Tutorial: Security in Electric Utility Control Systems

Steven Hurd
Sandia National Laboratories

Rhett Smith and Garrett Leischner
Schweitzer Engineering Laboratories, Inc.

Published in
Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions, 2018

Previously presented at the
VIII Symposium of Automation of Electrical Systems, August 2009,
and 61st Annual Conference for Protective Relay Engineers, April 2008

Originally presented at the
34th Annual Western Protective Relay Conference, October 2007

Tutorial: Security in Electric Utility Control Systems

Steven Hurd, *Sandia National Laboratories*
Rhett Smith and Garrett Leischner, *Schweitzer Engineering Laboratories, Inc.*

Abstract—**This paper provides a tutorial on practical security measures that can be implemented in power system communication networks. It also includes a discussion and comparison of NERC CIP regulations requirements and proven IT security implementations. This tutorial provides a straightforward look at what NERC CIP requires along with potential steps on how to comply, what basic cybersecurity practices are available today, and how these can be implemented quickly and inexpensively.**

This tutorial examines new security protocols in development for substation applications to achieve cybersecurity using proven and vetted IT security protocols tailored for substation use including Ethernet, serial, and modem communications links. This tutorial covers specifically emerging standards including the following:

1. **IEEE P1711—Trial-Use Standard for a Cryptographic Protocol for Cybersecurity of Substation Serial Links.**
2. **OPSAID (Open PCS Security Architecture for Interoperable Design)—Design standard vendors may use to build secure systems for use in industrial control applications. The standard comes from the OPSAID project, under the auspices of the U. S. Department of Energy Office of the Electric Delivery and Reliability's National SCADA Test Bed Program.**

I. Introduction

This paper describes basic cybersecurity practices that should be implemented. These practices are available today and have been proven in other industries and by third party evaluation. The paper describes and critiques the IEEE P1711 explaining the advantages/disadvantages of the protocol and how to use the protocols to secure legacy serial links. This is followed with a description and critique of the OPSAID standard. It includes a description of how OPSAID is used to secure Ethernet communications between substations and between substation and control centers using vetted open security procedures. Further, this paper discusses NERC CIP cybersecurity requirements and provides commentary on potential steps to compliance.

II. Explaining the Basics

A. IEEE P1711

IEEE P1711 is a trial-use standard for a cryptographic protocol for electric sector substation communications using serial links. This standard applies to SCADA (supervisory control and data acquisition) systems and, in particular, the communications between the SCADA master and the IED (intelligent electronic devices).

IEEE P1711 defines the cryptographic protocol to be used on serial links as they are defined in IEEE 1689, focusing on integrity and confidentiality. In addition to protecting the serial communications against cyberattack, this standard will enable vendor interoperability.

The IEEE P1711 standard is based upon the IEEE 1689 standard and the incomplete AGA 12-2. The American Gas Association (AGA) started work on AGA 12-2 to detail security requirements for retrofit solutions to secure legacy serial communication links in SCADA systems. The goal of the AGA specification was to add strong security without altering the existing hardware and software already deployed in the control system.

IEEE 1689 defines general requirements to protect serial SCADA communications and communications to maintenance ports of remote terminal units or intelligent electronic devices. In addition, IEEE 1689 outlines requirements to retrofit legacy control systems with security that minimizes needed changes.

To allow interoperability, IEEE P1711 is designed to strictly define the data as it appears on the serial link. This also allows enough flexibility in the implementation structure to work with diverse system architectures.

IEEE P1711 defines two cryptographic modules: SCADA cryptographic module (SCM) and maintenance cryptographic module (MCM). The SCM is applied to legacy serial communications paths running SCADA data at speeds from 300 to 115200 bps. The IEEE P1711 standard addresses support for a variety of communications media including radio, modems, microwave, and leased lines. The SCM is intended to be a bump-in-the-wire solution (having minimal impact to existing system installation). It operates in a variety of modes, not all of which require encryption. In an authenticated mode, which does not implement encryption, the traffic can be viewed but any modifications to the traffic would be detected. The SCM will build and tear down cryptographic sessions in point-to-point or multidrop systems, performing all cryptographic functions to encapsulate data passing between equipment in the control system.

The design of MCM supports legacy serial communication and installation as a bump-in-the-wire topology. The MCM is designed to be placed on the management port of an IED in a control system and will enable secure remote engineering access to the equipment. Two-factor authentication is used: one factor is a password, while the other is a token such as found on USB fobs. This secure channel will be terminated if the token is removed at any time or if a time out expires. The MCM establishes sessions and performs cryptographic functions. In addition to authentication, the MCM records important information about the session and stores operational data potentially needed for forensic purposes at a later time.

IEEE P1711 outlines technology focused on enabling strong security on existing serial communications, regardless of the media topology, with a cost-effective, easy-to-implement method. The goal of this standard is to protect SCADA messages and engineering access messages with thoroughly vetted cryptographic technology, implemented in a manner that has a minimal impact on the control data. This standard is flexible enough to allow control system owners to strike a balance between their cryptographic needs and control system bandwidth overhead, enabling them to make the choices needed to tightly secure critical links while maintaining business continuity throughout the system.

B. OPSAID

OPSAID is the Open PCS (Process Control System) Security Architecture for Interoperable Design, a project sponsored by the United States Department of Energy's Office of Electricity Delivery and Reliability (through their National SCADA Test Bed program).

OPSAID's goal is to accelerate the commercial development and adoption of comprehensive security functionality in PCS that communicate using an Internet protocol (IP). The OPSAID project is primarily focused upon the development and laboratory testing of widely used, open-source security modules, as well as an all-inclusive Linux-based reference implementation. The results of the OPSAID development and testing efforts provide the building blocks for the development of add-on PCS security appliances and a path for the development of PCS end-devices with built-in security functionality.

To provide comprehensive security functionality, OPSAID includes modules that provide the following:

- Encryption
- Authentication and Access Control
- Firewall
- Intrusion Detection (Network and Host)
- Centralized Logging
- Configuration Session Capture
- Basic Management and Visualization Capabilities

OPSAID's technical approach is to use existing, open-source technology wherever possible. For example, rather than developing a network-based intrusion detection system from scratch, the OPSAID project chose to select "Snort", a widely used open-source intrusion detection system. Specific technical details can be found in the "OPSAID Initial Design and Testing Report". [1] There are minor differences between the implementation of "field devices" versus "control center devices", and are related to the control center devices containing the databases and other centralized resources.

III. Mapping Technology to CIP Requirements

The North American Electric Reliability Council (NERC) recognized that "business and operational demands for managing and maintaining a reliable bulk electric system increasingly rely on cyber assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data." These assets have become a significant target for attack because of the increased reliance on communication and/or cyber-based control systems for the reliable operation of the electric power system. As a result, NERC has developed Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009. The NERC CIP standards "provide a cybersecurity framework for the identification and protection of critical cyber assets to support reliable operation of the bulk electric system" [2].

Reliability Standard CIP-005-1 "requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter." The electronic security perimeters are to encompass all the critical cyber assets that are identified using the risk-based assessment methodology required by Reliability Standard CIP-002-1. Multiple electronic security perimeters may be required; for example, one may be needed around a control room while another may be established around a substation. Once each electronic security perimeter has been established, the responsible entity must develop mechanisms to control and monitor electronic access to all electronic access points. Furthermore, the responsible entity must assess the electronic security perimeter's cybervulnerability and test every electronic access point at least annually [3].

The following paragraphs map OPSAID and IEEE P1711 to NERC-CIP requirements. Any device that meets either of these standards will aid in meeting NERC compliance.

A. CIP-005-1 Cybersecurity—Electronic Security Perimeter(s)

"**R2.** Electronic Access Controls—The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

"**R2.1.** These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified."

Description	OPSAID	IEEE P1711
What base security model(s) does the standard employ to ensure that access to a compliant device is limited to only those with explicit permissions? What levels of access discrimination (permission levels) are available via the standard?	Users or groups are either granted or denied access to a specific resource via an access control list. A user who is not a member of a group who has, or has been explicitly granted, access to a resource cannot access or modify it.	Unique roles are defined within a compliant device. These roles define a set of actions that the specific role can perform. A user account can only perform the actions defined within the role it is associated with.

"**R2.2.** At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services."

Description	OPSAID		IEEE P1711
What ports and services are required for operation and monitoring (including pass-through functions), and what additional ports and services are open or enabled by default?	A vendor may utilize ports, other than those specified below for expanded functionality		A serial port shall be used for the protected traffic, while the management interface shall be vendor specific.
	Protocol	**Port**	
	IPSec	TCP 500 UDP 4500	
	IKEv2	UDP 500	
	OCSP	TCP 8880	
	Syslog	UDP 514	

"**R2.4.** Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible."

Description	OPSAID	IEEE P1711
What strong technical controls (i.e., two factor RADIUS authentication, certificates, etc.) does the standard specify?	Three key methods are supported for message authentication: preshared passpharses, preshared X.509 certificates, and CA signed X.509 certificates. IKEv2 shall be used for session key generation.	Preshared keys are used during initializing of a session to generate a unique session key.

"**R2.5.** The required documentation shall, at least, identify and describe: … **R2.5.2.** The authentication methods."

Description	OPSAID	IEEE P1711
Describe the default authentication methods (identified in R2.1) in technical detail.	—	A compliant device shall use HMAC SHA-1, or HMAC SHA-256 for ensuring message authentication.

"**R2.6.** Appropriate Use Banner—Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner."

Description	OPSAID	IEEE P1711
What Appropriate Use Banner is employed on a compliant device, and what access methods are presented with this Banner (i.e., interactive logon, telnet passthrough, etc.)?	A user configurable login banner shall be displayed prior to any login attempts into a compliant device.	A use banner is not covered in the standard and is dependent on vendor specific implementation.

"**R3.** Monitoring Electronic Access—The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

"**R3.2.** Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess logs for attempts at or actual unauthorized accesses at least every ninety calendar days."

Description	OPSAID	IEEE P1711
What logging do you perform of authorized/unauthorized access attempts or successes?	A compliant device shall log all login attempts on the system as syslog messages.	On a message that failed validation, a log entry shall be created for the session with the reason for failure. Management logging is not defined by the standard and is dependent on vendor specific implementation.

IV. Vetting of Technology

A. IEEE P1711

The vetting of the IEEE P1711 standard includes examination of three distinct areas: cryptographic algorithms, cryptographic implementation, and control system impact. The first two areas focus on the integrity and confidentiality of the messages while the third focuses on the availability of the system.

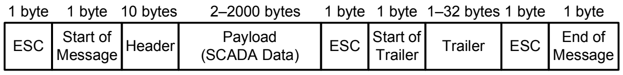
The cryptographic algorithms that are used in IEEE P1711 include AES (Advanced Encryption Algorithm) and HMAC SHA-1 and SHA-256 (Hashed Message Authentication Code Secure Hash Algorithm). All three of these algorithms are approved by the federal information processing standards (FIPS) and have been proven to be strong protection by the public and private sector. FIPS are guidelines developed by the National Institute of Standards and Technology, delivered to and approved by the Secretary of Commerce, to be deployed government-wide to address security and interoperability.

The IEEE P1711 protocol is organized into three layers: session layer, transport layer, and link layer. The session layer denotes different types of messages and negotiates the session key and abstract data exchange. The transport layer is in charge of integrity checking, cryptography, and adds the header and trailer. The link layer formats the message to and from the communications channel. This link layer determines which messages are encrypted and which are sent as plaintext (when running in mixed mode). It is also in charge of adding the start of message (SOM), start of trailer (SOT), end of message (EOM), and escape (ESC) elements into the data stream.

Each layer has different responsibilities in formatting the message. The session layer handles the SCADA message as a sequence of bytes (or octets). The transport layer handles the session layer as a payload and is responsible for encrypting the payload and adding the header and trailer. The link layer formats the transport layer by adding delimiters around the transport layers header, payload, and trailer. This message layout is designed to permit most types of SCADA messages without interference and allow for mixed-mode operation.

Mixed-mode operation is very similar to multidrop configurations with the exception that not all devices attached to the host need to be secured. In mixed-mode operation, some devices run in a secured communication path while others are left in cleartext. Reasons to run mixed mode include a gradual rollout of equipment or a decision by the utility to protect high-priority sites while not having to budget extra money for low-priority sites. The standard specifies how to handle this complex mix of plaintext and ciphertext while avoiding random characters in the ciphertext accidentally mimicking a plaintext SCADA message.

1) Packet Structure



1 byte	1 byte	10 bytes	2–2000 bytes	1 byte	1 byte	1–32 bytes	1 byte	1 byte
ESC	Start of Message	Header	Payload (SCADA Data)	ESC	Start of Trailer	Trailer	ESC	End of Message

Fig 1. Packet Structure

Additional cryptographic overhead should be considered when analyzing the communications path. There needs to be enough time between SCADA messages to ensure the added overhead is transmitted before the next message is received, or a flow control topology must be implemented. This cryptographic overhead is 17 to 48 bytes for every payload of data.

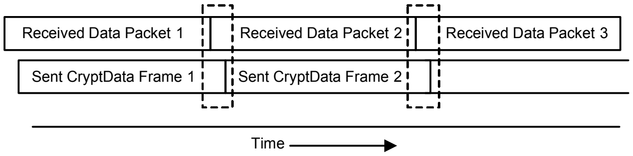
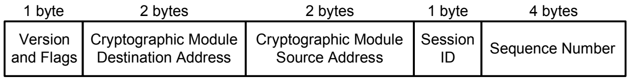


Fig 2. Back-to-Back Received Data With Equal Serial Port Data Rates

a) Header

Fig 3 shows the structure of the header.



1 byte	2 bytes	2 bytes	1 byte	4 bytes
Version and Flags	Cryptographic Module Destination Address	Cryptographic Module Source Address	Session ID	Sequence Number

Fig. 3. Structure of Header in MAP Packet

The header is 10-bytes long and can be separated into five sections.

- The first byte denotes what version (3 bits), alert flag (1 bit), and message type (4 bits) are set for this packet.
- The next two bytes are the cryptographic module destination address.
- Then two bytes for the cryptographic module source address.
- The next byte is the session ID.
  Session IDs are used to distinguish different types of data destined for the same cryptographic module. This allows management data and SCADA data to be performed on the same connection.
- The last four bytes are the sequence number.
  Sequence numbers are used to protect against replay attacks. The sequence number increments by one for every packet; when the sequence number reaches the programmed data session message limit there will be a rekey.

b) Trailer

The trailer is variable from 1 to 32 bytes and holds the authentication data of the header and payload. The trailer length is dependent on the amount of authentication strength required.

c) Latency

IEEE P1711 adds additional latency to a SCADA system. The amount of additional overhead depends on the cryptographic suite selected, the maximum frame length and data session trailer length settings.

To calculate the additional overhead please consider the following:

> Latency = [12 bytes for the header] + [5 to 36 bytes for the trailer] + [length of message being encrypted] + 16 bytes

2) Testing

The implementation of cryptographic features in IEEE P1711 addresses all aspects of establishing a communication session, the transmission of data, and tear down of the session. Initial key loading is in accordance with FIPS and used for static sessions. Static sessions are used exclusively to create dynamic sessions, using randomly generated keys combined with a nonce. The nonce is a variable that only appears once for each session and for this standard has a minimum length of 2^64. In addition to the nonce, IEEE P1711 has a sequence number ordering the messages in the session to prevent replay attacks and uses a timer function in the protocol to prevent an adversary from delaying messages in transit. There are multiple cryptographic suites that can be chosen in IEEE P1711, allowing the end user the flexibility to apply the appropriate amount of security depending on the sensitivity of the communications channel. Finally, there is a keyed hash appended to every message adding strong authentication.

Extensive testing has been conducted to measure the control system impact resulting from the technology outlined in this standard. GTI SCADA test bed, PNNL, and control system asset owners performed tests including five SCADA protocols, twelve vendor’s SCADA software, six vendor’s RTUs, four vendor’s modems, and with data rates up to 9600 bps. These tests validate the control system impact this technology will have [4].

B. OPSAID

OPSAID has completed extensive technology vetting, through lab testing at Sandia National Laboratories, as well as with industrial partners. What follows is a summary of testing results; complete details of testing efforts can be found in the “OPSAID Initial Design and Testing Report”. [1]

Several test scenarios and locations were investigated:

- Sandia National Laboratories (including tests run between the California and New Mexico locations),
- Between Sandia (NM) and Schweitzer Engineering Laboratories, Inc., and
- Within a testing laboratory at a major electric utility.

Tests performed include:

- Verifying installation procedures and configuration parameters
- Testing basic communication capabilities and functionality (given different network scenarios)

- Security efficacy
- Rudimentary stress testing

Installation procedures were generally successful. Comments from each round of testing have been incorporated into the installation procedures found in the OPSAID Initial Design and Testing Report.

Basic communications capabilities and functionality was also successful. After verifying initial connectivity between OPSAID devices and proper network routing and firewall settings, PCS-related traffic was successfully communicated end-to-end. In addition, OPSAID-specific traffic (such as network alerts) successfully traversed the network.

As soon as firewall configuration information was properly entered into the OPSAID systems, security efficacy testing was successful. The OPSAID systems performed as expected, protecting the PCS from a wide variety of network attacks.

The results of rudimentary stress testing demonstrated that the OPSAID devices added negligible latency to existing communications and were able to process traffic successfully under typical operating scenarios.

V. Interoperability

For many years, now, organizations have been creating complex proprietary methods for interdevice communication. Interfacing with these proprietary communications methods has been restricted to a select few with access to the proprietary implementation. With no way for other vendors to access the interface and subsequent data, they are forced to create their own homegrown method of conveying this data.

There are a variety of locations where devices are required to be interoperable. Interoperability, as defined by this paper, is any interaction that leaves the boundary of a device and communicates with another device. Interoperability enables a device to communicate out of the box with software and hardware from other vendors.

Homegrown proprietary devices have the disadvantage that their implementation is, in most cases, not published and the security implementation cannot be easily verified. The lack of interoperability is a major drawback of these homegrown implementations. Once a vendor is selected, unless a complete system overhaul is performed, a new vendor's device cannot be introduced and be expected to interface with the existing implementation.

VI. Advantages/Disadvantages

A. IEEE P1711

IEEE P1711 is designed to add security to existing control systems without the need to change existing SCADA hardware or software. This approach allows security to be added in a cost effective manner. Utilities can deploy this technology without extensive educational programs because this additional security does not change the way authorized control and operations happen.

IEEE P1711 is flexible in its configuration. Users may make decisions based on their risk assessment to choose how much security to apply. Users have ten cipher suite options to choose from. The cryptographic overhead is also user configurable. Users may truncate some of the cryptographic material sent on the communication channel depending on how bandwidth limited they are.

This technology is specified as a bump-in-the-wire topology allowing security to be added with minimal modifications.

This protocol is designed to work with existing SCADA systems as well as new systems, with minimal assumptions about the SCADA protocol. It accomplishes this through detecting the beginning and end of the SCADA message, locating the SCADA device address, and recognizing SCADA broadcast messages. The IEEE P1711 protocol only sends messages when the SCADA system sends messages. This minimizes the additional collisions, overhead, and latency that might occur because of the addition of cryptography on communications.

B. OPSAID

The OPSAID approach to security functionality provides important benefits to PCS owners, as OPSAID takes both a comprehensive and modular approach to PCS security. OPSAID was designed to take the best available, well-tested open-source security modules and combine them strategically to provide comprehensive security services. OPSAID exemplifies "defense-in-depth", where complementary layers of security are combined such that they provide significantly better security than any individual layer of security.

OPSAID layers of security include the following:

- Transmission Security: Encrypted communication links ensure both privacy and integrity of communications.
- Perimeter Security: The firewall blocks all but designated network traffic (by policy).
- Authentication and Access Control: Not only for management of an OPSAID device but also potentially for the PCS end device (depending on implementation).
- Intrusion Detection: Network-based intrusion detection looks for attack signatures. Host-based intrusion detection continually looks for changes in OPSAID device configuration (indicative of an attack).
- Logging and reporting: Activity and intrusion detection logs are collected and forwarded to the control center where they can be analyzed and generate alerts.

Depending on implementation, several of these layers of security provide powerful protection not only from cyber-attacks from "outsiders" but also inappropriate or malicious connections involving "insiders".

An additional advantage with OPSAID is that the reference implementation continues to undergo extensive performance and efficacy testing. This testing uses a variety of lab settings, communications links, and PCS end equipment to verify OPSAID's suitability for securing PCSs.

While OPSAID effectively addresses many security issues, it is not a panacea. Seemingly all security functionality involving transmission or perimeter security provides a potential source of denial-of-service and less overall system reliability, either through it becoming an additional point of failure or the target of attack. On the other hand, OPSAID would seem to be far more resilient in the face of targeted attack than unprotected PCS devices. Thus, the hope is that overall system reliability (when cyberattack is considered) is higher with OPSAID than unprotected PCS devices.

As OPSAID takes advantage of commonly used open-source security modules, it is likely that more attackers would be familiar with and potentially target this technology. While this is true, the defense-in-depth aspects of OPSAID should provide additional layers of protection should a single layer be breached. Furthermore, the intrusion detection and logging features should provide an alert when such activity takes place. With such modules, it is important that as security patches are available and appropriately tested, they are deployed in the field. The current OPSAID reference implementation provides a rudimentary capability in this area.

OPSAID's ability to protect against unauthorized access is predicated upon the ability to define specifically what access is authorized and correctly configure OPSAID devices for the PCS network. While OPSAID is designed to be simple to implement and use, each PCS environment is different, thus knowledge of the overall PCS network architecture and authorized functionality is critical to successfully implement OPSAID. Nevertheless, this is true for any security approach.

OPSAID is designed to secure PCS from unauthorized access. Yet, authorized access is obviously allowed. OPSAID can enforce policies, such as what computers can communicate with certain PCS devices. At this time, OPSAID provides user authentication and firewall services that restrict access to the PCS device, but it is a vendor-specific implementation to define the level of granular access control implemented (e.g., controlling which user can issue which command, etc.). Hopefully, future enhancements to OPSAID will define more granular control that will reduce this possible inconsistency between vendors.

Finally, OPSAID is not a monolithic standard. Individual manufacturers can choose to implement any combination of OPSAID security modules. This can result in systems from different vendors not being able to successfully interoperate. The OPSAID project team is working on creating interoperability guidance that will hopefully address this issue.

VII. Conclusion

These standards define a baseline for security. This ensures that any device that implements one of these standards shall provide adequate security for SCADA and Engineering Access traffic. In addition these standards provide a defined communications method allowing products that meet the standard to interoperate with other existing products.

By defining an interoperable design in these standards, end users have greater assurance that any device which implements the standard will not only successfully communicate with other devices from the same vendor, but also other vendors' devices, providing a guaranteed, documented level of security.

VIII. References

[1] U.S. Department of Energy Office of Electric Delivery and Reliability's National SCADA Testbed Program, "*OPSAID Initial Design and Testing Report*"—publishing forthcoming.

[2] North American Electric Reliability Council (NERC), CIP Standard, ftp://www.nerc.com/pub/sys/all_updl/standards/sar/CIP-002-009-1_30-day_Pre-ballot_Comment.pdf.

[3] Mandatory Reliability Standards for Critical Infrastructure Protection (July 20, 2007). U.S.A. Federal Energy Regulatory Commission, 18 CFR Part 39 [Docket No. RM06-22-000] [Online]. Available: http://www.ferc.gov/whats-new/comm-meet/2007/071907/E-4.pdf.

[4] A. Wright, W. Rush, A. Shah, M. Hadley, and K. Huston. (Aug 2007). "AGA 12 Part 2 Preliminary Functional and Performance Test Report," [Online]. Available: http://www.gtiservices.org/security/AGA-12Part2_TestResults_Draft.doc.

IX. Biographies

Steven Hurd is a Senior Member of Technical Staff in Computer and Network Security, and the Program Manager for the Center for Cyber Defenders Student Intern Program at Sandia National Laboratories, California. In his twenty years at Sandia, Steve has worked in a wide variety of capacities, ranging from Computer Security Research and Operations to Computer Network/Server Design and Implementation. Steve holds a B. A. in Economics and Mathematics (High Honors) from the University of California Santa Barbara, and an M. B. A. in Information Systems Management from the University of Texas, Austin.

Rhett Smith, GSEC is an Applications Engineer in the Security Solutions division at Schweitzer Engineering Laboratories, Inc. In 2000, he received his B.S. in Electronics Engineering Technology graduating with honors, Magna Cum Laude. Before joining SEL, he was an applications engineer with AKM Semiconductor located in San Jose CA. Mr. Smith has his GSEC professional certification (GIAC Security Essentials Certification).

Garrett Leischner is a Product Engineer with Schweitzer Engineering Laboratories Automation Integration and Engineering Division, where he manages the Rugged Computing Platform. Prior to joining SEL, he worked for Cray, Inc. He received his BA in Business from Western Washington University in 2003, and his MS in Computer Engineering from the University of Idaho in 2006. He is an active member of the IEEE Computer Society, Association for Computing Machinery, and the Software Engineering Institute, and has several patents pending. During his time at SEL, he has co-authored several technical papers and instructional courses.

Previously presented at the 2008 Texas A&M
Conference for Protective Relay Engineers.

20070912 • TP6286-01