Non-Repudiation *
Physical Security *
Replication and Backup - Software * #
Security Alarm Management *
Security Monitoring * #
Security Policy Management *
Security Service Management *
Software Licensing Protection *
System Configuration Protection
User Interface for Security

Authorization *
Certification - Enterprise Credentials *
Certification and Accreditation
Confidentiality - Stored Data
Contingency Planning *
Directory Service
Enterprise Registration * #
Environment Security *
Incident Reporting * #
Integrity Protection - Message
Integrity Protection - Stored Data
Message Replay Protection #
Personnel Security *
Replication and Backup - Data * #
Risk Management * #
Security Measurement and Metrics *
Security Operations Management *
Security Provisioning *
Security Training and Awareness *
System Audit
Trusted Time * #
User Support