Cyber Attack Exposure Evaluation Framework for the Smart Grid

Adam Hahn, *Student Member, IEEE*, and Manimaran Govindarasu, *Senior Member, IEEE*

***Abstract*—The smart grid's heavy reliance on cyber resources introduces numerous security concerns. The substantial attack surface presented by the advanced metering infrastructure (AMI) along with the dissemination of sensitive data including privacy, billing, and control information will provide attackers with significant economic incentive. In addition, the scale and complexity of the architecture will stress the capabilities of many security controls such as public key encryption (PKI), authentication, and access control. The aforementioned concerns produce a requirement for increased risk management including security models that have the capability to scale to such a complex environment. A security model is introduced to represent various privilege states in a large architecture and evaluates viable paths that an attacker could exploit. The resulting model is used to produce a quantitative information-based *exposure* metric to evaluate the completeness of implemented security mechanisms. Various applications are proposed to show how the metric can enhance current risk management processes by identifying information dependencies of the deployed security mechanisms. Finally, the applicability of the proposed methodologies has been evaluated through a simulation study using realistic AMI infrastructure to demonstrate the utility of the proposed metric.**

***Index Terms*—Cyber security, smart grid, SCADA, common information models, metrics.**

I. Introduction

SMART GRID advancements present an undetermined level of risk to electric grid reliability. The coupling of the power infrastructure with complex computer networks substantially expand current cyber attack surface area and will require significant advances in cyber security capabilities. Strong security metrics are necessary to ensure security-based decisions accurately reflect a realistic understanding of cyber risk. National Institute of Standards and Technology (NIST) specifically addresses this requirement and recommends research in "tools and techniques that provide quantitative notions of risks, that is, threats, vulnerabilities, and attack consequences for current and emerging power grid systems" [18].

Attack trees and graphs have previously been used to model network security, unfortunately these models will not scale to large networks. While they provide detailed information on potential attack methods, their development is based on an understanding of potential attacker goals. Current trends show attackers increasingly rely on exploiting zero-day vulnerabilities [24], which reduces the accuracy of models depending on the evaluation of known vulnerabilities.

Developing security models for a large, networked environments such as the smart grid should focus on the critical information necessary to support the grid and the resulting security mechanisms deployed to protect it. The electric grid can typically be categorized into domains including generation, transmission, distribution, and market operations. While a significant amount of intradomain communication occurs, interdomain communication is imperative for grid stability as shown in Fig. 1. Since interdomain trust is a key characteristic for grid communication, a strong security model must accurately represent the trust levels and any associated risks.

Smart grid technology has developed increasing sophisticated common information models (CIMs) which standardize the information necessary to support system operation and assist with increasing requirements for communication between domains. Fortunately, CIMs also provide increasing awareness of information dependencies which should be leveraged to improve cyber security. This research provides a novel network security model tailored to provide a quantitative exposure metric based on these information objects by identifying and analyzing their dependency on security mechanisms as they traverse a network. This research also demonstrates how the exposure metric can be utilized to perform various cyber security related activities such as vulnerability impact analysis and security investment analysis.

II. Related Work

Recent concerns over electric grid cyber security have lead to the creation of compliance standards. The North American Electric Reliability Corporation (NERC) has recently developed Critical Infrastructure Protection (CIP) standards which introduce cyber security compliance requirements for power systems [20]. These standards primarily focus on the identification and protection of cyber assets considered critical to the bulk electric system. In additional to NERC's effort, NIST has produced technical documents addressing cyber security concerns for industrial control systems, such as SCADA. NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," addresses ISC specific threats, vulnerabilities, and provides guidance on enhancing current security controls [12]. NIST has also released NISTIR 7628, "Guidelines for Smart Grid Cyber Security," which provides a comprehensive overview of smart grid domains, actors, and the resulting logical

Manuscript received October 15, 2010; revised April 27, 2011; accepted June 05, 2011. Date of publication September 23, 2011; date of current version November 23, 2011. This work was supported by the National Science Foundation under Grant CNS 0915945. Paper no. TSG-00180-2010.

A. Hahn is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: adamhahn@iastate.edu).

M. Govindarasu is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2011.2163829

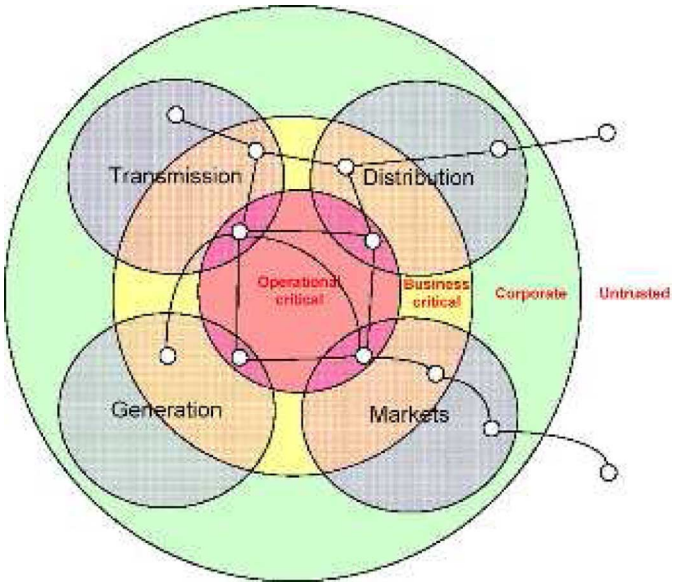

Fig. 1. Power system domains [7].

interfaces between various actors. In addition to the smart grid overview the document also provides current constraints and research directions required to establish an appropriate smart grid security posture [18].

A. Attack Surface

Research on attack surface evaluation has been introduced by Manadhata and Wing [17], [16]. This work defines a service's attack surface as the set of entry points, exit points and data channels in a system and utilizes this information to produce quantitative measurements of security. The relationship between excessive attack surface area and decreased security is then shown through the comparison of similar software platforms. While this work is a useful component in software engineering, the metric requires a formal review of software functionality and does not address the complexity of large-scale, distributed systems.

B. Attack Tree

An attack tree is a model which enumerates all potential vectors an attacker could use to gain access to some target resource. Each branch in the tree represents a set of intermediate steps the attacker must take prior to gaining access to the target. Previous attack tree work by Ten has shown applicability to modeling SCADA cyber security [2], [23]. Attack tree models such as Morda demonstrate how system risk can be calculated based on an understanding of attack objectives, strategy and potential mission impact [6]. Unfortunately the development of accurate trees is a difficult process when attacker capabilities and objectives are not well known.

C. Privilege/Attack Graphs

Previous work on security modeling was performed by Dacier, *et al.* through the implementation of privilege graphs which evaluate various privilege states in a computer system to determine whether known security states are violated [5]. This work was then expanded upon to show that the transitioning between nodes in a privilege graph can be used to model attacks against a system as an attacker escalates their privilege level [3]. In addition, this research addresses the relationships between security and various path characteristics, specifically length and quantity [4].

Attack graphs take a different approach to modeling security concerns by producing a privilege graph and analyzing the attack paths provided by all known vulnerabilities [15]. Detailed analysis of feasible attack capabilities can then be determined to establish whether critical resources are appropriately secured. Work by Wang *et al.* has utilized attack graphs for security metrics based on both path length and quantity [14]. Research performed by Idika and Bhargava has extended the path-based analysis by comparing potential metrics [10]. While the attack graph approach provides comprehensive view of a system's security, the difficultly of the vulnerability discovery and mitigation process reduces model accuracy and applicability to a large architecture with unknown vulnerabilities.

III. Smart Grid Introduction

The smart grid focuses on the increased integration of information technologies throughout the power grid. Fig. 2 provides an example cyber architecture for a smart grid deployment. Technologies such as phasor measurement units (PMUs) are being deployed to increase wide area measurements throughout the bulk power system to provide increased reliability. Additional intelligence within substation automation also provides increased reliability through improved fault management. However, from a cyber security perspective the advanced metering infrastructure seems to introduce the greatest concern due to its integration within a community, and ability to impact consumer's privacy and electricity availability.

A. AMI Introduction

AMI attempts to reduce cost and increase electricity reliability through the deployment of smart meters at consumer locations. These meters provide the customer with granular control over consumption and the ability to selectively use electricity when prices are low. Utilities benefit from being able to remotely detect outages, perform remote meter readings and offer prepaid options to customers. AMI also enables demand side management (DSM) which exercises direct/indirect control over consumer power consumption. This allows the increased integration of green technologies due to their inconsistent production.

The infrastructure necessary to support smart metering will require the integration of many novel and tailored technologies. Typically, a user's home area network (HAN) may communicate with a smart meter or some other data source to gain access to real-time pricing information. Networking technologies such as RF-Mesh or power line carrier (PLC) are often suggested to support this functionality. This infrastructure is commonly referred to as the neighborhood area network (NAN). Once metering data has been aggregated within a neighborhood it can be transmitted back to the central office for billing purposes. A wired or wireless field area network (FAN) will makeup the backhaul portion of the network.

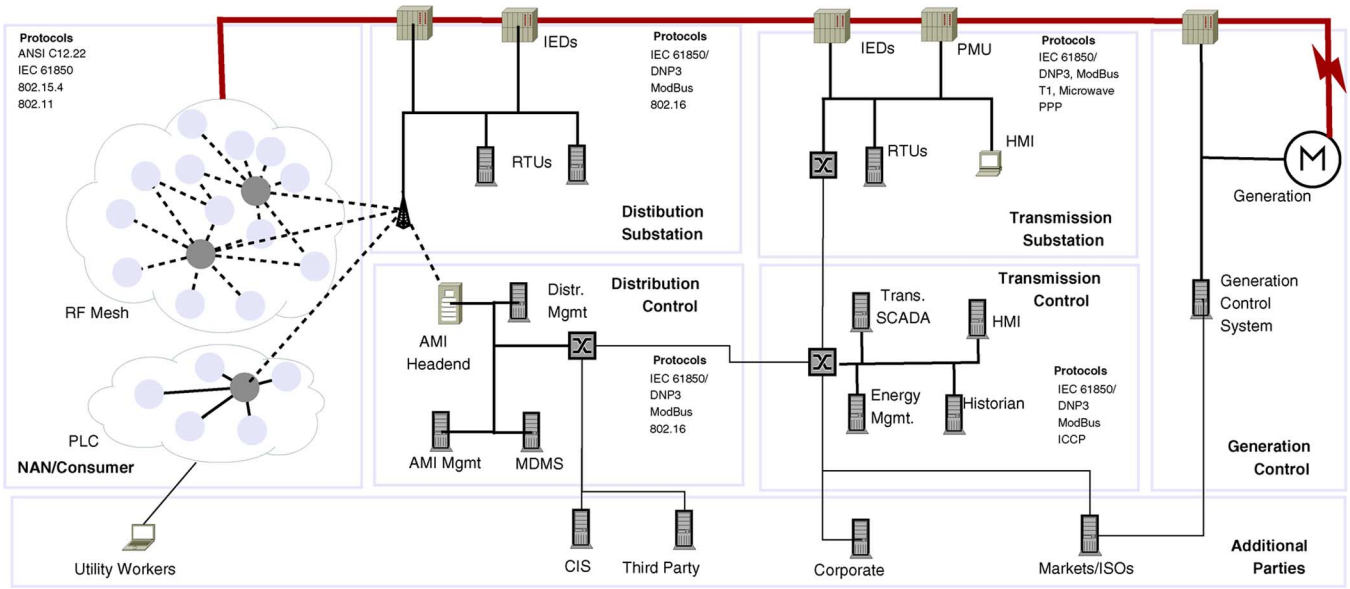

Fig. 2. A schematic of smart grid cyber infrastructure.

Maintaining a secure AMI infrastructure presents a challenging task. The geographically diverse deployments and long lifespans required for the infrastructure will significantly increase the exposure to attack. Additionally, large-scale device deployment, dependency on embedded systems, and constrained network bandwidth will limit the amount of security monitoring that can be performed. Finally, the large quantities of privacy data contained within the devices and networks raises consumer concerns.

B. Common Information Models

The smart grid will also increase the use of CIMs to provide a common format for expressing and communicating the information required to support the grid [9]. Current CIMs such as IEC 61968, which focuses on distribution systems, and IEC 61970, for transmission systems, are represented as an ontology that formalizes the information and relationships necessary to support the grid. CIMs have been primarily developed to facility increased system integration through consistent data representation and exchange formats. This research leverages these properties as a key component in understanding impacts from cyber security failures.

IV. Exposure Evaluation Framework

The development of a secure infrastructure is contingent on the ability to accurately assess the effectiveness of the current security mechanisms. The proposed framework achieves this goal by evaluating all paths an attacker must take in order to access critical resources. This work models the flow from security mechanisms to their protected privileges and the information accessible by that privilege. With this model the various sets of security mechanisms required to protect information as it traverses through a network can be reviewed.

The risk management process requires a comprehensive and continuous set of operations to ensure adequate system security. NIST provides a suggested framework which identifies all required activities and details the efforts necessary to perform risk management within industrial control systems [12]. The proposed exposure evaluation integrates with NIST's management framework to provide a more accurate assessment of risk. The interactions between the risk management and exposure analysis framework are displayed in Fig. 3.

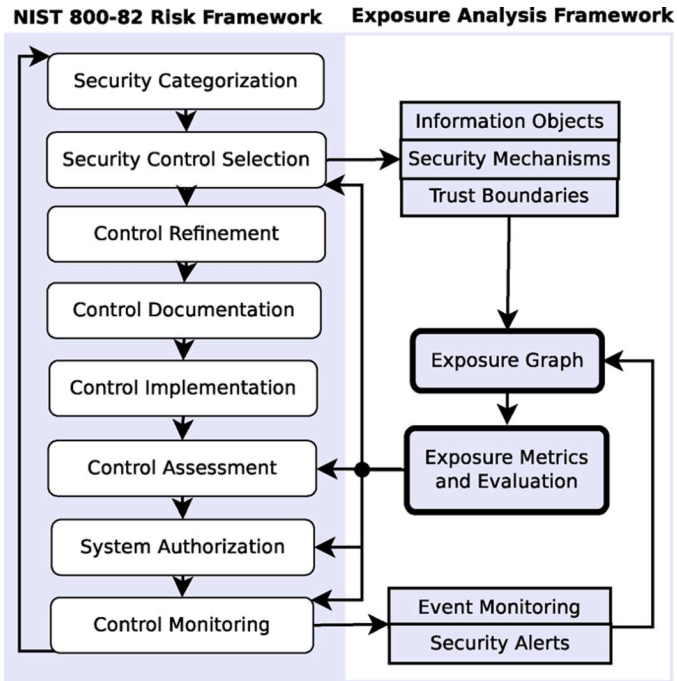

Fig. 3. Attack exposure evaluation framework.

The proposed model and metric leverage data from the security control selection process to determine the set of implemented security mechanisms. These security mechanisms along with the system's information model are necessary for the exposure graph development, which is detailed in Section IV-B. Once this graph has been developed it can be utilized to compute the proposed exposure metric which is discussed in Section IV-C. The resulting exposure metric has applicability throughout the risk management process. Proposed applications include:

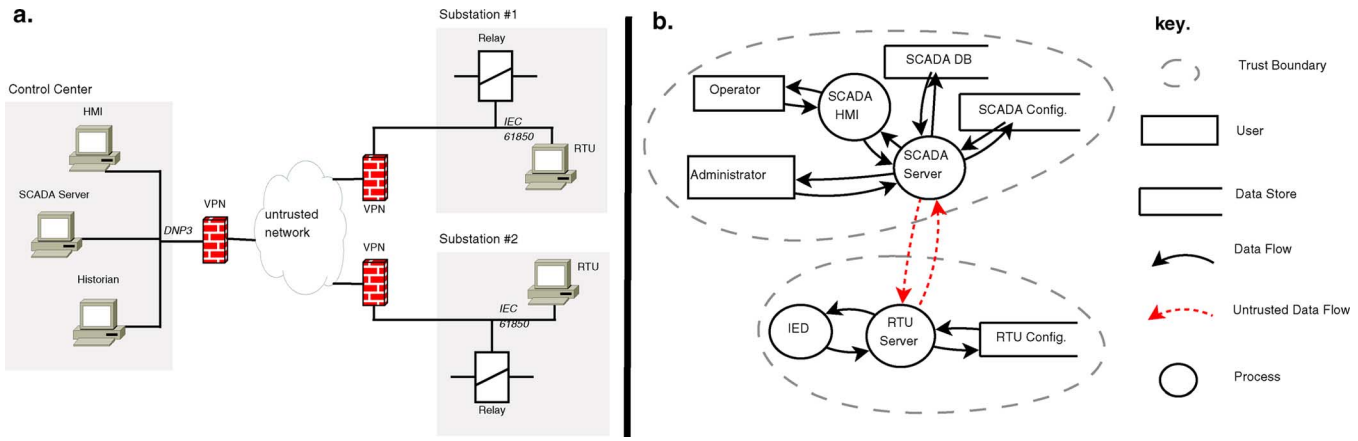

Fig. 4. (a) Testbed network architecture. (b) Testbed data flow diagram.

- vulnerability analysis;
- cyber security investment optimization;
- cyber contingency analysis.

A. Identifying Cyber Risk

Determining the set of security mechanisms required to support the cyber architecture is a challenging research area. There are currently numerous risk management processes which require the implementation of baseline security mechanisms within an environment [12], [20].

Traditional computer security models attempt to evaluate the current state of a computer and analyze whether the state corresponds to a known security status. A set of security mechanisms or controls are utilized to restrict system use to only those secure states. This paper presents a similar model based on a set of privileges, P, which identify the set of available states in the systems. Each privilege represents user/system access to some set of attributes within a CIM representation of the information within the system. These attributes, or information objects, are represented by the set IO. The model also assumes privileges are enforced with a set of security mechanisms, SM, such as access control, authentication, and encryption.

To determine an appropriate set of security mechanisms this paper utilizes the threat modeling process introduced by Microsoft [22]. The process first requires the identification of users, processes, data flows, entry/exit points, and data stores within the architecture. Next, each of the data flows are reviewed for possible (S)poofing, (T)ampering, (R)epudiation, (I)nformation disclosure, (D)enial of service, and (E)scalation of privileges. The threat modeling process begins with the development of a data flow diagram (DFD) which is then utilized to identify trusted boundaries and identify potential untrusted input.

The PowerCyber SCADA testbed at ISU, detailed in Fig. 4(a), is utilized to produced the example DFD between the control center and one substation in Fig. 4(b) [8]. In this example there are two trusted zone, the first is the control center where operators interact with a human-machine interface (HMI) to control the SCADA server. This provides the ability to remotely monitor and control the substation. The substation contains a remote terminal unit (RTU) that aggregates data from an intelligent electric device (IED), which performs various sensing and actuation functions. Additionally, all data flows between trust zones are considered untrusted as they are potentially vulnerable to external attack.

The information transmitted within the system is fairly limited. Since only one IED is utilized on each substation, only the following information is necessary to control the IEDs from the control center:

1) Operate Breaker (Control Center $\rightarrow$ RTU $\rightarrow$ IED);
2) Status Reading (Control Center $\leftarrow$ RTU $\leftarrow$ IED);
3) Voltage Reading (Control Center $\leftarrow$ RTU $\leftarrow$ IED).

In order to protect this environment from cyber attacks, security mechanisms must be provided to specifically target the untrusted areas. Fig. 5(a) extends the original DFD to model the necessary set of security mechanisms required to protect the system from malicious attack. Table I explains these security mechanisms in greater detail. This information will be utilized in the proposed model development along with the definition of information necessary to support the system.

B. Exposure Graph Development

This section introduces the exposure graph which formalizes the relationship between the security mechanisms, privileges and information objects within a system. The relationship between these objects will then be evaluated to determine the exposure of the information objects through the analysis of feasible attack paths. This exposure graph, defined as the directed graph $G = (SM, P, IO, A, E)$ contains the following vertex and edge definitions:

- SM—vertex (security mechanisms);
- P—vertex (system privileges);
- IO—vertex (information objects);
- A—vertex (untrusted users);
- E—edges (directed).

Developing the exposure analysis graph should begin by identifying the untrusted data flows within a network. This is modeled through a node, A, that represents potential attackers access. This node should connect to all possible systems accessible by the attacker. Since the system's security policy should ensure untrusted users cannot access any system resources without first bypassing some security mechanisms, all edges from A should connect to the set of accessible mechanisms SM and apply an edge weight of 1 to represent the attack effort required to bypass this mechanism. Each node in SM should

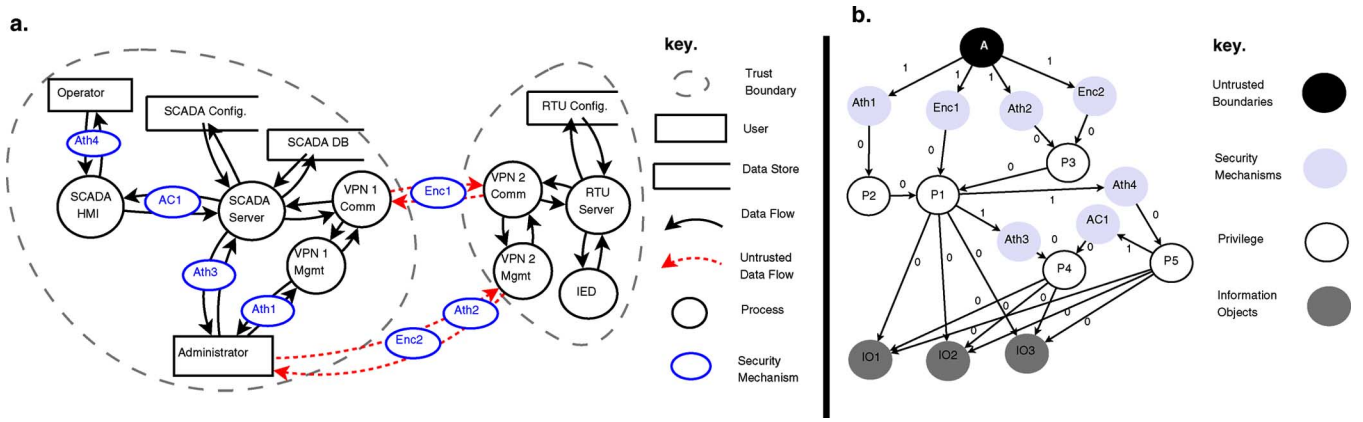

Fig. 5. (a) Testbed DFD with security mechanisms. (b) Resulting exposure graph.

then be connected to the set of privilege nodes, P, representing the set of privileges obtained if this security mechanism fails, these nodes should have a weight of 0. Edges can also exist between the privileges, as a privilege p_i could dominated another privilege p_j if it contains a superset of privileges. In this case a directed edge would be (p_j, p_i) added with a weight of 0. Finally information object, IO, nodes must be created for each object in the CIM for that architecture. A directed edge should then be placed between each node in IO and the set of nodes in P that either consume or produce that information. Fig. 5(b) provides an example of the resulting exposure graph developed based on the DFD in Fig. 5(a).

Algorithm 1: Exposure Analysis Algorithm

IOExposure Analysis();
input : $G = (\{SM, P, IO, A\}, E)$
output: exp
foreach $io \in IO$ **do**
  $exp_{io} = EvalPath(io, \{\}, 0)$;
end
EvalPath();
input : $node, VisitedSM, len$
if $node \in A$ **then**
  $return \frac{1}{max(len, 0.1)}$;
end
else
  foreach $i \in incident(node))$ **do**
    $EvalPath(i, VisitedSM, len + w(e(i, node)))$;
  end
  if $node \in SM$ **then**
    $VisitedSM = VisitedSM \cup node$;
  end
end

C. Exposure Evaluation

After the exposure graph has been developed, analysis can be performed to evaluate the exposure of the information objects.

TABLE I
EXAMPLE SECURITY MECHANISMS AND PRIVILEGES

SYSTEMS	SECURITY MECH./ PRIVILEGES	DESCRIPTION
VPN 1	Enc1	VPN encryption algorithm
	Ath1	Management authentication
	P1	VPN network access privilege
	P2	VPN management privilege
VPN 2	Enc1	VPN encryption algorithm
	Ath2	Management authentication
	Enc2	Management encryption alg.
	P1	VPN network privilege
	P3	VPN management privilege
SCADA Server	Ath3	Administrator authentication
	AC1	OS access control
	P4	Server access privilege
HMI	Ath4	Operator authentication
	P5	HMI access privilege

The exposure metric exp determines the attack surface of an information object as it traverses through various systems and networks. The exposure metric is computed through the analysis of all security mechanisms utilized to protect the set of privileges that either produce or consume the information object. Metric computation incorporates the number of attack paths through the security mechanisms protecting this asset while also factoring the path length as a method to evaluate the effort required to exploit a path.

Algorithm 1 documents the exposure metric calculation for the information objects within the graph G. Starting from each IO node, the algorithm identifies all privilege nodes with incoming edges into IO. Each incident edge is reviewed for neighboring nodes until the paths are traced back to A. Since edges incident to a element of SM are assigned with a weight of 1, paths length will be determined by number of SM elements within that path. Once a potential attack path has been traced back, the inverse of that path's length is the added to the exposure value for that information object. After all relevant attack paths have been traced, the resulting exp_{io} value can be determined.

The documented algorithm outputs an exposure computation for each information object. In this example, all three objects are communicated along the same path and will result in the same exp value. For this example the computed exposure for all 3 information objects is 4. This

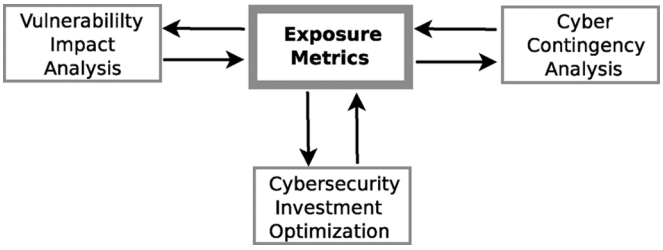

Fig. 6. Exposure metric applications.

score is determined as there are only four potential paths, each with a length of one, required to access the IO set. These paths are $\{\mathrm{A}, \mathrm{Ath1}, \mathrm{P2}, \mathrm{P1}, IO\}$, $\{\mathrm{A}, \mathrm{Enc1}, \mathrm{P1}, IO\}$, $\{\mathrm{A}, \mathrm{Ath2}, \mathrm{P3}, \mathrm{P1}, IO\}$, and $\{\mathrm{A}, \mathrm{Enc2}, \mathrm{P3}, \mathrm{P1}, IO\}$. The remaining paths are not relevant since once privilege $P1$ has been obtained the attacker can gain access to the IO set without requiring any additional effort. Section VI provides a more detailed evaluation with increased exp variations.

V. Exposure Metric Applications

This section presents applications of the exposure metric to assist in the development and management of a robust cyber infrastructure. Fig. 6 identifies three proposed metric applications including vulnerability and impact analysis, cyber security investment optimization, and contingency analysis within cyber resources.

A. Vulnerability Analysis

Computer systems are continuously affected with new vulnerabilities which present security challenges and unknown system impact. As documented within the NIST Risk Framework, continuous monitoring for possible security weaknesses is an important aspect of a strong risk management process. The first step in the monitoring process should be the collection of new information on possible threats or attack trends. Information sources should include security alerts from US-CERT and product vendors, individual vulnerability assessment results, intrusion detection alerts, and system events occurring within the environment.

Exposure analysis should be recomputed during the continual monitoring process and whenever significant changes have been found within system security mechanisms. The recomputation should address all information sets that depend on the security mechanisms in concern. For example, a failure of security mechanism sm_i will propagate to some privilege set P' and also some information object set IO'. Determining the exact exposure can be done by setting $w(e(\{x\}, \mathrm{sm}_i)) = 0$ where x represents all incident nodes, since the mechanisms can no longer be trusted to protect the system. The resulting exposure analysis should then be recomputed to determine the new, increased exposure due to the shortening of the path lengths.

Once the recomputation of all exposure values have been performed, the resulting architecture can be reviewed for its adequacy. The vulnerability's impact on critical information may leave it in an unacceptably exposed state. In this situation additional security mechanisms would be necessary. An example of this analysis is shown in Section VI-B1.

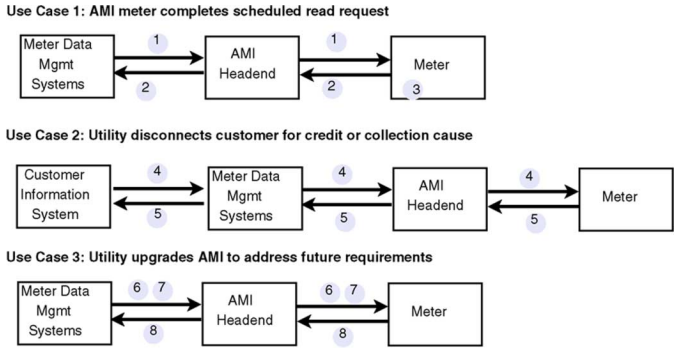

Fig. 7. Simulation AMI use cases.

B. Cyber Security Investment Optimization

Determining the effectiveness of cyber security enhancements presents a difficult strategy in large, distributed environments. Numerous possible investment strategies could be utilized to reduce the probability of a successful cyber attack. Two possible enhancement, $E1$ and $E2$, may have very different impacts on an infrastructure's security as they protect different subsets of privileges on different systems. The exposure metric provides a novel mechanism to compare the resulting additional security provided by the additional enhancements.

Enhancements can be evaluated by redeveloping the SM set to represent the infrastructure assuming the enhancement has been deployed. Once the new graph has been developed, the exposure can be recomputed and then utilized to compare various enhancements to determine their ability to protect critical information objects. Section VI-B2 provides a detailed example of performing security enhancement evaluations.

C. Cyber Contingency Analysis

Traditional compliance within power system requires n-1 and n-2 contingency throughout the physical components [19]. However, there is limited current understanding of whether cyber architectures remain survivable during security failures. Cyber contingency analysis should be targeted towards the information required to support the physical system. By analyzing IO sets and the SM sets that enforce the current security policy, direct correlations can be made between failures of cyber security mechanism and physical system occurrences. Additionally, this could instigate the development of cyber contingency analysis policies which mirror those found within physical systems.

VI. Metrics Evaluation

To evaluate the metric's applicability within a smart grid environment, this section presents an example AMI architecture and then computes the resulting exposure calculations based on

TABLE II
EXAMPLE SECURITY MECHANISM FOR AN AMI ARCHITECTURE

Domain	Device/Protocol	Security Requirement	Implementation Type	Protected Privileges
HAN	HAN GW	Authentication	x.509 Cert (Meter)	Individual HAN gateway
	Zigbee	Encryption	Link/Network Key Exchange	All HAN gateways & meters
			Link/Network Algorithm	All HAN gateways & meters
		Authentication	Network Key	Individual HAN gateway & meter
NAN	Meter	Physical		Individual meter
		Authentication	Meter-NAN private key	Individual meter
		Key Establishment		All meters
		Access Control	DAC (customer/mgmt function)	All meters
	Zigbee	Encryption	Link/Network Key Exchange	All NAN meters
			Link/Network Algorithm	All NAN meters
		Authentication	Network Key	All NAN meters
FAN	Headend	Authentication	x509 Cert (Meter)	Individual meter
			Key Signer	All meter
		Access Control	DAC (inter-customer)	All meter
	WiMax [1]	Authentication	x509 (meter), EAP	All FAN Stations
		Key Establishment	KEK, TEK	All FAN Stations
		Encryption	DES/AES (Payload)	All FAN Stations
Enterprise LAN	MDMS	Authentication	x509 Cert (Headend)	
		Access Control	DAC (inter-customer)	

various cyber security relevant events. These results are then interpreted to demonstrate the metric's applicability to this environment.

A. Simulated Environment

The simulated environment will model an AMI architecture that includes a HAN domain containing user meter gateways, a NAN domain containing smart meters, and FAN domain containing a AMI headend and meter data management system (MDMS). Both the HAN and NAN networks will be assumed to be using a wireless network such as Zigbee while the FAN is assumed to utilize a wireless WiMax network.

The information model for the simulation is based upon a subset of the AMI use cases published by Southern California Edison's (SCE) [21]. Fig. 7 reviews the use cases which provided a basis for system requirements for this simulation and demonstrate the flow of information between systems.

Based on these use cases, Table III provides a description of the information objects referenced in Fig. 7 and also cites likely attributes from an IEC 61968-9 based CIM. Future analysis within this section will reference the exposure of these information objects.

A set of security mechanisms is also presented to provide a realistic set of protections. Table II documents all of the assumed security mechanisms utilized to protect the various systems and networks within this environment. The Protected Privileges column is utilized to determine the set of systems privileges that are protected by the resulting security mechanisms.

B. Simulation Results

Based on the previously proposed environment we perform the resulting exposure computation and then provide demonstrations of the impact on the systems security.

1) Vulnerability Assessment: Fig. 8 provides the result from the exposure calculation on the simulation environment. The Normal State calculations provide the evaluation of a system that is operating in its intended state and is not impacted from any outstanding security concerns. Note that $IO1$-$IO2$ and $IO4$-$IO8$ maintain similar exposure values due to their similar paths throughout the network while $IO3$ has a limited exposure based on an assumption that certain granular meter readings with privacy concerns are protected by only being stored on the meter. Next the exposure for the same architecture is evaluated with the following two vulnerability scenarios.

- A. Compromised meter management authenticator.
- B. Vulnerable meter customer/management access control.

Fig. 8 also provides the resulting exposure calculations after vulnerability A is discovered. In this simulation it is assumed that vulnerability A has compromised the certificate utilized to perform meter management function which provides the attacker with the ability to modify configuration data and obtain access to some usage data. Note that the resulting exposure of all information objects except $IO3$ have significantly increased, $IO3$ exposure still remains relatively low since the meter's access control mechanism enforces separation between granular customer reading and management functions.

Next, its assume that a vulnerability B is discovered which allows the bypassing of the meter's customer/management access control mechanism. This vulnerability significantly increases the exposure of $IO3$, but does not notably increase that of $IO1$

TABLE III
EXAMPLE SET OF INFORMATION OBJECTS

Use Case	Data Objects	IEC 61968-9 [11]
Meter Reading		
	1. Read Request	MeterReadSchedule
	2. Usage (Response)	MeterReadings
	3. Usage (Protected)	
Meter Disconnection		
	4. Off Message	EndDeviceControl
	5. Confirm: Meter	EndDeviceEvent
Meter Firmware Upgrade		
	6. Firmware update	EndDeviceFirmware
	7. Execute firmware	EndDeviceFirmware
	8. Status check	EndDeviceEvent

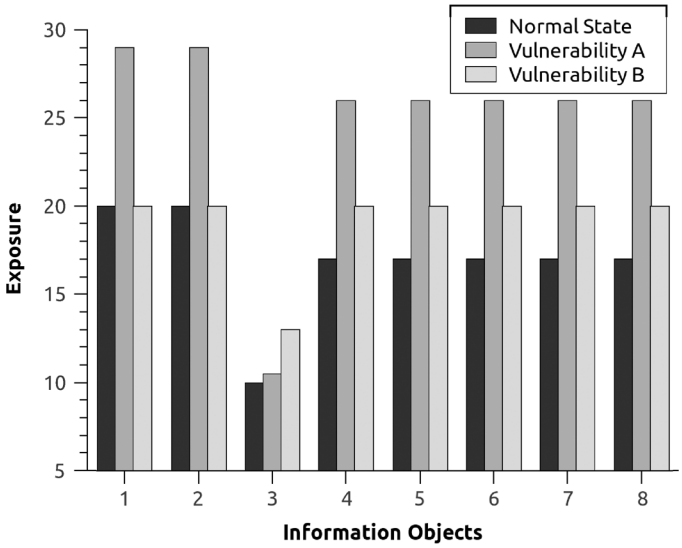

Fig. 8. Exposure metrics for normal/vulnerable scenarios.

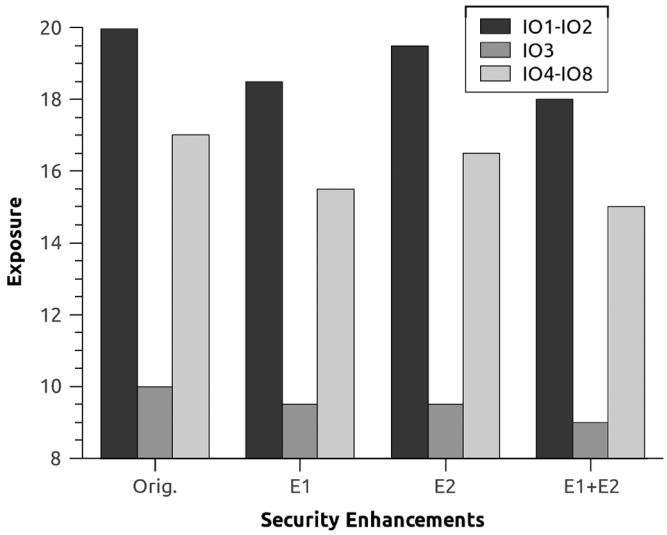

Fig. 9. Exposure after security enhancements.

and $IO2$ as they are already accessible from both the customer and management privileges. Also, note that meter firmware upgrade information, $IO6$-$IO8$, and meter management information, $IO4$-$IO5$, have been significantly increased. Since this information was originally protected from customer access, but now may be potentially exposed due from the resulting vulnerability.

2) Security Investment: In addition to the vulnerability and impact assessment application, evaluation results have also been utilized to demonstrate the exposure metrics utility within the security investment process. The current exposure value of various resources is first evaluated on the system's normal state, then the exposure resulting from the insertion of additional security mechanism is performed and the resulting exposure is computed to evaluate the improvement.

Fig. 9 provides the results of the enhancements. The x-axis contains the various security enhancement results. The first set labeled "Orig" assumes no enhancement has occurred. The next two sets of results assume that enhancement $E1$ and $E2$ have been implemented individually while the final set assumes that both $E1$ and $E2$ have been implemented together. The proposed enhancements for this evaluation include:

- E1—Application layer authentication/encryption;
- E2—Tamper resistant meter hardware.

The first enhancement, $E1$, assumes that the additional encryption and authentication is being performed on the meter application level which, for example, could be implemented by the IEC 62351 security protection standard. This would increase the amount of effort required for an attacker to access this information when it is in transit between the system. The second enhancement, $E2$, assumes a tamper resistant hardware is utilized within the environment which limits the smart meters accessibility to physical attacks.

The results show that the additional encryption and authentication provide a greater impact to the general system's exposure and will likely constitute a more useful investment. This is primarily due to the fact that it protects information throughout its life span as opposed to $E2$ which focuses primarily on the protection of data-at-rest within the meter. However, the combination of both $E1$ and $E2$ further reduce the exposure for the resources, although there still remains a number of potential attack vectors.

VII. Conclusion

This paper has addressed quantitative security metrics for large scale networked environments such as a smart grid. The proposed model utilizes a pragmatic development process which integrates within a modern risk management process and is based on information that is well known to security engineers and operators. An exposure metric has been proposed to identify the set of security mechanisms required to protect the various information objects utilized within a network. A test environment has been proposed to model likely AMI deployments and example exposure metrics have been computed. The metric's application to the security investment situation has been demonstrated with comparisons between various potential security enhancement strategies. Additionally, the metrics has shown how vulnerability impacts can be evaluated by simulating vulnerabilities and demonstrating their impact on information object's exposure. Future research within this domain will address scalability to larger system deployments and system-level metrics to facilitate more comprehensive architecture analysis.

References

[1] M. Barbeau, "WiMax/802.16 threat analysis," in *Proc. 1st ACM Int. Workshop Quality Service Security Wireless Mobile Netw. (Q2SWinet'05)*, New York, pp. 8–15, ACM.

[2] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern., Syst. Hum.*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[3] M. Dacier and Y. Deswarte, "The privilege graph: An extension to the typed access matrix model," in *Proc. Eur. Symp. Comput. Security (ESORICS'94)*.

[4] M. Dacier, Y. Deswarte, and M. Kaniche, "Models and tools for quantitative assessment of operational security," in *Proc. 12th Int. Security Conf. (IFIP/SEC'96)*.

[5] M. Dacier, Y. Deswarte, and M. Kaniche, "Quantitative assessment of operational security: Models and tools," LAAS Res. Rep. 964493, May 1996.
[6] E. Shelby, H. David, K. Elizabeth, P. John, and W. James, "Risk-based systems security engineering: Stopping attacks with intention," *IEEE Security Privacy*, vol. 2, no. 6, pp. 59–62, 2004.
[7] G. N. Ericsson, "Cyber security and power system communication essential parts of a smart grid infrastructure," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1501–1507, Jul. 2010.
[8] A. Hahn, B. Kregel, M. Govindarasu, J. Fitzpatrick, R. Adnan, S. Sridhar, and M. Higdon, "Development of the PowerCyber SCADA security testbed," in *Proc. 6th Annu. Workshop Cyber Security Inf. Intell. Res. (CSIIRW'10)*, New York, pp. 21:1–21:4.
[9] J. Hughes, "Harmonization of IEC 61970, 61968, and 61850 models," Electric Power Research Initiative (EPRI) Rep., Dec. 2006.
[10] N. Idika and B. Bhargava, "Extending attack graph-based security metrics and aggregating their application," *IEEE Trans. Dependable Secure Comput.*, to be published.
[11] *Interfaces for Meter Reading & Control*, IEC 61968, International Electrotechnical Commission (IEC).
[12] K. Stouffer, J. Falco, and K. Scarfone, "NIST SP 800-82: Guide to Industrial Control Systems (ICS) security," National Institute of Standards and Technology, Tech. Rep., Sep. 2008.
[13] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-Grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, 2010.
[14] L. Wang, A. Singhal, and S. Jajodia, "Toward measuring network security using attack graphs," in *Proc. 2007 ACM Workshop Quality Protection*.
[15] R. P. Lippman and K. W. Ingols, "An annotated review of past papers on attack graphs," Lincoln Laboratory, Project Rep., 2005.
[16] P. Manadhata and J. Wing, "An attack surface metric," Tech. Rep. CMU-CS-05-155, Jul. 2005.
[17] P. K. Manadhata, J. M. Wing, M. A. Flynn, and M. A. McQueen, "Measuring the attack surfaces of two ftp daemons," in *ACM Comput Commun. Security (CCS) Workshop Quality Protection (QoP)*, Oct. 2006.
[18] *Guidelines for Smart Grid Cyber Security*, NISTIR 7628, National Institude for Standards and Technology, Aug. 2010.
[19] *System Performance Under Normal Conditions*, TPL-001-0.1, North American Electric Reliability Corporation, Oct. 2008.
[20] Critical Infrastructure Protection (CIP) Reliability Standards, North American Electric Reliability Corporation, 2009.
[21] Southern California Edison's (SCE), AMI Use Cases.
[22] F. Swiderski and W. Snyder, *Threat Modeling*. Redmond, WA: Microsoft Press, 2004.
[23] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.
[24] "United State Computer Emergency Readiness Team (US-CERT)," USCERT Quarterly Trends and Analysis Report, 2006.

Adam Hahn received the B.S. degree in computer science from the University of Northern Iowa, Cedar Falls, and the M.S. degree in computer engineering from Iowa State University (ISU) Ames. He is currently working toward the Ph.D. degree in the Department of Electrical and Computer Engineering, ISU.

He is currently an Information Security Engineer at the MITRE Corporation, and has participated in Institute for Information Infrastructure Protection (I3P) projects. His research interests include cyber vulnerability assessment, critical infrastructure cyber security, and smart grid technologies.

Manimaran Govindarasu received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology (IIT), Chennai, in 1998.

He is currently a Professor in the Department of Electrical and Computer Engineering at Iowa State University, Ames, and has been on the faculty there since 1999. His research expertise is in the areas of network security, real-time embedded systems, and cyber physical security of smart grid. He has recently developed cyber security testbed for smart grid at Iowa State University to conduct attack-defense evaluations and develop robust countermeasures. He has coauthored more than 125 peer-reviewed research publications, and has given tutorials at reputed conferences (including IEEE INCOFOM 2004 and IEEE ComSoc *Tutorials Now*) on the subject of cyber security, served in technical program committee as chair, vice-chair, and member for many IEEE conferences/workshops, and served as session chair in many conferences. He is a coauthor of the text *Resource Management in Real-Time Systems and Networks* (MIT Press, 2001).

Prof. Govindarasu has served as guest coeditor for several journals including leading IEEE magazines. He had contributed to the U.S DoE NASPInet Specification project and is currently serving as the chair of the Cyber Security Task Force at IEEE Power and Energy Systems Society (PES) CAMS subcommittee.