ORNL/TM-2014/131

Cryptographic Key Management and Critical Risk Assessment

Robert K. Abercrombie

CRADA Final Report
For
CRADA Number
NFE-11-03562

UNLIMITED RELEASE

April 2014

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE US DEPARTMENT OF ENERGY

DOCUMENT AVAILABILITY

Reports produced after January 1, 1996, are generally available free via US Department of Energy (DOE) SciTech Connect.

Website http://www.osti.gov/scitech/

Reports produced before January 1, 1996, may be purchased by members of the public from the following source:

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
Telephone 703-605-6000 (1-800-553-6847)
TDD 703-487-4639
Fax 703-605-6900
E-mail info@ntis.gov
Website http://www.ntis.gov/help/ordermethods.aspx

Reports are available to DOE employees, DOE contractors, Energy Technology Data Exchange representatives, and International Nuclear Information System representatives from the following source:

Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831
Telephone 865-576-8401
Fax 865-576-5728
E-mail reports@osti.gov
Website http://www.osti.gov/contact.html

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ORNL/TM-2014/131

Computational Sciences and Engineering Division

Cryptographic Key Management and Critical Risk Assessment

Robert K. Abercrombie

Date Published: April 2014

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6085
managed by
UT-BATTELLE, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

Page

LIST OF FIGURES

Figure **Page**

ABSTRACT

The Department of Energy Office of Electricity Delivery and Energy Reliability (DOE-OE) Cyber Security for Energy Delivery Systems (CSEDS) industry led program (DE-FOA-0000359) entitled "Innovation for Increasing Cyber Security for Energy Delivery Systems (12CSEDS)," awarded a contract to Sypris Electronics LLC to develop a Cryptographic Key Management System for the smart grid (Scalable Key Management Solutions for Critical Infrastructure Protection). Oak Ridge National Laboratory (ORNL) and Sypris Electronics, LLC as a result of that award entered into a CRADA (NFE-11-03562) between ORNL and Sypris Electronics, LLC. ORNL provided its Cyber Security Econometrics System (CSES) as a tool to be modified and used as a metric to address risks and vulnerabilities in the management of cryptographic keys within the Advanced Metering Infrastructure (AMI) domain of the electric sector. ORNL concentrated our analysis on the AMI domain of which the National Electric Sector Cyber security Organization Resource (NESCOR) Working Group 1 (WG1) has documented 29 failure scenarios. The computational infrastructure of this metric involves system stakeholders, security requirements, system components and security threats. To compute this metric, we estimated the stakes that each stakeholder associates with each security requirement, as well as stochastic matrices that represent the probability of a threat to cause a component failure and the probability of a component failure to cause a security requirement violation. We applied this model to estimate the security of the AMI, by leveraging the recently established National Institute of Standards and Technology Interagency Report (NISTIR) 7628 guidelines for smart grid security and the International Electrotechnical Commission (IEC) 63351, Part 9 to identify the life cycle for cryptographic key management, resulting in a vector that assigned to each stakeholder an estimate of their average loss in terms of dollars per day of system operation. To further address probabilities of threats, information security analysis can be performed using game theory implemented in dynamic Agent Based Game Theoretic (ABGT) simulations. Such simulations can be verified with the results from game theory analysis and further used to explore larger scale, real world scenarios involving multiple attackers, defenders, and information assets. The strategy for the game was developed by analyzing five electric sector representative failure scenarios contained in the AMI functional domain from NESCOR WG1. From these five selected scenarios, we characterized them into three specific threat categories affecting confidentiality, integrity and availability (CIA). The analysis using our ABGT simulation demonstrated how to model the AMI functional domain using a set of rationalized game theoretic rules decomposed from the failure scenarios in terms of how those scenarios might impact the AMI network with respect to CIA.

1. STATEMENT OF OBJECTIVES

1.1 SCALABLE KEY MANAGEMENT SOLUTIONS FOR CRITICAL INFRASTRUCTURE PROTECTION

Sypris' Smart Grid Security solution was awarded a contract to provide the Energy Sector with a Cryptographic Key Management System (CKMS) that leverages the best practices of fielded DoD key management systems to protect high value data, and command and control information, while also providing the capability to quickly recover from a cryptographic key compromise situation or to fend off cyber-attack by use of an autonomous key distribution scheme. This scalable key management solution was design to provide generation, distribution, and revocation of keys to allow the utilities to manage and distribute cryptographic keys to provide secure communication flows between and within the Smart Grid domains.

This Cryptographic Key Management System will allow the utilities to compartmentalize the secure communications (i.e., use different keys for different locations or types of devices) into groups to isolate high value Smart Grid devices to better manage the risk associated with a compromised key. For example, should a disclosure of a cryptographic key for a residential smart meter occur, devices in the Distribution, Transmission, and Bulk Generation domains remain secure. Utility Operations will have the capability to control the compartmentalization of the keyed network groups using CKMS based on their trade off assessment of less management overhead of group keys versus greater security achieved through compartmented Smart Grid devices.

Another key benefit of CKMS is the compartmentalization of key generation. By compartmentalizing the key generation capability at CKMS within the Utility Operations, the strength and validity of the key can be assured, while also leaving the processing power and entropy at a computer that can satisfy these requirements instead of at smaller devices that are situated within the network.

Autonomous secure key distribution within the network (across potentially unsecure communication links) is to be accomplished via a hybrid approach. Smart Grid devices will have a certificate (asymmetric) that includes a public and private key. CKMS will initiate a rekey of symmetric key through just a few affiliated Smart Grid devices. The Smart Grid devices will then automatically propagate the key to authorized peers, where the authorized peers will then automatically propagate to their authorized peers, and so on. Smart Grid devices that are no longer considered authorized will not receive the new symmetric key; and therefore, be keyed out of the network.

2. BENEFITS TO THE FUNDING DOE OFFICE'S MISSION

The Department of Energy Office of Electricity Delivery and Energy Reliability (DOE-OE) Cyber Security for Energy Delivery Systems (CSEDS) has established partnerships over the past several years with industry, government, national laboratories and universities to advance and secure the energy system technologies. The prevailing theme that has surfaced repeatedly is that critical energy infrastructures are vulnerable to cyber-attack, with potential consequences including significant interruption of economic activity or, even, to catastrophic loss of life. To take the necessary steps to remedy these vulnerabilities, the CSEDS program is developing tools and algorithms (herein referred to as technologies) to reduce the risk of energy disruptions due to cyber-attacks on control systems.

The CSES was originally sponsored with ORNL internal funding. Further refinements of the tool were implemented by interns in the Science Undergraduate Laboratory Internship (SULI) and Department of Homeland Security (DHS) Homeland Security related Science, Technology, Engineering and Mathematics (HS-STEM) programs, mentored by ORNL principal investigators. Current sponsorship comes from the Department of Energy Office of Electricity Delivery and Energy Reliability (DOE-OE)[*] Cyber Security for Energy Delivery Systems (CSEDS) industry led program (DE-FOA-0000359)[†] entitled "Innovation for Increasing Cyber Security for Energy Delivery Systems (12CSEDS)," awarded to Sypris Electronics LLC to develop a Cryptographic Key Management System for the smart grid (Scalable Key Management Solutions for Critical Infrastructure Protection)[‡] and a CRADA (NFE-11-03562) between ORNL and Sypris Electronics, LLC.

2.1 SUPPORT FOR THE DEVELOPMENT, TEST AND EVALUATION OF THE CKMS FOR EDS

2.1.1 Task Description

ORNL, under DOE authorization, provided technical support to Sypris Electronics in assessing scientific and technological issues as they relate to DE-FOA-0000359 "Innovation for Increasing Cyber Security for Energy Delivery Systems (I2CSEDS), Topic Area 2 - Centralized (Compartmentalized) Cryptographic Key Management" in the areas of development, testing and evaluation of risks and vulnerabilities and to assess future concepts in the subject domain with respect to technical and operational procedures in key management including key generation, key distribution, and key maintenance.

2.1.2 Problem Addressed

The DOE (including DHS) facilitated the development of the Roadmap to Secure Control Systems in the Energy Sector. The Roadmap synthesizes expert input from the control systems community, including owners and operators, commercial vendors, national laboratories, industry associations, and government agencies, to outline a coherent plan for improving cyber security in the energy sector. The plan provided by the Roadmap presents a vision and supporting framework of goals and milestones for protecting control systems over the period of 2005-2015. Specifically the Roadmap's Vision for Securing Control Systems in the Energy Sector is, by 2015 (time period extended to 2020),[§] control systems for critical

[*] http://energy.gov/oe/office-electricity-delivery-and-energy-reliability

[†] https://www.fedconnect.net/fedconnect/?doc=DE-FOA-0000359&agency=DOE, http://www.netl.doe.gov/business/solicitations/fy10#00359

[‡] https://www.sypriselectronics.com/information-security/cyber-security-solutions/smart-grid-security/

[§] http://energy.gov/sites/prod/files/Energy Delivery Systems Cybersecurity Roadmap_finalweb.pdf, Roadmap to Achieve Energy Delivery Systems Cybersecurity, September 2011, Energy Sector Control Systems Working group, page 22.

applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function. This effort overall targets the milestone: “Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy.” [**] To a lesser extent, the effort addresses the milestone: “Make available security test harness for evaluating next generation architectures and individual components.”[††]

2.1.3 Background

The Cyber Security for Energy Delivery Systems (CSEDS) program has established partnerships over the past several years with industry, government, national laboratories and universities to advance and secure the energy system technologies. The prevailing theme that has surfaced repeatedly is that critical energy infrastructures are vulnerable to cyber-attack, with potential consequences including significant interruption of economic activity or, even, to catastrophic loss of life. To take the necessary steps to remedy these vulnerabilities, the CSEDS program desires to develop tools and algorithms (herein referred to as technologies) to reduce the risk of energy disruptions due to cyber-attacks on control systems.

2.1.3 Scope and Technical Approach

CKMS objectives were to develop and demonstrate technology for the secure management of cryptographic keys within the energy-sector infrastructure. Cryptographic keys must be securely exchanged, then held and protected on either end of a communications link. This is currently challenging for a utility with numerous substations that must secure the intelligent devices that comprise complex control systems. This challenge is magnified by the necessity of cryptographic key distribution among the millions of intelligent meters that comprise the Advanced Metering Infrastructure (AMI) being implemented as part of the National Smart Grid initiative. Without a means for secure cryptographic key management no cryptographic solution can be widely deployed to protect the energy-sector infrastructure from cyber-attack.

ORNL provided technical support to Sypris Electronics during this project to ensure critical risk assessment and testing of products/prototypes developed during the course of the performance period including future concepts in the EDS with respect to performance, risks, economics and operations. The lack of sound relevant and practical security metrics is severely hampering progress in the assessing and countering cyber threats, and ultimately protecting critical research, technology and infrastructure. On this basis ORNL:

- Tested and evaluated the key generation process and will recommend mitigating solutions for any recognized key-based threats.
- Tested and evaluated the security and usability of the proposed distribution methodology and suggest changes or mitigating techniques that can address any identified issues.
- Tested and evaluated key maintenance as it relates to those keys already deployed. We identified three main challenges in key maintenance: revocation, redistribution of a new key, and leaked key recovery.

There will be instances where a key is compromised. Key revocation must be done without a malicious adversary interfering in the revocation of the compromised key, and this process should be designed to limit a leaked key's damage. After revocation, redistribution of the new key must be secure and reliable. ORNL:

- Tested and evaluated the security and reliability of key maintenance within the key management system.

[**] Ibid, page 25.

[††] Ibid, page 63.

ORNL conducted a phased approach. Our past and current research in cyber security modeling, testing and evaluation had addressed several key elements that are critical for the proposed research including development, modeling and testing of algorithms and products/prototypes by other members of the team with respect to cryptographic key management.

During Phase I, the team developed and demonstrated initial technologies for the secure management of risks and vulnerabilities of cryptographic keys within the energy-sector infrastructure. ORNL identified and assessed the risks associated with candidate solutions.

During Phase II, ORNL implemented risk mitigating protocols and procedures to reflect the advances made by the Sypris Electronics team.

During Phase III, ORNL further refined the protocols, procedures, and prototypes and expanded the evaluation risk management tasks to reflect the advances made by the Sypris Electronics team.

3. TECHNICAL DISCUSSION OF WORK PERFORMED

The Cyber Security Econometrics System, or CSES, is a cybernomics tool for determining Mean Failure Cost (MFC), which has been demonstrated in the cyber security domain (for example, a failure is assumed to be the result of a malicious action). The MFC is a vector that assigns to each system stakeholder the statistical mean of the random variable that represents the loss sustained by that stakeholder as a result of possible security failures. It provides goals and milestones for protecting control systems, and has been applied using the National Institute of Standards and Technology Interagency of Internal Reports (NISTIR) 7628 as a basis. This provides a comprehensive basis for choosing courses of action with highest risk reduction return on investment, quantifies security for comparison of architectures for subject domains of interest, and gives a rigorous methodology/tool combining root cause and impact analysis for managing risk to a degree commensurate with a stakeholder's potential losses. It is a system that provides a quantitative indication of reliability, performance and/or safety of a system that accounts for the criticality of each requirement as a function of one or more stakeholders' interests in the requirement.

The CSES has the following advantages: It accounts for variances existing among different stakeholders of the same system; for a given stakeholder, it accounts for variance among stakes attached to meeting each requirement; and for a given specification, (such as combination of commercial hardware/software), it accounts for variance that may exist among levels of verification and validation (certification, for example), performed on various components of said specification (certification activity may produce higher levels of assurance across different components of specification than others).

An effective security metric should identify and measure properties necessary for decision making, be measurable in a quantitative and repeatable way, be supported by a system or process capable of accurate and repeatable measurement, and be independently verifiable via an outside datum or reference. In addition, it could be inexpensive, in terms of time and cost, to gather and determine, it can be independently refereed or audited (in terms of compliance, accreditation and certification), and it could be scalable between individual devices and computers within an enterprise network. The Mean Failure Cost fills most of these requirements.

The CSES uses the MFC rather than the Mean-Time-To-Failure (MTTF). This is because the MTTF ignores variance in stakes among stakeholders, fails to recognize that different components have different stakes, even for same stakeholder, and fails to recognize validation and verification actions have different impacts with respect to different components of specification. The MFC, however, reveals how much each stakeholder stands to lose from mission value due to lack of security and allows an analyst to estimate the security of a system in terms of the loss each stakeholder stands to sustain in the event of system breakdowns. The CSES uses risk considerations to balance information, assurance, discipline, and flexibility, and to answer other "how much is enough" questions.

The lack of sound and practical security metrics has severely hampered progress in the development of secure systems, and the large number of potential threats and corresponding vulnerabilities that lurk in an information system represent a significant risk to any enterprise due to potential exploitation. This magnifies the need to create more diverse strategies and mechanisms.

The CSES was used to design, implement and control a complex system, and it triggers an alarm when the MFC for a particular stakeholder rises above acceptable levels. The CSES helped to illuminate information technology and industrial control systems policy decisions by identifying quantitative and qualitative sources of cost and value associated with candidate decisions.

4. SUBJECT INVENTIONS (AS DEFINED IN THE CRADA)

4.1 PATENTS PENDING (DURING CRADA PERIOD OF PERFORMANCE – SOLELY BY ORNL)

- Publication Tracking System[‡‡] (PTS) ID 47936 –"Cyberspace Security System for Complex Systems," R. K. Abercrombie, F. T. Sheldon, A. Mili, U.S. Patent Application No.: 14/134,949, December 19, 2013.
    - PTS ID 45113 – "Cyberspace Security Econometrics Systems Enhancements for Evaluating Architectures," R. K. Abercrombie, F. T. Sheldon, A. Mili, and K. Hauser, U.S. Patent Pending, Application No. 61/748,235, Provisional Patent, January 2, 2013.
- PTS ID 47935 – "Information Security Analysis Using Game Theory and Simulation," R. K. Abercrombie and B. G. Schlicher, U.S. Patent Application No.: 14/097,840, December 5, 2013.

4.2 PATENTS PENDING (BROUGHT TO CRADA BY ORNL)

- "Cyberspace Security System," R. K. Abercrombie, F. T. Sheldon, and E. M. Ferragut, U.S. Patent Application No. 13/443,702, April 10, 2012 (Claims allowed by US Patent Office Examiner May 2, 2014).
    - "Cyberspace Security Econometrics System (CSES) Expansion to Address Dependent Events," R. K. Abercrombie and E. M. Ferragut, U.S. Patent Pending (Provisional Patent), February 15, 2011.
- "System and Method for Implementing and Monitoring a Cyberspace Security Econometrics System and other Complex Systems," R. K. Abercrombie, F. T. Sheldon, and A. Mili, U.S. Patent Pending, May 12, 2008, US Patent Application No. 12/421,933, November 12, 2009.

4.3 ORNL INTELLECTUAL PROPERTY – INVENTION DISCLOSURES (DURING CRADA PERIOD OF PERFORMANCE – SOLELY BY ORNL)

- PTS ID 45370 – R. K. Abercrombie, B. G. Schlicher, and F. T. Sheldon, ID 201303155, DOE S-124,743 "Game Theoretic Agent Based Models (ABMs) for Impact Matrix and Threat Vector," August 22, 2013.
- PTS ID 45109 – R. K. Abercrombie and B. G. Schlicher, ID201303084, DOE S-124,668, "Risk Assessment Analysis Using Game Theory and Simulation (RAA-GT&S)," May 17, 2013.
- PTS ID 45370 – R. K. Abercrombie, B. G. Schlicher, and F. T. Sheldon, ID 201303155, DOE S-124,743 "Game Theoretic Agent Based Models (ABMs) for Impact Matrix and Threat Vector," August 22, 2013.
- PTS ID 45109 – R. K. Abercrombie and B. G. Schlicher, ID201303084, DOE S-124,668, "Risk Assessment Analysis Using Game Theory and Simulation (RAA-GT&S)," May 17, 2013.

[‡‡] ORNL Publication Tracking System (PTS) is the official source for recording documents. PTS sends to Office of Science and Technology (OSTI) metadata for ORNL reports when the Information Category is marked as "Unlimited." In addition, if a full-text document is uploaded into PTS, then a URL to that document is included in the metadata and made available to OSTI if the Document Access is "Public" and the Communication Type is not "Journal article."

- PTS ID 45107 – R. K. Abercrombie and B. G. Schlicher, ID201202961, DOE S-124,539 “Information Security Analysis Using Game Theory and Simulation,” October 16, 2012.
- PTS ID 45106 – R. K. Abercrombie, F. T. Sheldon, and A. Mili, ID 201202954, DOE S-124,531 “Cyberspace Security Econometrics Systems Enhancements for Evaluating Architectures (CSES-EA),” October 8, 2012.
- PTS ID 45105 – R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, and A. Mili , ID 201202949, DOE S-124,526 “Cyberspace Security Econometrics Systems Enhancements for Balancing (CSES-E),” September 25, 2012, and updated October 8, 2012.

4.4 ORNL INTELLECTUAL PROPERTY – INVENTION DISCLOSURES (BROUGHT TO CRADA BY ORNL)

- R. K. Abercrombie and F. T. Sheldon, Invention Disclosure Number: 201002514, DOE S-Number: 124,068, “Cyber Security Econometrics System (CSES) for Assessing/Ranking Threats,” December 3, 2010.
- R. K. Abercrombie and E. M. Ferragut, Invention Disclosure Number: 200902343, DOE S-Number: S-115,383, Cyberspace Security Econometrics System (CSES) Expansion to Address Dependent Events,” November 9, 2009.
- R. K. Abercrombie, F. T. Sheldon, and A. Mili, Invention Disclosure Number: 200902274, DOE S-Number: S-115,312, “Method of Providing Return on Investment for Cyber Security Econometrics System,” May 20, 2009.
- R. K. Abercrombie, F. T. Sheldon, and A. Mili, Invention Disclosure Number: 1300001980, DOE S-Number: S-111,598, “Cyber Security Econometrics System,” September 5, 2007.

4. 5 COPYRIGHT SOFTWARE (DURING CRADA PERIOD OF PERFORMANCE – SOLELY BY ORNL)

- PTS ID 45102 – Robert K. Abercrombie and Bob G. Schlicher, “Information Security Analysis Using Game Theory and Simulation (ISA-GT&S),” (Initial input, January 30, 2013, submitted July 22, 2013).
- PTS ID 45103 – Robert K. Abercrombie, Bob G. Schlicher, Frederick T. Sheldon, Margaret W. Lantz, Katie R. Hauser “Cyber Security Econometrics System (CSES),” (Initial input, September 24, 2012, adapted/corrected [applied to CRADA] October 16, 2012, Request to Assert Copyright UT-Battelle, January 23, 2013, submitted May 22, 2013).

4.6 COPYRIGHT SOFTWARE (BROUGHT TO CRADA BY ORNL)

- R. K. Abercrombie, F. T. Sheldon, A. Mili, and A. Ben Aissa, “Cyber Security Econometrics System (CSES)” submitted December 10, 2010.

4.7 PUBLICATIONS (DURING CRADA PERIOD OF PERFORMANCE)

- PTS ID 49200 – A. Ben Aissa, L. B. A. Rabai, R. K. Abercrombie, F. T. Sheldon, and A. Mili, “Quantifying Availability in SCADA Environments Using the Cyber Security Metric MFC,” 2014 Proceedings of the 9th Annual Cyber and Information Security Research Conference (CSIRC-2014), Oak Ridge, TN, April 8-10, 2014.

- PTS ID 46738 – R. K. Abercrombie, B. G. Schlicher, and F. T. Sheldon, "Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation," 2014 47th Hawaii International Conference on System Sciences (HICSS-47), Waikoloa, Big Island, Hawaii, January 6-9, 2014, Computer Society Press, 2014, pp. 2015-2024.
- PTS ID 49753 – C. Vishik, F. T. Sheldon, and D. Ott, "Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment," in H. Reimer, N. Pohlmann, and W. Schneider (Eds.), ISSE 2013 Securing Electronic Business Processes, Springer Fachmedien Wiesbaden, 2013, pp. 133-147 (DOI: 10.1007/978-3-658-03371-2_12).
- R. K. Abercrombie, F. T. Sheldon, B. G. Schlicher, and H. Aldridge, "Resilient Cyber-Physical Systems Risk Assessment, A Game Theoretic Simulation Approach," 1st International Symposium on Resilient Cyber Systems 2013 (Submitted April 22, 2013, withdrawn), San Francisco, CA, August 13-15, 2013.
- PTS ID 47805 – R. K. Abercrombie, B. G. Schlicher, and F. T. Sheldon, "Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation," presentation at 2014 47th Hawaii International Conference on System Sciences (HICSS-47), Waikoloa, Big Island, Hawaii, January 7, 2014.
- PTS ID 45075 – R. K. Abercrombie, F. T. Sheldon, and B. G. Schlicher, "Information Security Analysis for CKMS Using Game Theory and Simulation – Phase II and Phase III," ORNL/TM-2013/306, June 11, 2013.
- PTS ID 38393 – R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Failure Impact Analysis of Key Management in AMI Using Cybernomic Situational Assessment (CSA)," 2013 Proceedings of the 8th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2013), Oak Ridge, TN, October 30 – November 2, 2012, rescheduled to January 8-10, 2013 (DOI: 10.1145/2459976.2459998).
- PTS ID 40930 – R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Failure Impact Analysis of Key Management in AMI Using Cybernomic Situational Assessment (CSA)," Briefing authored by R. K. Abercrombie for presentation at 8th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2013), Oak Ridge, TN, January 8-10, 2013 (DOI: 10.1145/2459976.2459998).
- PTS ID 38394 – M. Duren, H. Aldridge, R. K. Abercrombie, and F. T. Sheldon, "Designing and Operating Through Compromise: Architectural Analysis of CKMS for the Advanced Metering Infrastructure," 2013 Proceedings of the 8th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2013), Oak Ridge, TN, October 30 – November 2, 2012, rescheduled to January 8-10, 2013 (DOI: 10.1145/2459976.2460031).
- PTS ID 39156 – R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Risk Assessment Methodology Based on the NISTIR 7628 Guidelines," Proceedings of 46th Hawaii International Conference on System Sciences (HICSS-46), Wailea, Maui, Hawaii, January 7-10, 2013, Computer Society Press, 2012, pp. 1802-1811, (DOI: 10.1109/HICSS.2013.466, PTS ID 40931 presentation). Nominated best paper and received Runner-Up Acknowledgment.
- PTS ID 49031 – R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Risk Assessment Methodology Based on the NISTIR 7628 Guidelines," Briefing presented by R. K. Abercrombie at 46th Hawaii International Conference on System Sciences (HICSS-46), Wailea, Maui, Hawaii, January 7-10, 2013, Computer Society Press, 2012, pp. 1802-1811, (DOI: 10.1109/HICSS.2013.466). Nominated best paper and received Runner-Up Acknowledgment.
- PTS ID 40678 – A. Ben Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Defining and Computing a Value Based Cyber-Security Measure," Information Systems and E-Business Management, Volume 10, Issue 4, pp 433-453, Springer London: December 1, 2012, (Online First, April 23, 2011), (DOI:10.1007/s10257-011-0177-1).

- PTS ID 40029 – R. K. Abercrombie and F. T. Sheldon, “ORNL CRADA - Status Briefing Update (Oct. 2012) on CEDS Portion of Project - Topic 2 Cryptographic Key Management System (CKMS),” ORNL/LTR-2012/538, Purdue University, West Lafayette, IN, October 4, 2012 (Distributed October 2012).
- PTS ID 34735 – B. G. Schlicher and R. K. Abercrombie, "Information Security Analysis Using Game Theory and Simulation," Proceedings of the 2012 International Conference on Security and Management (SAM '12), 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP '12), Las Vegas, NV, July 16-19, 2012, pp 540-546.
- PTS ID 37664 – B. G. Schlicher and R. K. Abercrombie, "Information Security Analysis Using Game Theory and Simulation," Presentation at the 2012 International Conference on Security and Management (SAM '12), 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP '12), Las Vegas, NV, July 16-19, 2012.
- PTS ID 39920 – R. K. Abercrombie and F. T. Sheldon, “ORNL CRADA - Phase I Deliverable Report (March 2012) on CEDS Project - Topic 2 Cryptographic Key Management System (CKMS),” ORNL/LTR-2012/256, March 2012.
- PTS ID 33066 – R. K. Abercrombie, F. T. Sheldon, H. Aldridge, M. Duren, E. Bertino, A. Kulatunga, and U. S. Navaratne, “Secure Cryptographic Key Management System (CKMS) Considerations for Smart Grid Devices,” Proceedings of 7th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2011), ACM International Conference Proceeding Series, Oak Ridge, TN October 12-14, 2011 (DOI:0.1145/2179298.2179364). D. Dasgupta, M. H. Ali, R. K. Abercrombie, B. G. Schlicher, F. T. Sheldon, and M. Carvalho, “Secure VM for Monitoring Industrial Process Controllers,” Proceedings of 7th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2011), ACM International Conference Proceeding Series, Oak Ridge, TN October 12-14, 2011 (DOI:0.1145/2179298.2179341).
- PTS ID 34187 – F. T. Sheldon, H. Aldridge, M. Duren, L. M. Hively, D. Dasgupta, and R. K. Abercrombie, "Adaptive Bio-Inspired Resilient Cyber-Physical Systems: R&D Prospective," International Symposium on Resilient Control Systems, Cyber Awareness, Boise, ID, August 9-11, 2011.

4.8 PUBLICATIONS (BROUGHT TO CRADA BY ORNL)

- PTS ID 36253 – A. Ben Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, “Defining and Computing a Value Based Cyber-Security Measure,” Proceedings of 2nd Kuwait Conference on e-Services and e-Systems (KCESS 2011), ACM International Conference Proceeding Series, Kuwait University, Kuwait, April 5-7, 2011 (DOI:0.1145/2107556.2107561).
- PTS ID 27295 – R. K. Abercrombie, E. M. Ferragut, F. T. Sheldon, and M. R. Grimaila, “Addressing the Need for Independence in the CSE Model,” Proceedings of 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2011) - Symposium Series on Computational Intelligence (IEEE SSCI 2011), Paris, France, April 11-15, 2011.
- PTS ID 26428 – R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Validating Cyber Security Requirements: A Case Study," IEEE Proceedings of the 44th Annual Hawaii International Conference on System Sciences (HICSS-44), Koloa, Kauai, Hawaii, January 4-7, 2011, Computer Society Press, 2011 pp. 1-10.
- PTS ID 24770 – R. K. Abercrombie, F. T. Sheldon, and M. R. Grimaila, "A Systematic Comprehensive Computational Model for Stake Estimation in Mission Assurance," Proceedings of International Workshop on Mission Assurance: Tools, Techniques, and Methodologies (MATTM 2010), 2nd IEEE International Conference on Social Computing

(SocialCom 2010) / 2nd IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT 2010), Minneapolis, MN, August 20-22, 2010, Computer Society Press, pp. 1153-1158.

- PTS ID 24375 – R. K. Abercrombie, "Identification and Monitoring of Critical Success Factors for Effective e-Commerce, e-Learning, e-Training, and e-Democracy," Proceedings of 1st International Conference on Electronic Management, Tripoli, Libya, June 1-3, 2010.
- PTS 24228 – A. Ben Aissa, A. Mili, R. K. Abercrombie, and F. T. Sheldon, "Modeling Stakeholder/Value Dependency through Mean Failure Cost," Proceedings of 6th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2010), ACM International Conference Proceeding Series, Oak Ridge, TN April 21-23, 2010.
- PTS ID 24230 – A. Ben Aissa, A. Mili, F. T. Sheldon, and R. K. Abercrombie, "Software Requirements for a System to Compute Mean Failure Cost," Proceedings of 6th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2010), ACM International Conference Proceedings Series, Oak Ridge, TN April 21-23, 2010.
- PTS ID 23295 – A. Ben Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Quantifying Security Threats and Their Potential Impacts: A Case Study," Innovations in Systems and Software Engineering, Volume 6, Number 4, pp. 269-281 (December 2010).
- PTS ID 11711 (Adapted) – F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," IEEE Intelligence and Security Informatics 2009 (ISI 2009), Keynote presentation, presented by F. T. Sheldon, Dallas, TX, June 11, 2009.
- PTS ID 15581 – A. Ben Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Quantifying Security Threats and Their Impact," Proceedings of 5th Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW-2009) - Theme: Cyber Security and Information Intelligence Challenges and Strategies, ACM International Conference Proceeding Series, Oak Ridge, TN April 13, 2009.
- PTS ID 14164 – R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Managing Complex IT Security Processes with Value Based Measures," Proceedings of 2009 IEEE Symposium on Computational Intelligence in Cyber Security (CICS '09), Nashville, TN, April 1, 2009.
- PTS ID 11712 – F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," IEEE Proceedings of the 42nd Annual Hawaii International Conference on System Sciences (HICSS-42), Waikoloa, Big Island, Hawaii, January 5-8, 2009, Computer Society Press, 2009 (10 pages).
- PTS ID 12589 – R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Synopsis of Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission Value," Proceedings of the 11th IEEE High Assurance Systems Engineering Symposium (HASE'08), Nanjing, China, pp. 479-482, December 3-5, 2008.
- PTS 11708 – F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," in Proceedings of 4th Annual Cyber Security and Information Intelligence Research Workshop - Theme: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, ACM International Conference Proceeding Series, Vol. 288, Oak Ridge, TN, May 14, 2008.
- PTS ID 11711 – F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," Briefing: Appendix in Proceedings of 4th Annual Workshop on Cyber Security and Information Intelligence Research Workshop - Theme: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, ACM International Conference Proceeding Series, Vol. 288, Oak Ridge, TN, May 14, 2008.

4.9 INVITED TALKS/PRESENTATIONS (DURING AND JUST PRIOR TO CRADA)

- R. K. Abercrombie and B. G. Schlicher, "Risk Assessment Methodology - All Hazards Econometrics System (AHES, pronounced Oz)," DOE Microgrid R&D Program Quarterly Meeting, Oak Ridge National Laboratory, Oak Ridge, TN, November 18, 2013.
- Authored by R. K. Abercrombie; F. T. Sheldon represented team and presented, "Failure Impact Analysis Using Cybernomic Analytics," Research Lecture: Milibo Webinar published: http://www.youtube.com/watch?v=ULu88QY4RTM, June 21, 2013.
- PTS ID 45010 – R. K. Abercrombie, F. T. Sheldon, and B. G. Schlicher, "Information Security Analysis for CKMS Using Game Theory and Simulation," Invited Talk authored by R. K. Abercrombie, presented at 1st International Symposium on Resilient Cyber Systems, San Francisco, California, August 13-15, 2013.
- PTS ID 39781 – R. K. Abercrombie and B. G. Schlicher, "Big Data, Social Networks, and Analytics (Big Data Science at ORNL)," University of Memphis Center for Information Assurance Cyber Security Expo, Invited Keynote Speaker, October 19, 2012.
- PTS ID 45099 – R. K. Abercrombie, "SCADA Security: Workshop/Tutorial on Automation and Control Device/SCADA," Invited Guest Panelist, FedEx Institute of Technology, University of Memphis, Memphis, TN, October 18, 2012.
- R. K. Abercrombie, "Recent Findings and Impressions with Respect to ORNL Key Roles in DOE Cyber Security For Energy Effort," Seminar on Cyber and Physical Security of Critical Infrastructure, Keynote Speaker, Herff College of Engineering and The Center for Information Assurance, University of Memphis, Memphis, TN October 7, 2011.
- PTS ID 24375 – R. K. Abercrombie, "Identification and Monitoring of Critical Success Factors for Effective e-Commerce, e-Learning, e-Training, and e-Democracy," Keynote Speaker, 1st International Conference on Electronic Management, Tripoli, Libya, June 1-3, 2010.
- PTS ID 11711 (Adapted) F. T. Sheldon, R. K. Abercrombie, and A. Mili, "Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," IEEE Intelligence and Security Informatics 2009 (ISI 2009), Keynote presentation, presented by F. T. Sheldon, Dallas, TX, June 11, 2009.

5. CONCLUSIONS

The Cyber Security Econometrics System, or CSES, is a cybernomics tool for determining Mean Failure Cost (MFC), which has been demonstrated in the cyber security domain (for example, a failure is assumed to be the result of a malicious action). The MFC is a vector that assigns to each system stakeholder the statistical mean of the random variable that represents the loss sustained by that stakeholder as a result of possible security failures. It provides goals and milestones for protecting control systems, and has been applied using the NISTIR 7628 as a basis. This provides a comprehensive basis for choosing courses of action with highest risk reduction return on investment, quantifies security for comparison of architectures for subject domains of interest, and gives a rigorous methodology/tool combining root cause and impact analysis for managing risk to a degree commensurate with a stakeholder’s potential losses. It is a system that provides a quantitative indication of reliability, performance and/or safety of a system that accounts for the criticality of each requirement as a function of one or more stakeholders' interests in the requirement.

The CSES has the following advantages: It accounts for variances existing among different stakeholders of the same system; for a given stakeholder, it accounts for variance among stakes attached to meeting each requirement; and for a given specification, (such as combination of commercial hardware/software), it accounts for variance that may exist among levels of verification and validation (certification, for example), performed on various components of said specification (certification activity may produce higher levels of assurance across different components of specification than others).

An effective security metric should identify and measure properties necessary for decision making, be measurable in a quantitative and repeatable way, be supported by a system or process capable of accurate and repeatable measurement, and be independently verifiable via an outside datum or reference. In addition, it could be inexpensive, in terms of time and cost, to gather and determine, it can be independently refereed or audited (in terms of compliance, accreditation and certification), and it could be scalable between individual devices and computers within an enterprise network. The Mean Failure Cost fills most of these requirements.

The CSES uses the MFC rather than the Mean Time To Failure (MTTF). This is because the MTTF ignores variance in stakes among stakeholders, fails to recognize that different components have different stakes, even for same stakeholder, and fails to recognize validation and verification actions have different impacts with respect to different components of specification. The MFC, however, reveals how much each stakeholder stands to lose from mission value due to lack of security and allows an analyst to estimate the security of a system in terms of the loss each stakeholder stands to sustain in the event of system breakdowns. The CSES uses risk considerations to balance information, assurance, discipline, and flexibility, and to answer other “how much is enough” questions.

The lack of sound and practical security metrics has severely hampered progress in the development of secure systems, and the large number of potential threats and corresponding vulnerabilities that lurk in an information system represent a significant risk to any enterprise due to potential exploitation. This magnifies the need to create more diverse strategies and mechanisms.

The CSES may be used to design, implement and control a complex system, and it triggers an alarm when the MFC for a particular stakeholder rises above acceptable levels. The CSES will help to illuminate information technology policy decisions by identifying quantitative and qualitative sources of cost and value associated with candidate decisions.

5.1 POSSIBLE ALTERNATIVE

Information security (IS) continues to evolve in response to disruptive changes with a persistent focus on information-centric controls. A healthy debate is needed to address balancing endpoint and network protection, with a goal of improved enterprise / business risk management. IS analysis can be performed using game theory implemented as dynamic simulations of ABMs. Such simulations can be verified against the results from game theory analysis and further used to explore larger scale, real world scenarios involving multiple attackers, defenders, and information assets. We've concentrated our analysis on the AMI domain of which the NESCOR WG1 has currently documented 29 failure scenarios [1]. The strategy for the game was developed by selecting/analyzing five representative failure scenarios of the twenty-nine. We classified each of the five into one or more of three specific threats that may affect the confidentiality, integrity or availability of the system. Analysis using our ABM theoretic simulation [2] demonstrated that the AMI functional domain was simply and accurately modeled, the game theoretic rules were decomposed and analyzed as to their respective impacts (confidentiality, integrity, and availability) on the AMI network [3].

When considering the cost of mitigations as they address either some of the most pernicious or the most likely of threats we need quantitative indications of reliability, performance, and/or safety/security (aka resiliency). The CSES approach accounts for (i.e., by deriving MFC) the criticality of each requirement as a function of one or more stakeholders' interest in that requirement, the underlying infrastructure (component-by-component) and an estimate of the likelihood of threats (combined with an existing vulnerability) emerging. By using the AD-ABS approach (Fig. 1) we hope to establish a methodology for discovering insights through sensitivity analysis (perhaps as an approximation of the vertex cover problem) the set of paths of least resistance to disrupting/failing a mission requirement [4]. In this way, we can have higher confidence and precision for estimates of threat emergence probability. Then, combined with the results from CSES, we plan to develop a comprehensive bottom line basis for asset owners to decide in what and how much to invest, choosing courses of actions that reduce the most risks for the lowest cost.

5.1.1 Increasing Reliance on Advanced Technology

Increasing reliance on smart grid advanced technology capabilities and the worsening threat environment mean that asset owners are under pressure to invest more in information/cyber security.

A **challenge** is that the choices are hard: money is tight, objectives are not clear, and there are many relevant experts and stakeholders. A significant proportion of the research in security economics is about helping people and organizations make better security investment and policy decisions. Yet there is no clear guidance or method that helps those asset owners understand the cost of implementing security mitigations (i.e., pricing), nor a clear basis for return on investment (ROI). One question that is coming up more and more is the impact of methods (using economic/ cost models) that are based on Cost/ROI/MFC (mean failure cost) in helping decision makers choose from alternative courses of action and investments.

The opportunity: The smart grid (energy delivery system) provides a basis for looking at a realistic security problem and it's associated (information/cyber and physical) infrastructure toward encompassing the broad range of different factions included as justifications for the decisions that such stakeholders must make. The security professional is an important and influential stakeholder in the organization's decision-making process and arguably has a more complete understanding of the problem. They also may be more suitable for persuading a broader business audience in regards to hardening the critical infrastructure and potentially avoiding costly calamities.

The theoretical foundation: Cases similar to the one presented above can feed important information for adjusting assumptions and techniques in theoretical models evaluating more general economic mechanisms. These mechanisms, in turn, can be applied to improve and validate metrics and risk analysis for concrete situations.

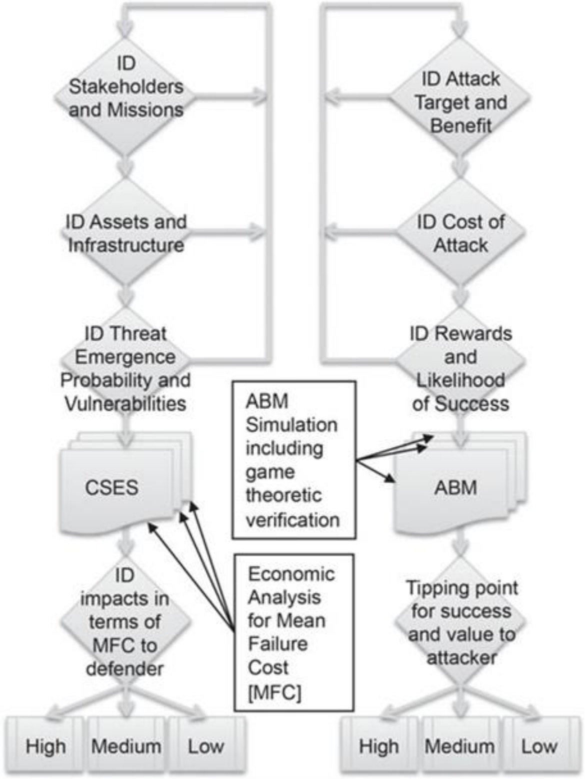
ID Stakeholders and Missions
ID Assets and Infrastructure
ID Threat Emergence Probability and Vulnerabilities
CSES
ID impacts in terms of MFC to defender
High
Medium
Low
ID Attack Target and Benefit
ID Cost of Attack
ID Rewards and Likelihood of Success
ABM
Tipping point for success and value to attacker
High
Medium
Low
ABM Simulation including game theoretic verification
Economic Analysis for Mean Failure Cost [MFC]

Fig. 1. Linking ABM Simulation with economic impact analysis.

6. REFERENCES

1. A. Lee, "Electric Sector Failure Scenarios and Impact Analyses - Draft," in National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1 vol. Version 0.9, ed. Washington, D.C., 2013.
2. G. Schlicher and R. K. Abercrombie, "Information Security Analysis Using Game Theory and Simulation," in WORLDCOMP'12 - The 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing; SAM'12 - 2012 International Conference on Security and Management, Las Vegas, NV, 2012, pp. 540-546.
3. R. K. Abercrombie, B. G. Schlicher, and F. T. Sheldon, "Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation," in 47th Hawaii International Conference on System Sciences (HICSS-47), Waikoloa, Big Island, HI USA, 2014, pp. 2015-2024.
4. C. Vishik, F. T. Sheldon, and D. Ott, “Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment,” in H. Reimer, N. Pohlmann, and W. Schneider (Eds.), ISSE 2013 Securing Electronic Business Processes, Springer Fachmedien Wiesbaden, 2013, pp. 133-147.

ORNL/TM-2014/131

INTERNAL DISTRIBUTION

1. R. K. Abercrombie
2. A. D. Brock
3. S. S. Gleason
4. B. Kay
5. T. J. King, Jr.
6. R. H. Morris
7. M. J. Paulus
8. S. J. Prowell
9. B. G. Schlicher
10. ORNL Office of Technical Information and Classification (L. K. Laymance)

EXTERNAL DISTRIBUTION

11. C. Hawk, Program Manager, Cyber Security for Energy Delivery Systems, Office of Electricity Delivery and Energy Reliability, Research and Development Division, 1000 Independence Ave. SW Washington DC 20585
12. S. Peters, CRADA Number NFE-11-03562 Participant PI, Project Director, Sypris Electronics, LLC, 10901 N. McKinley Drive, Tampa, Florida, 33612
13. F. T. Sheldon, 9436 Polo Club Lane, Knoxville, TN 37922
14. U.S. Department of Energy ORNL Site Office, Mission Integration & Projects Division (R. T. Chung), P. O. Box 2008, MS-6269, Oak Ridge, TN 37831-6269
15. U.S. Department of Energy ORNL Site Office, Mission Integration & Projects Division (M. H. Rawlins), P. O. Box 2008, MS-6269, Oak Ridge, TN 37831-6269