Measuring Cyber Security in Intelligent Urban Infrastructure Systems

Jennifer L. Bayuk
School of Systems and Enterprises
Stevens Institute of Technology
Hoboken, NJ USA

Ali Mostashari
School of Systems and Enterprises
Stevens Institute of Technology
Hoboken, NJ USA

***Abstract*— An important consideration in secure system design is the ability to verify and validate the level of security of alternative systems architectures. In the case of smart infrastructure, verification and validation processes require suitable metrics that both represent the security of the cyber network as well as the physical processes it supports. Current literature in security metrics offers a plethora of choices which are considered accurate, valid, consistent, current, replicable, comparable and. In this paper, we describe categories of security metrics that can be customized for different intelligent urban infrastructure systems such as intelligent transportation systems (ITS), smartgrids and cognitive radios among others. It includes a smart grid case study.**

Keywords- securit,y smart grid, metrics

I. INTRODUCTION

One of the critical components of intelligent infrastructure systems is the security of the data networks providing information and control over the physical infrastructure [1]. If concepts such as intelligent city [2] or cognitive city [3] are going to be developed on an architectural level, it is important that cyber security is considered as an integral part of the architecture rather than being added on as an afterthought. Although systems engineering texts typically present cyber security as a non-functional requirement, increasingly frequent cyber security breaches have fostered recognition that security features are essential to the attribution of integrity and availability of the system as whole. Hence, systems as cyber-dependent as a smart infrastructure must consider cyber security as a functional rather than a non-functional requirement.

An important consideration in secure system design is the ability to verify and validate the security of alternative systems architectures. In the case of smart infrastructure, verification and validation processes require suitable metrics that both represent the security of the cyber network as well as the physical processes it supports. Current literature in security metrics offers a plethora of choices which are considered accurate, valid, consistent, current, replicable, comparable and informative [4]. In this paper, we will look at some potential categories of security metrics that can be customized for different intelligent urban infrastructure systems such as intelligent transportation systems (ITS), smartgrids and cognitive radios among others. These categories include security targets, vulnerability, and usability metrics.

Identify applicable sponsor/s here. *(sponsors)*

This paper will illustrate how these three categories of cyber security metrics may be productively applied to determine the relative cyber security level of cognitive city architectures.

II. TYPES OF SECURITY METRICS

A. Targets

Security target metrics are the most common type, and these are based on compliance with a technical evaluation criteria such as the Orange Book or Common Criteria [5, 6]. They rely on accurate and reliable maps from system functions to components, and standards for configuring each component according to a security model.

Target metrics treat the configuration of a single component as a binary measure. Either the target complies with the standard configuration or it does not. As systems typically have multiple different types of components, the compliance of each type of component would be measured separately, and measures for each type of component would then be aggregated using the total number of the components of a given type as a denominator for a ratio measure. Components are also typically assigned a criticality level so that the impact on system security from a given non-standard component is evident. The criticality level would typically appear as a weight in aggregations of the component metric to the whole system security assessment. The results of target metrics are typically displayed in a dashboard presentation that aggregates compliance ratios for all component types within the system of interest. The individual target measures are meaningful only as a percentage of a total in some reference data that is authoritative as to the number of components in the system.

B. Vunerability

Vulnerability testing relies on formal models of vulnerabilities such as software weaknesses compiled in the National Vulnerability Database (NVD), and applies assessment criteria such as the Common Vulnerability Scoring System (CVSS) to determine their relevance to the security of a given system [7, 8]. The use of this data in security metrics has typically been for a security software vendor to provide automated tests that will probe each node on a customer's network to make sure that the vulnerabilities do not exist. Tests for systems-level vulnerabilities are typically referred to as penetration tests or pentests, for short. They are measured by the count of vulnerabilities in the database that are found in the

system, and like target metrics, these may be segregated by criticality of potential system impact for presentation.

Judging security on the basis of testing for known flaws is itself inherently flawed in that it is fraught with both false positives and negatives due to the difficulty of designing and executing tests in multiple environments [9]. Hence, it is most effective when it is combined with a design basis threat (DBT). A DBT describes characteristics of the most powerful and innovative adversary that it is realistic to expect security to protect against [10]. In New York City, it may be a terrorist cell equipped with sophisticated communications and explosive devices. In Idaho, it may be a 20-strong posse of vigilantes carrying machine guns on motorcycles. Adopting a DBT approach to security implies that the strength of security protection required by a system should be calculated with respect to a technical specification of how it is likely to be attacked.

In physical security, this process is straightforward. If the DBT is a force of 20 people with access to explosives of a given type, then the strength of the physical barriers to unauthorized entry must withstand the ton of force that these twenty people could physically bring into system contact. Barrier protection materials are specified, threat delay and response systems are designed, and validation tests are conducted accordingly.

In systems security, potential attacks are generally derived from an analysis of the threat environment which is unique to the system purpose. Threat actors are individuals who benefit from damage to the system or diversion of system resources to unauthorized use cases. As in the physical security case, each threat is analyzed from the perspective of the goals of an attacker, and the corresponding activities an attacker must engage in to achieve each goal. Systems security is then measured in terms of the capability to deter, detect, delay, and defend against those activities.

C. Usability

Usability metrics adopt a stakeholder's perspective on system security, and test the ability of the system to provide stakeholder-requirement functionality in the face of known threats. These include failure mode analysis techniques, reliability and recovery, and may be used for both verification and validation [11].

Concepts in failure model analysis are the same whether they are used as system functional performance metrics or security usability metrics. They include nominal measures of failure type, such as primary and secondary, to distinguish between failure due to natural aging and those caused by excessive and unanticipated stress. Both types of failures can be complete or gradual, intermittent, incipient, or sudden.

Reliability metrics utilize functions that compare time that a system may be exposed to a given load based on its strength. An example of such a function used in security metrics is the calculation of the computing cycles it would take to decrypt data that was encrypted with a given algorithm and key size.

Recovery metrics include mean time to recover from failures in security features. A single case of unauthorized access may be easy to stop in progress by disabling an account. But the system vulnerability that allowed the intrusion may persist, and so the true recovery time involves not just resumption of system functionality, but reconstitution of the failed security feature to prevent further exploit. An individual mean time to recover may be measured in minutes, while the complete security recovery may be measured in days, weeks, or months.

Usability metrics extend to circumstances in which security appears to prevent user access to systems. For example, the time it takes for a user to decrypt data may demotivate them to follow standards for encryption, and hence detract from system security.

III. A COGNITIVE CITY CASE STUDY

A. A Smart Grid

Power Grids are evolving to become Smart Grids. The grid and its associated activities support a community that encompasses individual and enterprise consumers of electricity, as well as their local, state, and federal governments. Grid service providers and customers share common principles and regulatory requirements that create a reliable distributed service from diverse and independent operational strategies.

Following NIST terminology, the Smart Grid is composed of these major domains: service providers, customers, transmission, distribution, bulk generation [12]. These domains include actors in the form of devices, computer systems, software programs, individuals, or organizations that operate in harmony to produce and consume power. The Smart Grid has one "universal" architecture composed of six logical functions in the areas of metering, distribution grid management, electric storage, electric transportation, customer networks, and situational awareness. Each has its own system, so the Grid is a system of systems. Each of these functions has defined interfaces, some of which are Grid system interfaces.

Distributed control systems place power on the grid, either from generators or bulk storage. Customers may either consume electricity or contribute it to the grid via appliances. Grid metering infrastructure includes Supervisory Control and Data Acquisition (SCADA) systems to maintain an inventory of devices, distribution feeder parameters, bulk supply interface points, and customer meter activity. Distributed grid management utilizes Remote Terminal Units and/or Intelligent Electronic Devices (RTUs or IEDs) to receive data from sensors and power equipment. These can issue manual or pre-programmed control commands, such as tripping circuit breakers if they sense voltage, current, or frequency anomalies, or raise/lower voltage levels in or out of electronic transportation and storage facilities in order to maintain a desired service level. The Smart Grid should also enable service providers to respond to sensor data by warning customers of the potential impact of imminent overutilization. Customers would be expected to respond to those signals by issuing commands (or having systems programmed to automatically issue commands) to decrease electricity usage.

B. *Smart Grid Security Target Metrics*

To establish security target metrics, one must first specify a secure configuration for system components. In the case of the Smart Grid, system components are SCADA, RTUs, programmable logic circuits, sensors, and networks that support these and other components using multiple communications protocols. Such diversity of implementation presents a challenge for any attempt to establish target security metrics. As Swirbul described in an article on smart grid communications strategies, where there are no standards, it is difficult to specify what interoperability looks like [13]. The same is true in security.

The closest thing that the Smart Grid has to a component listing is its list of logical functions as defined by NIST [12]. Each of these functions has defined interfaces, some of which are Grid system interfaces, so they may be thought of as systems and the Grid as a system of systems. These functions are not completely realized, but are documented with the intention to provide direction for entrepreneurs, technologists, and researchers with an interest in contributing to national goals for energy economics and interoperability.

TABLE I. SMART GRID LOGICAL FUNCTIONS

Table 1:			
1	AMI	Advanced Metering Infrastructure	Sensors and timely data analysis for decision-support as well as support for data aggregation for historical analysis
2	DGM	Distribution Grid Management	Networked system of feeders, transformers, and other distribution components integrated with both transmission and customer premises equipment
3	ES	Electric Storage	Direct or indirect energy storage facilities
4	ET	Electric Transportation	Accommodation for Plug-in Vehicles (PEV)
5	HAN/ BAN	Home Area Network/Business Area Network	Mechanisms for distribution on demand as well as incentives for customer-initiated economy and efficiency.
6	WASA	Wide Area Situational Awareness	Tools and techniques that allow real-time monitoring, data collection, and data analysis.

When these functions are fully implemented it will be supported with components that are interoperable. The components will presumably have security features. The technical configuration of each security feature would be set based on the owner/operator standards the target security metric would be for 100% of the components of each logical function to have its technical configuration target met. Figure 1 is a security dashboard presenting example metrics for this target. It is in the form of a heat map, where the size of each component indicates its importance to security of the whole, relative to the others. Components that don't meet their security configuration targets appear in red or orange, depending on the extent of the discrepancy.

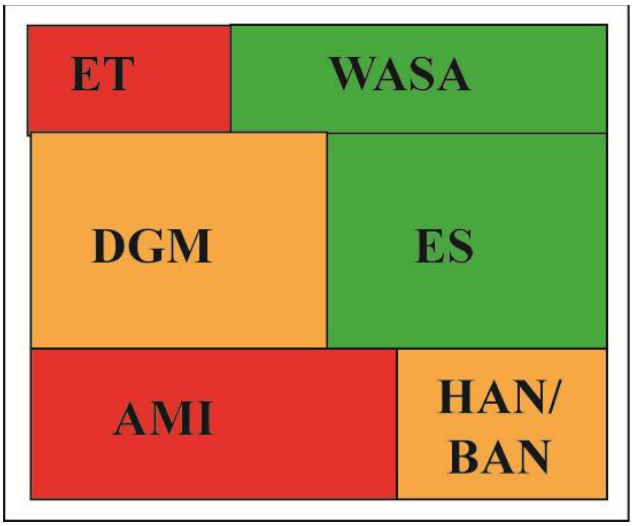

Figure 1. Example Heat Map for a SmartGrid Security Target Metrics

C. *SmartGrid Vulnerability Metrics*

To establish security vulnerability metrics for a SmartGrid, it is first necessary to establish the expected threats. Design basis threats may be derived from a list of known system adversaries with attack goals. For the Smart Grid, adversaries may be (though not limited to) disgruntled employees of power companies, terrorists, or industrial saboteurs. Goals of these adversaries may be to create power outages or to gain free access to grid resources. Attack goals are typically analyzed with an attack modeling tool called an attack tree. The goal is at the top of the tree and the methods to achieve the goal are subgoals that form branches. The leaves of the tree are individual attacker activities that when combined may achieve the attack goal. Figure 1 is an example of an attack tree wherein the attacker goal is a power outage. The goal can be achieved in one of two ways, by disabling infrastructure or subverting control systems.

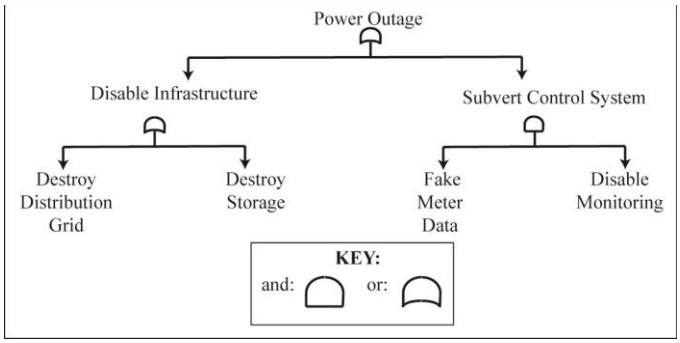

Figure 2. Attack Tree for a Power Outage

Vulnerability metrics are typically created by anticipating adversary activity in support of attack goals within an estimation of the expected level of effort that an adversary may have available to rally to their cause. In the case of the activity in Figure 2, *Destroy Distribution Grid*, an owner/operator may assume that the largest force that would assemble for such activity may be 10 people with semi automatic weapons. Attack scenarios would be plans using those forces against physical defense mechanisms surrounding the Grid. Although

simulations of such attacks are rare for physical security metrics, they are more common in cyber security metrics. The *subvert control system* goal achievement via *faking meter data* and *disabling monitoring* may actually be attempted by the force expected of an adversary on a system normally used for testing. In either case, the results of these exercises become metrics demonstrating whether or not security goals are met.

Note that vulnerability measures may not always use accurate projections of adversary effort nor assemble the same skill sets in their test teams that adversaries may have. Hence they can only prove that systems are not secure. They do not provide evidence that systems have been secured, especially when tests are not performed on the action system. For this reason, one security expert has labeled these tests, "badness-ometers [14]." As depicted in Figure 3, badness-ometers are scales in which all measures are bad. There is no measure that could result from the test that shows security is good.

Figure 3. A Badness-ometer [14]

D. Smart Grid Security Usability Metrics

To establish security usability metrics for Smart Grid., one must first specify performance criteria for operation. Concepts and usability corresponds to avoidance of failure due to adversary activity. Adversaries may be internal or external. Security failure modes, like other failure modes, are measured in terms of reliability under stress. Reliability functions are often referred to as *survivor* functions. Generic systems reliability functions such as mean time to failure (MTTF), mean time between failure (MTBF), and mean time to repair (MTTR) may be used to measure system security in that any effort to improve robustness and resiliency for any reason will serve a security purpose in that the improved performance will be less vulnerable to some type of threat. Security-specific usability metrics include response capability required in the event of an adversary attack. They are used in conjunction with system performance measures to add security dimensions to a system usability assessment.

An example of a security specific usability metric approach to this comparison is a Security Work Factor Ratio ("SWFR") between "time to protect" and "time to attack" [93]. A SWFR is a product of two measurements, defined as:

- The time to protect (TTP) is the average interval between when a target is first aware of the existence of a new threat and when it successfully deflects it. This measure depends mainly on the speed and effectiveness of a target's response capability.
- The time to attack (TTA) is measured as the median lifetime of malicious activity emanating from a specific source. This is useful to measure in situations where attackers must constantly create and abandon original points to evade detection. The shorter this median lifetime, the heavier is the burden on the attacker to continuously change its location to evade detection.

To the extent the ratio TTP/TTA is minimized, the defenders are successfully thwarting attacks. To the extent it increases, the attackers are more successful. The goal of absolute security would be measured with a TTP/TTA metric that is better as the ratio approached zero.

To measure whether security goals met in a given Smart Grid, the TTP may be derived from a combination of the vulnerable components that need to be compromised for an attack to succeed, and the security controls that detect failure in those components and follow that detection with a response that neutralizes the attack. SWFA measures extent to which attacks can be routinely deflected with minimum damage to the system. As adversaries develop new attacks, the SWFA may change without warning. If adversaries may repeatedly successfully execute the same or similar attacks, the SWFA is clearly inadequate.

For example, assume that a cyber attack replaced a Smart Grid's meter feeds with data that shows there is no demand for power and replaced its monitoring data in correspondence. The control system, following its normal program, would reduce power distribution, causing a power outage due to control system subversion, as depicted in Figure 2. Such a scenario could be detected by security monitoring features that triggered appropriate response such as automated restoration of data feeds via a backup system. However, consider a case wherein the response takes so long that power outage could not be avoided, and the attackers are able to repeat the attack with little fear of retribution. The detection and recovery scenario would then not be sufficient to secure this system.

For example, assume that the attack could be executed repeatedly over a period of five days with little or no impact to adversary capability while the recovery took 12 hours to respond to the first attack. Assume that the recovery restored capability, but did not close the vulnerability that was exploited to complete the attack. In this case, the MTBF may be expected to be ~14 hours because the adversaries will see the power come back soon after the repair is complete. Against this backdrop of security failure induced performance failure, the security situation may be measured using SWFR. However, one of the components of the SWFR is the TTP, which requires successful deflection of the attack. The difference between security recovery and normal system recovery metrics is that returning the system to the state just prior to attack does not count as security recovery. While this system is still vulnerable during the adversaries time to attack. Assume that the experience of the first attack provided the system owner/operator with enough information to reconfigure their system to avoid further vulnerability, but that the, but that they were not able to implement a fix prior to experiencing the second attack, which occurred immediately after the first, and

further, that they did successfully deflect the third. Then the time of recovery is not 12 hours, but includes all time between initiation of the first attack up to reconfiguration. Assume 25 hours is the actual TTP. The SWFR is 25/120 = ~0.2. However, if attacks are difficult to detect, there is still the potential for the system to be down for the lifetime of the adversary capability. Hence incident detection and response capability metrics are key performance indicators for actual secure operation.

IV. Comparing Security Architecture

Assuming that security metrics may be established by following the above guidelines, these metrics could then be used to compare two systems of the same type. The target security metrics could be used to verify whether designs were properly implemented. The vulnerability security metrics could be used to determine whether design goals for security were met. The usability security metrics could be used to determine whether the services provided by the infrastructure are themselves secure. The following three figures show how each of the individual examples of depiction of security metrics may be expanded to compare the metrics of two different systems. Figure 1 compares the target metrics for each Smart Grid component identified in Table 1 in different cities to each other. Figure 2 compares the efficacy of the same penetration tests in achieving adversary goals in three different infrastructures. Figure 4 compares the Security Work Factor Ratio between attackers and defenders for different Smart Grid owner/operators in different cities.

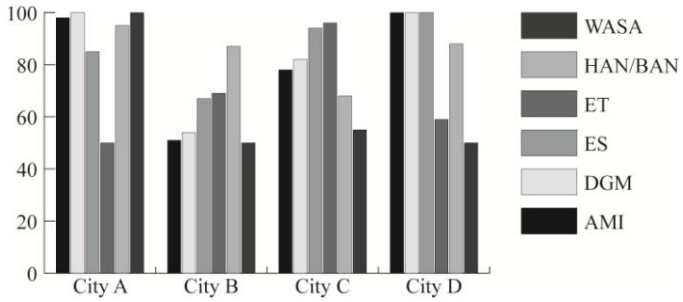

Figure 4. Security Target Metrics Comparison

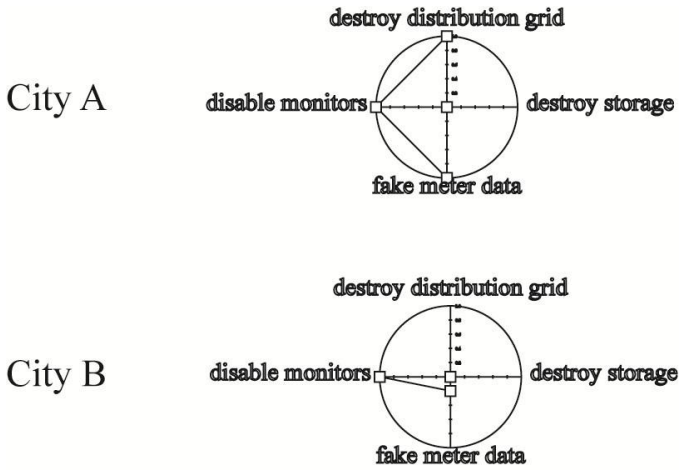

Figure 5. Security Vulnerability Metrics Comparison

TABLE II. Security Usability Metrics Comparison

Adversary Activity	**Metrics**	**City 1**	**City 2**
Disable infrastructure	TTP	2	4
	TTA = 24 hours	24	24
	SWFR	.8	.16
Subvert control system	TTP	12	24
	TTA = 120 hours	120	120
	SWFR	.1	.2

V. Conclusion and Next Steps

We have shown that security target, vulnerability, and usability metrics can be productively customized for a quintessential intelligent urban infrastructure system: a Smart Grid. These techniques may also be productively utilized for other intelligent urban infrastructure systems such as intelligent transportation systems and cognitive communications systems. We have demonstrated how to compare the security of two or more such systems using security metrics. Where such measurements are applied to emerging infrastructures, they may be correlated with actual security events in an attempt to validate which metrics are more effective for a given architecture pattern.

Were requirements for measuring security considered in the design stage for intelligent urban infrastructure systems, the application of security metrics techniques would be easier to accomplish. As sets of security metrics are validated for given architectures, the architectures themselves should be expanded to ensure that provisioning tools and techniques for security measurement are part of their core functionality. Comparative research on security metrics in the future may then also reveal that certain types of functional security measures are more economical and efficient than others.

References

[1] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*: Momentum Press, 2010.

[2] R. Hollands, "Will the real smart city please stand up?," *City* vol. 12, pp. 303-320, December 2008.

[3] A. Mostashari, "Systems-Level Modeling of Sociotechnical Systems," in *Socio-Technical Networks*, F. Hu, *et al.*, Eds., ed: CRC Press, 2011.

[4] D. Herrmann, *The Complete Guide to Security and Privacy Metrics*. Boca Raton, FL: Auerbach Publications, 2007.

[5] DoD, "The Orange Book, Trusted Computer System Evaluation Criteria," vol. (supercedes first version of 1983), ed: Department of Defense, 1985.
[6] ISO/IEC, "Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model (ISO/IEC 15408)," ed: International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2009.
[7] P. Mell, *et al.*, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," Forum of Incident Response and Security Teams (FIRST)June, 2007 2007.
[8] MITRE, "Common Vulnerabilities and Exposures, dictionary of common names for publicly known information security vulnerabilities," ed. http://cve.mitre.org Ongoing.
[9] E. B. Fernandez and N. Delessy, "Using Patterns to Understand and Compare Web Services Security Products and Standards," in *Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT/ICIW 2006)*, 2006.
[10] M. L. Garcia, *The Design and Analysis of Physical Protection Systems*: Butterworth-Heinemann, 2008.
[11] M. Rausand and A. Hoylan, *System Reliability Theory, Second Edition*: Wiley, 2004.
[12] The Smart Grid Interoperability Panel – Cyber Security Working Group, "Smart Grid Cyber Security Strategy and Requirements - DRAFT NISTIR 7628," ed: National Institute of Standards and Technology, Information Technology Laboratory, 2010.
[13] C. Swirbul, "Smart Grid Communications," *Transmission & Distribution World*, 2011.
[14] G. McGraw, *Software Security*: Addison-Wesley, 2006.