SecureCyber : Risk-Based Optimization through Common Vulnerability Systems Scoring Over Energy Smart Grid

Shahir Majed
Advance Informatics School,
Universiti Teknologi Malaysia,
Shahir.majed@mimos.my

Suhaimi Ibrahim
Advance Informatics School,
Universiti Teknologi Malaysia,
suhaimiibrahim@utm.my

Mohamed Shaaban
Centre of Electrical Energy Systems
Universiti Teknologi Malaysia,
m.shaaban@fke.utm.my

ABSTRACT
This paper introduces the idea of CVSS-host scores which utilize CVSS parameters to provide impact scoring for Smart Grid Environment. This scoring mechanism presents a novel view of system risk by framing an-upper bounds on the criticality of potential vulnerabilities in that system. Once this scoring system has been established, the CVSS vectors can then be utilized to perform more sophisticated calculations to investigate optimal costs and benefits for future security enhancements.

Categories Subject Descriptors
[C.2.0] **Computer-Communication Networks:** Security and Protection
[C.2.1] **Network Architecture and Design:** Distributed Networks
[D.4.6] **Security and Protection:** Access Control
[K.6.5] **Security and Protection:** Physical Security

General Terms
Design, experimentation, performance

Keywords
Vulnerability Assessment, Smart Grid Security, Security Metrics, Critical Infrastructure Protection**.**

1. INTRODUCTION

Smart grid advancements present an undetermined level of risk resides to electric grid reliability. The coupling of the power infrastructure with complex computer networks substantially expand current targeted cyber-attack surface area and will require significant advances in cyber security posture. Strong security metrics are necessary to ensure security-based decisions accurately reflect a realistic understanding of security risk. NIST specifically addresses this requirement for the smart grid 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"[2]. This paper proposes a new metric for evaluating system risk based on pragmatic, industry accepted risk management practices.

Very few metrics have gained noticeable popularity throughout the security community. However, the Common Vulnerability Score System (CVSS) has obtained almost universal acceptance as an accurate and consistent way to score vulnerability severity. CVSS was initiated as a public effort to standardize vulnerability scoring and has matured through continual re-evaluation[6]. The system uses a set of linear functions to assign a quantitative value to known vulnerabilities based on a variety of system, temporal and environmental specific attributes. While vulnerability scoring is an important component of risk management, the current upsurge of zero- day vulnerabilities shows that system risk cannot be accurately determined through vulnerability analysis alone. By leveraging certain CVSS parameters this work presents a method of evaluating architectural risk through CVSS-host scores. It then displays how the scoring system introduces the capability of optimizing the risk/cost trade-off by formulating a binary integer programming problem which address these concerns. This work attempts to identify those assets in the smart grid which will likely present the greatest amount of risk. It applies the proposed risk assessment process on example smart grid architectures provided by NIST. CVSS-host scores are assigned to the NIST provided smart grid interfaces based on the documented system interfaces and reliability impact requirements.

iiWAS '14, December 04 - 06 2014, Hanoi, Viet Nam
Copyright 2014 ACM 978-1-4503-30015/14/12…$15.00

http://dx.doi.org/10.1145/2684200.2684308

2. RELATED WORKS

Previous research has utilized CVSS scores or other scoring systems to determine optimal security postures. Work by Tupper and Zincir-Heywood computes CVSS scores for all known vulnerabilities in a network to produce a comprehensive security metric [3]. Research by Chen produce a similar vulnerability scoring system and utilizes it to produce quantitative data on the amount of architecture risk[8]. Finally, Houmb leverages certain CVSS parameters in a Bayesian Belief Network (BBN) in an attempt to predict attack frequencies [1]. The work proposed in this paper differentiates from previous research as it assumes not all vulnerabilities can be determined during the risk evaluation process and provides a vulnerability-agnostic risk analysis method.

III. TRADITIONAL CVSS COMMON PRACTISE

CVSS provides a metric for evaluating vulnerability's potential negative impact on a computer system. CVSS was designed to be both quantitative and vector-based to encourage its use in future research methods[6]. The scoring system works by performing calculations based on fourteen individual metrics and producing a score ranging from 0 to 10 which represents the criticality of the vulnerability. The metrics are categorized as either Base, Temporal, or Environmental, these groups provide flexibility to the scoring as temporal and environmental information may not be available for all evaluations. The base metrics addresses basic potential exploit effects and system characteristics. Individual metrics for the base group include the Access Vector, Access Complexity and Authentication. The Access Vector evaluates who is able to access the vulnerability, specifically whether the individual requires access to a special network or local access. Access Complexity determines whether the exploitation of vulnerability requires non-standard or especially difficult attack methods. Authentication evaluates the type of authentication required to access the vulnerability. The environmental metrics provide context to the criticality of the vulnerable systems and their

Base Group Metrics	Values
Access Vector (AV)	Local (L) = 0.395
	Adjacent (A) = 0.646
Access Complexity (AC)	High (H) = 0.35
	Medium (M) = 0.61
Authentication (AU)	Multiple (M)=0.45
	Single (S)= 0.56
Confidentiality Impact (CI)	None (N) = 0.0
Integrity Impact (II)	Partial (P) = 0.275
Temporal Group Metrics	Values
Exploitability (E)	Unproven (U)= 0.85
	Proof-of-Concept (POC)=0.9
	Functional (F)= 0.95
Remediation Level (RL)	Official-Fix (OF)= 0.87
	Temporary-Fix (TF) = 0.90
	Workaround (W) = 0.95
Report Confidence (RC)	Unconfirmed (UC) = 0.90
	Uncorroborated (UR) = 0.95
Environmental Group	Values
Collateral Damage Potential	None (N) = 0
(CDP)	Low (L) = 0.1
	Low-Medium (LM)= 0.3
Target Distribution (TD)	None (N)= 0
	Low (L)= 0.25
	Medium (M)= 0.75
Integrity Req. (IR)	High (H)= 0.5
Confidentiality Req. (CR) Availability Req. (AR)	Medium (M)= 1.0

INDIVIDUAL CVSS METRICS

prevalence. Environmental metrics include Collateral Damage Potential, Target Distribution, Confidentiality Requirement, Integrity Requirement and Availability Requirement. The Confidentiality, Integrity and Availability Requirement metrics analyze the security requirements of the system based on NIST FIPS-199 pro- vided guidance[4]. Collateral Damage Potential evaluates the damage that may occur to the environment if the vulnerability is successfully exploited. Target Distribution represents the percentage of the systems that contain the vulnerability. Finally, the temporal group is used to identify the quality of vulnerability information and also the likelihood of a functional exploit. This group is not used in this evaluation due to this vulnerability- agnostic perspective.

Software Platform	Areva e-terrahabitat EMS		
Software Vulnerability (CVE)	NETIO 2009-0211	2009-0212	MFL 2009-021
CVSS Base	AV:N AC:L Au:N	AV:N AC:L Au:N	AV:N AC:L Au:N C:N
CVSS Base Score	7.8	7.8	10.0

Table III Areva Vulnerability CVSS Scores

Each metric has a number of possible values which may be assigned; table 1 defines these values for the individual metrics. Once the individual metrics have been assigned the base, temporal, and environmental scores can be computed utilizing the equations in table 2. These computations result in the final CVSS score. Example CVSS usage is provided in table 3. Base CVSS scores are computed for vulnerabilities discovered in Areva's e-terrahabitat energy management software (EMS). The three distinct vulnerabilities CVE-2009-021, CVE-2009-0211, and CVE-2009-021 were located within the same software pack- ages. Both CVE-2009-021 and CVE-2009-0211 are Distributed Denial of Service (DDoS) vulnerabilities in the NETIO component of the software while CVE-2009-021 is a buffer overflow in MLF software component. The National Vulnerability Database (NVD) provides the following base scores for the vulnerabilities [7].

- CVE-2009-0211 - Base Score:7.8
  CVSSVector:
  (AV:N/AC:L/Au:N/C:N/I:N/A:C)

- CVE-2009-0212 - Base Score:7.8
  CVSSVector:
  (AV:N/AC:L/Au:N/C:N/I:N/A:C)

- CVE-2009-021 - Base Score:10.0
  CVSSVector:
  (AV:N/AC:L/Au:N/C:C/I:C/A:C)

4. MODELING GRID SYSTEM CRITICALTY WITH CVSS

Although CVSS was intended to determine vulnerability's potential impact, a number of the individual metrics evaluate well known system characteristics. Since these metrics are utilized in the final score calculation they can also be used to identify systems which have a greater likelihood of possessing vulnerability with a high CVSS score. A potential impact can be determined by evaluating those previously known characteristics and determining worse-case scenarios for the remaining metrics. This provides a metric which evaluates whether the system is capable of producing high impact vulnerability. Table 4 is a modification of table 3 displaying how individual metrics for specific systems could be computable without the context of vulnerability.

Base Equations

1. BaseScore = ((0.6 * Impact)+(0.4 * Exploitability) - 1.5) * 1.176
2. Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
3. Exploitability = 20 * AccessVector * AccessComplexity * Authentication

1. Temporal Equations

4. TemporalScore = BaseScore * Exploitability * RemediationLevel * ReportConfidence

2. Environmental Equations

5. EnvironmentalScore = (AdjustedTemporal + (10-AdjustedTemporal) * CollateralDamagePotential) * TargetDistribution

3. 6. AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)*(1-AvailImpact*AvailReq))

Table 2. CVSS Vector Equations

Software Platform	Areva e-terrahabitat EMS		
CVSS Metrics	CR IR AR TD CDP		
Software Component	NETIO		MFL
CVSS Metrics	AV:N AC:L Au:N C:N I:N A:C		AV:N AC:L Au:N C:C I:C A:C
Vulnerability (CVE)	2014-0211	2014-0212	2014-021
CVSS Metrics	E RL, RC	E RL, RC	E RL RC

Table IV System Specific CVSS Parameters

This section provides a method for determining system risk through CVSS analysis utilizing only those scores specific to the system. Scores produced using this method will be referred to as CVSS-host scores.

- CVE-2014-0211 - Base Score:7.8 CVSSVector: (AV:N/AC:L/Au:N/C:N/I:N/A:C)
- CVE-2014-0212 - Base Score:7.8 CVSSVector: (AV:N/AC:L/Au:N/C:N/I:N/A:C)
- CVE-2014-021 - Base Score:10.0 CVSSVector: (AV:N/AC:L/Au:N/C:C/I:C/A:C)

A. Producing CVSS-host Scores

CVSS-host metrics should be assigned similarly to those in the traditional CVSS. While most CVSS-host scores should be applied in the same manner as if they would in vulnerability scoring, there are certain metrics that maintain some uncertainty. Particularly poorly mappings include AC, CDP, C, I, and A. The scores for C, I, and A are set to Complete as its assumed that critical vulnerability could completely compromise these attributes. AC provides another difficulty as its intended to evaluate the difficulty of exploiting vulnerability. Previous analysis of CVSS shows that this metric is set to Low the majority of the time[5]. For the CVSS-host scoring this parameter is set to Low unless its previously known that vulnerability exploitation is extremely challenging on a system. CDP also provides a difficult mapping between CVSS and CVSS-host as its difficult to evaluate the collateral damage potential without having detailed knowledge about a vulnerability. For CVSS- host scoring its suggested the CDP set to be equivalent to the highest value of CR, IR, or AR. The temporal values Exploitability (E), Report Confident (RC) and Remediation Level (RL) should all be considered Not Defined (ND) as they are entirely dependent on the presences of vulnerability. Table 5 provides additional information on CVSS-host metric scoring.

Metric	Scoring Method
Access Vector (AV)	Determine whether access to host/service is available to
Access Complexity (AC)	Low, unless configuration
Authentication (AU)	Level of required
Conf. Impact (CI) Integrity Impact (II)	Complete (C), assumes worst case vulnerability
Exploitability (E)	
Report Confidence (RC)	Not Defined (ND)
Confident Req. (CR) Integrity Req. (IR)	Based on FIPS 199 impact ratings
Collateral Damage (CDP)	Assume highest score
Target Distribution (TD)	Services distribution percentage

Table V Scores Applied To Interface

B. Smart Grid Assets

National Institute of Standards and Technology (NIST) Internal Reports (IR) 7628, "Smart Grid Cyber Security Strategy and Requirements" details a logical architecture for the smart grid and provides reliability impact levels for the specific AMI interfaces between domains, sub-domains and actors[1]. The document also identifies those interfaces involved in the Advanced Metering Infrastructure (AMI), Distribution Grid Management (DGM), Electric Storage (ES), Electric Transportation (ET), Home Area Network/Business Area Network (HAN/BAN) and also Wide Area Situational Awareness (WASA) domains. The reliability impact levels are assigned a score of Low, Medium, or High for Confidentiality, Integrity, and Availability requirements based on FIPS 199 definitions [4]. Utilizing the provided interfaces, knowledge about their connectivity and FIPS 199 impact levels we can produce CVSS-host scores for each documented interface which provides an understanding of systems with the potential for critical vulnerabilities. This paper will focus on the risk evaluation of the Advanced Metering Infrastructure (AMI) domain as it introduces a unique architecture due to the expansive attack surface.

Customer	Customer Appliances and Equip
Customer	Customer Energy Management system
DER	Energy Services/Interface (HAN Gateway)
Electric Vehicle	Distribution SCADA
Meter	Distribution Management System
AMI Headend	Meter Data Management System
Submeter	Customer Information System
Customer Portal	Customer Service Representative
Billing	
Third Parties	

Table VI
NIST IR 7628 Ami Domain Systems

The systems documented in the AMI domain are listed in table 6. Utilizing the CVSS-host scoring method for all AMI interfaces provides an understanding of systems with greatest security concerns.

The appendix provides the results from the CVSS-host analysis as applied to the documented AMI interfaces in NIST IR 7628. Based on this analysis it appears that most interfaces have comparable CVSS-host scores, however a certain class of systems maintain exceptionally high scores. The average CVSS-host score for the interfaces was 7.7, this was primarily the result of all interfaces maintaining High level Integrity, Confidentiality, or Availability Impact requirements and Adjacent Access Vectors. Exceptionally high CVSS-host score systems were those between Customers and the Consumer Portal and Customers and the Customer Service Providers. These scores were higher due the combination of both High impact requirements and also Network Access Vector which significantly increases the likelihood of targeted attack.

The lack of granularity in the scoring is primarily due to a combination of CIA requirements provided in NIST 7628 as most interfaces are assigned a High impact score. The CVSS calculations also do not differentiate between High impacts for one or all CIA requirements.

V. RISK-BASED CVSS-HOST SCORES OPTIMIZATION

The CVSS-host scores provide a quantitative scoring sys- tem for evaluating system risk. This introduces capability for mathematical analysis of the system scores in a larger architec- ture. This section documents a process for formulating binary integer programs which can be used to determine optimal configurations for both cost and risk in the architecture. Certain CVSS metrics are will remain static throughout a host's lifespan. For example, requirements from Confidentiality, Availability or Integrity Requirements. Parameters such as Access Vector will remain static as there are likely reasons services need to be offered to users or systems on various networks. Other CVSS parameters are potentially configurable and provide a representation of security investments, these parameters include Authentication, Target Distribution, and Access Complexity. Authentication can be flexible as higher levels of authentication can increase security but also increase the cost of deploying and maintaining the authentication solutions. IT systems primarily implement password-based authentication, unfortunately passwords are vulnerable to brute force guesses and may also be stolen from attacked client systems. Multi-factor authentication which utilizes a password and hardware or software token provides substantially more robust authentication and will resulting in lower the CVSS score. Target distribution can be decreased through efforts to diversify the software and services running on a network. While this has additional cost, a diverse operating environment provides increased security as it requires that attackers implement a wider array of vulnerabilities to gain system access. Finally, Access Complexity can be considered an additional method to increase a system's security posture. While this metric is more obtusely defined as it incorporates an array of potential protection mechanism such as configuration changes and other exploit prevention techniques [5].

The binary integer program defined in this section specifically addresses manipulations in the AU metric as the sole variable. The program minimizes cost spent on authentication solutions while maintain a threshold CVSS score for all system interface. The required variables for this problem are defined below.

- $CVSS\text{-}host_i$ - the computed CVSS-host for interface i
- $CVSS_{max}$ - maximum allowed CVSS score
- $cost_n$, $cost_{sf}$, $cost_{mf}$ - cost of no authentication, single factor, and multi-factor
- $|au_n|$, $|au_{sf}|$, $|au_{mf}|$ - number of systems with no authentication, single factor, and multi-factor
- au_n^i , au_{sf}^i , au_{mf}^i - whether interface *i* implements no authentication, single factor, and multi-factor

Utilizing these definitions we can compose the following binary integer program to optimize cost.
Minimize:

$$|au_n| * cost_n + |au_{sf}| * cost_{sf} + |au_{mf}| * cost_{mf}$$

Subject to

$$\sum_{i=1}^{I} CVSSHostSCADAScore \leq CVSS_{\max}$$

$$0.46 * au_{mf}^{i} + 0.56 * au_{sf}^{i} + 0.704 * au_{n}^{i} = AU_i$$

$$au_{mf}^{i} + au_{sf}^{i} + au_{n}^{i} = 1$$
$$au_{mf}^{i} = 0.1$$
$$au_{sf}^{i} = 0.1$$
$$au_{n}^{i} = 0.1$$

6. FUTURE WORK

The accuracy of both CVSS-host scores and the binary integer program formulation rely on the correctness of the CVSS scoring system. Since CVSS was developed to address vulnerability criticality and not system security there are some difficulties with mapping metrics to a host scoring mechanism. Fortunately CVSS is a continually evolve system and future versions will likely increase its ability to score both vulnerabilities as well as host security properties. A worthy area of future research could address a score system specifically tailored to host scoring which could then be combined with a vulnerability specific system such as CVSS. The binary integer programs in this paper only address variations in authentication mechanisms, other parameters such as target distribution and access complexity could also be added to produce a more flexible problem which more accurately addresses all variable security parameters.

7. CONCLUSION

This paper introduces a risk analysis method which is based on CVSS scoring. The smart grid AMI systems documented in NIST IR 7628 are evaluated utilizing this system to evaluate those systems which introduce the most risk into the environment. After establishing the CVSS-host scoring system it displays how these scores can be utilized to perform more advanced analysis of system security. By evaluating binary integer programs established with the CVSS-host scores it is possible to determine optimal cost/benefit analysis of risk mitigation solutions throughout a large scale architecture.

8. ACKNOWLEDGEMENT

This research is funded by the Universiti Teknologi Malaysia (UTM) in collaboration with the Malaysian Ministry of Education under the Vot no. 4F238. The authors would like to thank the Research Management Centre of UTM and the Malaysian Ministry of Education for their support and cooperation including students and other individuals who are either directly or indirectly involved in this project.

9. REFERENCES

[1] Houmb, S.H., et al. Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Software, 2009. doi:10.1016/j.jss.2009.08.023.

[2] Lee, A. Smart Grid Cyber Security Strategy and Requirements, Draft NISTIR 7628. National Institude for Standards and Technology, 2010.

[3] Melanie Tupper, A. Nur Zincir-Heywood. VEA-bility Security Metric:A Network Security Analysis Tool. 2008 Third International Conference on Availability, Reliability and Security, pages 950–957, 2008.

[4] National Institute of Standards and Technology. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

[5] P. Mell and K. Scarfone. Improving the Common Vulnerability Scoring System. IET Information Security, London, England, pages 119–127, September 2007.

[6] Scarfone, K. Mell, P. An Analysis of CVSS Version 2 Vulnerability Scoring. Third International Symposium on Empirical Software Engineering and Measurement, 2009.

[7] US-CERT. Vulnerability Note VU337569, AREVA e-terrahabitat SCADA systems vulnerabilities, 2009

[8] Yue Chen, Barry Boehm, Luke Sheppard. Value Driven Security Threat Modeling Based on Attack Path Analysis. 40th Annual Hawaii International Conference on System Sciences (HICSS'07), page 280a, 2007.