Failure Impact Analysis of Key Management in AMI Using Cybernomic Situational Assessment (CSA)

Robert K. Abercrombie
Frederick T. Sheldon
Oak Ridge National Laboratory
P. O. Box 2008
Oak Ridge, TN 37831-6085
+001-865-241-6537/576-1339
abercrombier@ornl.gov
sheldonft@ornl.gov

Katie R.Hauser[1]
Margaret W.Lantz[1]
Oak Ridge National Laboratory
P. O. Box 2008
Oak Ridge, TN 37831-6085
+001-509-432-3874/540-435-8505
khauser@hmc.edu
lantzmw@dukes.jmu.edu

Ali Mili
Department of Computer Science
College of Computing Sciences
New Jersey Institute of Technology
Newark, NJ 07102-1982
+001-973-596-5215
mili@cis.njit.edu

ABSTRACT

In earlier work we presented a metric that quantifies system security in terms of the average loss per unit of time incurred by a stakeholder of the system as a result of security threats. The computational infrastructure of this metric involves system stakeholders, security requirements, system components and security threats. To compute this metric, we estimate 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 apply this model to estimate the security of the Advanced Metering Infrastructure (AMI), by leveraging the recently established NISTIR 7628 guidelines for smart grid security and IEC 63351, Part 9 to identify the life cycle for cryptographic key management, resulting in a vector that assigns to each stakeholder an estimate of their average loss in terms of dollars per day of system operation.

Categories and Subject Descriptors

D.4.6, D.6.5 [**Security and Protection**]

General Terms

Algorithms, Measurement, Performance, Design, Economics, Reliability, Experimentation, Security, Theory, Verification.

Keywords

Cyber Security Metrics, Risk Management, Information Security

1. INTRODUCTION AND PAPER ORGANIZATION

DOE's vision states that by 2020, resilient energy delivery systems are to be designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions [1]. This strategy includes: building a culture of security; assessing and monitoring risk; developing and implement new protective measures to reduce risk; managing incidents; and sustaining security improvements.

According to the International Energy Agency [2], the widespread deployment of smart grids is crucial to achieving a more secure and sustainable energy future. The benefits should include greater grid reliability, integration of renewable generation and plug-in vehicles, reduced electricity peak demand, and stronger cyber security.

However, US energy utilities face a monumental challenge as they address compliance with the North American Electric Reliability Corporation's Critical Infrastructure Protection (CIP) standards. Consequently, utilities have had to establish electronic security perimeters (ESPs) to monitor, protect, and control their infrastructure.

Utilities need relevant security that helps reduce the risks of cyber threats, which are often agile, multifaceted, well resourced, and persistent. In addition, any efforts to modernize and protect such a critical cyber physical infrastructure must balance the need for better performance and lower cost with better security.

A case in point is the current wave of smart meters (SMs) being deployed; more than 20 million SMs have been installed in the US (www.eia.gov). Industry representatives have raised concerns that cryptographic-key-management systems only support SMs and might not scalably interoperate among other smart-grid domains. (Such domains include energy control systems; wide-area monitoring, protection, and control; synchronized phasor measurements; distributed and renewable energy resources; electric transportation; and energy storage.)

For situations such as these to change, stakeholders need tools, including cyber economic metrics and incentives, for rationalizing the development of more adaptive and resilient Internet infrastructures. One such possible tool is the 2011 Roadmap to

[1] Department of Homeland Security (DHS) Homeland Security related Science, Technology, Engineering and Mathematics (HS-STEM) Summer Intern at Oak Ridge National Laboratory. Katie Hauser is currently a student at Harvey Mudd College and Margaret Lantz is currently a student at James Madison University.

The submitted manuscript has been authored by a contractor of the U.S. Government under contract DE-AC05-00OR22725. Accordingly, the U.S Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

CSIIRW'12, October 30 – November 2, Oak Ridge, Tennessee, USA
Copyright © 2012 ACM 978-1-4503-1687-3 … $15.00

Achieve Energy Delivery Systems Cyber Security [1]. "Increased insight from private-public collaborations will allow us to better protect the nation's energy delivery systems that keep our lights on and the power flowing," said US Department of Energy Secretary Steven Chu. "The 2011 Road map takes the necessary steps to strengthen the security and reliability of our country's electric grid, in a climate of increasingly sophisticated cyber incidents."

Quantifying the return on investments in cyber security is difficult. Moreover, we know of no comprehensive plan to track the cost of losses due to failures caused by cyber security breaches in the energy sector.

Yet, if the smart grid undergoes only a generational upgrade (that is, minimizing cost and maximizing performance) without designed-in security and resiliency (the ability, among others, to quickly and cost effectively adapt to new threats), then the cost to respond to new attacks might be prohibitive. Tracking the cost of security breaches is essential to determining inherent risk and developing effective incentives toward making cyber security ubiquitous. In this way, we can know whether the savings from a smarter, more efficient grid will offset the costs resulting from disruptive cyber-intrusions.

Over the last several years, ORNL has been developing and refining the Cyberspace Security Econometrics System (CSES) [3, 4]. The system has evolved to the state that we are now ready to use CSES as a useful tool for evaluating Cryptographic Key Management Systems (CKMS) and Advanced Metering Infrastructure (AMI) systems. In this paper, we develop an example of CSES tailored to an AMI system. To accomplish this, we identify the security requirements in Section 2. In Section 3, 4, 5 and 6 we determine the stakeholders, requirements, components, and threats, then populate the matrices with justified values from [5]. Initially, one would think this is a very daunting task, but when investigating the AMI at a higher level rather than trying to consider every piece of hardware and software involved, we address a straight-forward strategy. To accomplish the task, we utilize standards and guidelines for smart grid security [6]. This allows us to choose the stakeholders, requirements, components, and threats for the example. The next challenge is to estimate the probability of the threats. In Section 5, we review the literature and select an industry standards group (IEC 63351, Part 9) to identify the life cycle for cryptographic key management [7]. From this subset, we populate the stakes, dependency, and impact matrices, and the threat vector (Section 7). Each Stakeholder's Mean Failure Cost is then computed. In Section 8, we address the metric Mean Failure Cost (MFC) and finally summarize conclusions.

2. SECURITY REQUIREMENTS

Following Title 44 of the U.S. Code [8], three security requirements are imposed upon the AMI and CKMS and are more tightly defined , as follows:

- Confidentiality – ensure that only authorized parties are able to access cryptographic keys. A loss of confidentiality could result in unauthorized parties gaining access to any information that is protected by the key, including but not limited to personally identifiable information (PII) about a customer and customer energy usage data.
- Integrity – ensure that cryptographic keys are not altered by unauthorized parties. A failure of integrity may result in such consequences as power being shut off to a meter.
- Availability – ensure that cryptographic keys are available whenever needed. When availability is not met, possible consequences include power being shut off to a meter.

3. REFERENCEWORK – STAKEHOLDERS' ESTIMATED LOSS

We recognize five stakeholders in the system, as provided in [6], namely, a power utility, an AMI vendor, a CKMS provider, a corporate customer, and a critical infrastructure customer (e.g. a hospital). In [5], we consider how much money each stakeholder stands to lose when one of the security requirements has not been met. For the purposes of this example, we used publicly available data to estimate the stakes for each stakeholder. We describe this estimation process for each stakeholder.

4. STAKES MATRIX (ST)

We recognize five stakeholders in the system, as provided in [6], namely, the power utility, the AMI vendor, the CKMS provider, a corporate customer, and a residential customer. In this example we substitute residential customer with a critical infrastructure customer (e.g., a hospital) and populate the stakes matrix (Table 1), we consider how much money each stakeholder stands to lose when one of the security requirements has not been met. For the purposes of this example, we used publicly available data to estimate the stakes for each stakeholder from [5], assuming that the loss from the hospital is ten times that of a corporate customer.

5. DEPENDENCY MATRIX (DP)

For the components of the system we take the Smart Grid Architecture Logical Interface Categories 13-18 relevant to AMI from the NISTIR 7628, Guidelines for Smart Grid Cyber Security [6]. The component specifics are detailed in the Table 2 below.

Although other possible sets of components exist for AMI systems, we choose to pursue this route because the NISTIR 7628 contains extensive details about each of the interface categories and we want to remain at a high level of abstraction for the purposes of this example. Another convenience of the categories is that the NISTIR ranks how important Confidentiality, Integrity, and Availability are within each interface category, which aids in populating the Dependency Matrix (Table 3). As research and development progress, it will be important to refine the values in this and all of the matrices to better reflect physical AMI systems.

Table 1. Stakes Matrix: Stakeholders vs. Requirements

Stakes (ST)		Requirements			
		Confidentiality	**Integrity**	**Availability**	**No Requirement Failure**
Stakeholders	Utility	$762,044	$10,000	$10,000	$0
	AMI Vendor	$762,044	$100,000	$5,000	$0
	CKMS Provider	$762,044	$100,000	$200,000	$0
	Corporate Customer	$31,140	$1,363	$1,363	$0
	Critical Infrastructure Customer	$311,400	$13,630	$13,630	$0

Note: The NRF column represents the cost associated when no requirement fails and is provided for completeness (to explicitly denote this case).

Table 2. Advanced Metering Infrastructure related interfaces

Component Details	
Category	**Description – Interfaces between…**
13	Systems that use the AMI network
14	Systems that use the AMI network for functions that require high availability
15	Systems that use customer site networks
16	External systems and the customer site
17	Systems and mobile field crew equipment
18	Metering equipment

Table 3. Dependency Matrix

Dependency (DP)		**Components (Smart Grid Architecture AMI Logical Interface Categories from NISTIR 7628)**						
		13	**14**	**15**	**16**	**17**	**18**	**No Component Failure (NCF)**
Requirements	**C**	.3	.3	.1	.3	.1	.1	0
	I	.3	.3	.2	.2	.3	.3	0
	A	.1	.3	.2	.1	.2	.1	0
	NRF	.3	.1	.5	.4	.4	.5	1

Note: the NRF row represents the case when a component fails but does not affect the associated requirement. The NCF column represents the case when no component fails.

The only result expected in the case that no component fails is that no requirement is violated, so the NCF column is filled with zeros except for the final cell, which links NCF and NRF with a probability of 1. For comparison, if an interface in Category 15 experiences a failure and this failure causes no more than one requirement to be violated, then there is probability 0.2 that the violated requirement be integrity..

6. IMPACT MATRIX (IM)

In determining the threats against the AMI system, we consult Part 9 of the IEC 62351 series [7] which specifies how to generate, distribute, revoke and handle digital certificates, cryptographic keys to protect digital data and communication. We enumerate the life cycle of key management as shown in Figure 1 into threats categories (Tx) as follows: T1 Generation, T2 Registration, T3 Certification, T4 Distribution, T5 Installation, T6 Storage, T7 Derivation, T8 Update, T9 Archiving, T10 Deregistration, T11 Key Revocation, T12 Destruction, and T13 No Threat.

From these scenarios, according to Part 9 of the IEC 62351 Draft Standard, we extract the threat categories for the system detailed in Table 4. For the purposes of this example, Part 9 of the IEC 62351 Draft is sufficient for estimating threat categories. This is a reasonable assumption since key management is a mature discipline. We do expect the Component Categories from the NISTIR 7628 to evolve [6]. Further revision of the IM Matrix is undoubtedly necessary as failure scenarios are simulated and studied.

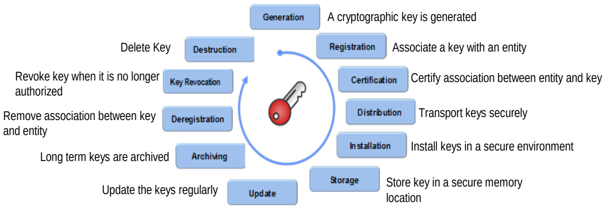
Generation
A cryptographic key is generated
Delete Key
Destruction
Registration
Associate a key with an entity
Revoke key when it is no longer authorized
Key Revocation
Certification
Certify association between entity and key
Remove association between key and entity
Deregistration
Distribution
Transport keys securely
Long term keys are archived
Archiving
Installation
Install keys in a secure environment
Storage
Store key in a secure memory location
Update the keys regularly
Update

Figure 1. Life cycle of key management.

The IM Matrix reads in a manner similar to that of the DP Matrix. For example, we consider the situation in which threat T1 has materialized. Assuming threat T1 may cause no more than one component to fail, there is a probability of 0.21 that the component that fails be component 13. .

7. THREAT VECTOR (PT)

We assume no threat materializing during a day is probably most likely as shown in Table 5. Since the life cycle of key management is a mature discipline, we assume the threat against the life cycle to be reasonably distributed among the 12 threat categories. As the smart grid and AMI mature, the populating of the Threat Vector will use empirical results to verify these probabilities.

8. MEAN FAILURE COST (MFC) – RESULTS

The ST matrix contains the stakes that each stakeholder has in each of the requirements, where each row belongs to a stakeholder and each requirement has a column. Each entry in the matrix is an amount of money that one of the stakeholders stands to lose if one of the requirements is not met. In the DP matrix, the requirements shift to become the rows, and the components are the columns. The entries in the matrix represent the likelihood that a requirement will be violated given that a certain component has failed. The components shift to become the rows of the IM matrix, in which the threats are the columns. Each entry approximates the probability that a component will fail given that a certain threat has materialized. Lastly, the PT vector is a single column populated by the probabilities of each threat materializing within a specified time frame.

Table 4. Impact Matrix

Impact (IM)		**Threats**												
		T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**	**T10**	**T11**	**T12**	**No Threat**
Components	**13**	.21	.10	.14	.14	.14	.14	.14	.14	.14	.14	.14	.14	0
	14	.02	.26	.14	.14	.14	.14	.14	.14	.14	.14	.14	.14	0
	15	.01	.08	.14	.14	.14	.14	.14	.14	.14	.14	.14	.14	0
	16	.02	.26	.14	.14	.14	.14	.14	.14	.14	.14	.14	.14	0
	17	.05	.09	.14	.14	.14	.14	.14	.14	.14	.14	.14	.14	0
	18	.35	.10	.14	.14	.14	.14	.14	.14	.14	.14	.14	.14	0
	NCF	.35	.10	.16	.16	.16	.16	.16	.16	.16	.16	.16	.16	1

Note: the NCF row represents the case when a threat materializes but does not affect the associated component. The No Threat column represents the case when no threat materializes.

Table 5. Probability Threat Vector

Threat Vector (PT)		Probability of threat materializing per day
Threats	T1 Generation	0.02
	T2 Registration	0.10
	T3 Certification	0.05
	T4 Distribution	0.05
	T5 Installation	0.05
	T6 Storage	0.05
	T7 Derivation	0.04
	T8 Update	0.04
	T9 Archiving	0.04
	T10 Deregistration	0.03
	T11 Key Revocation	0.04
	T12 Destruction	0.02
	T13 No Threat	0.47

The Mean Failure Cost (MFC) is calculated with the development of the Equation 1, as follows:

$$MFC = ST \circ DP \circ IM \circ PT. \tag{1}$$

Essentially the vector of MFC (one entry per stakeholder) developed by the systematic substitution of the successful analysis of the stakeholder's requirements, components, and threats that cause failures, if and when they materialize [3, 4].

Table 6. Stakeholder Mean Failure Cost

Mean Failure Cost		Cost per day
Stakeholders	Utility	$83,689
	AMI Vendor	$94,272
	CKMS Provider	$106,479
	Corporate Customer	$3,595
	Critical Infrastructure Customer	$35,950

Table 6 shows the individual Stakeholder's Mean Failure Cost in units of currency per time frame, e.g. dollars per day. The MFC gives stakeholders a sense of how much they will lose, on average, if a threat develops. Stakeholders can use the MFC to determine which security measures are worth implementing in their system and which are more expensive to implement than what the stakeholder stands to lose on average (not necessarily in any particular circumstance).

9. CONCLUSIONS AND FUTURE RESEARCH

In the documented example, we use the currently existing standards/guidelines [6] and the Draft Standard IEC 6235 Part 9 – Key Management [7] Life cycle to begin the process of developing the MFC for specific stakeholders within the AMI environment of the smart grid subject domain. The numbers we need generally aren't available in the public domain, and as such we utilize the logic for the establishment (i.e., seeding) of the initial values needed from [5]. Vendors that are already providing smart meter services should begin keeping these data for further use, if they are not yet collecting them. We believe the stakes matrix was the most interesting to populate, as it results in addressing the MFC for each stakeholder. In this paper, we consider the possible outcome for the failure of the requirements of confidentiality, integrity and availability, then reference information about the effects of these outcomes on entities similar to our stakeholders. The other matrices require more estimation based upon our knowledge of the components of the AMI system. In the future, the team intends to have subject matter experts directly assist in the determination of these values. For now, we are interested in the insight that can be gained from the example rather than the specific numbers involved. In the future, we plan to conduct a detailed analysis of failure scenarios and their associated impacts using the CSES approach that clearly delineates risk as a function of threat, vulnerability and consequence. The example described here only accounts for a small number of stakeholders, interfaces (components) and threat categories. There are currently 29 failure scenarios in [9] that need to be fully addressed, as well as additional requirements (e.g., no unauthorized access), and other functional requirements that are at risk (e.g., sustained operations), and interfaces (e.g., components among the other smart grid categories (e.g., control systems) of which there are 22 defined in NISTIR 7628 [6]. Our future analysis needs to comprehend the established electronic delivery systems threat models, detailed failure scenarios used by utilities, criteria and methods for prioritization of the failure scenarios. We also want to investigate threat mitigations, active defenders' responses and courses of action.

10. ACKNOWLEDGEMENTS

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the author's academic institutions or companies, the DOE, or the U.S. Government.

11. REFERENCES

[1] "Roadmap to Achieve Energy Delivery Systems Cybersecurity," ed: Energy Sector Control Systems Working Group, 2011.

[2] "International Energy Agency Technology Roadmap Smart Grids," International Energy Agency, Paris, 2011.

[3] F. T. Sheldon, K. A. Robert, and A. Mili, "Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," in *Proceedings of Forty-second Hawaii International Conference on System Sciences*, Waikoloa, Big Island, Hawaii 2009, pp. 1-10.

[4] A. B. 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*, vol. 6, pp. 269-281, 2010.

[5] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili, "Risk Assessment Methodology Based on the NISTIR 7628 Guidelines," in *Proceedings of Forty-sixth Hawaii International Conference on System Sciences*, Wailea, Maui, Hawaii 2013 (accepted), pp. 1-10.

[6] "National Institute of Standards and Technology (NIST) Interagency Report (NISTIR) 7628 Guidelines for Smart Grid Cyber Security," NIST, Ed., ed. Gaithersburg: NIST, 2010.

[7] "IEC 62351 Part 9 – Key Management," ed: International Electrotechnical Commission, 2012, p. 40.

[8] "Public Printing and Documents," in *44 USC 3502*, ed. USA, 2009, p. 3542.

[9] "Electric Sector Failure Scenarios and Impact Analyses," in *National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1*, ed, Draft - July 3, 2012.