Security V&V

Jennifer Bayuk, Ali Mostashari, and Brian Sauser
Stevens Institute of Technology

Overview

Current security standards provide guidance on how to select and implement security measures, but they leave high level decisions on enterprise security architecture and risk to the system owner or operator [1-4]. Enterprise security programs may comply with security standards, yet still not serve the mission of a given enterprise [5]. NIST characterizes this distinction as *correctness versus effectiveness (C&E)* [6]. This paper provides a path to security *effectiveness* that also imparts security *correctness*. It offers methodology with which to quantify security success and failure by contrasting metrics of security C&E, as well as metrics of security testing and evaluation (T&E).

In the field of systems engineering, the terms *correctness* and *effectiveness* may properly be translated as *verification* and *validation (V&V)*. *Verification* and *correctness* criteria ask, "*Did we build the system according to specifications?*" *Effectiveness* and *validation* ask, "*Did we specify the right system?*" Yet the systems engineering approach to security has yielded no better outcome than security standards bodies. Although one systems engineering textbook attempted to model enterprise security using an enterprise architecture framework [7], that attempt did not result in a comprehensive way to validate enterprise security, and the book is now out of print. Even textbooks that combine security and engineering principals emphasize the mindset of the security engineer rather than suggest any standard methods, tools, and procedures with which to approach systems security engineering [8, 9].

Recent data breach cases and industrial control system incidents call attention to the inadequacy of current approaches to systems security [10, 11]. Each case presents more compelling evidence of the potential economic impact of cybersecurity threats. Each case adds to the recognition that security cannot be assumed to be provided by existing correctness standards for technology control. Vast amounts of sums have been directed toward cybersecurity solutions [12, 13]. Yet there is no theoretically proven method of deciding on what that money should be spent, and no new paradigms have evolved to guide management decisions toward practical security solutions [14, 15]. By contrast, we present an approach that could provide clear direction for decision-makers who must make critical decisions on how security dollars should be spent.

Current approaches to cyber security metrics apply standards criteria to an enterprise security program to determine its security strength. Such approaches measure process rather than results and do not account for the value of the assets/resources that are potentially subject to compromise, or the degree of certainty that threats will materialize and assets succumb [16].

Where current security decision guidance includes value loss and uncertainty measures, it concentrates on security risk, the cost of controls, and the expected benefit of return on a single security investment [17]. In contrast, a system security architecture approach to making optimal security decisions includes security requirements corresponding to enterprise mission and threat environment. This requires major enhancements to security metrics data generation, collection and analysis, and the corresponding decision analysis and response options. The decisions made using these improved methods will lead to increases in security effectiveness as well as more cost-effective deployment of security resources.

This research is the first attempt to prove that one approach to systems security is provably better than another by:

- proposing a framework for measuring system security at the architecture level.
- providing an explanatory and descriptive model for systems security that decision-makers may use to understand the security implications of system design alternatives.

System security architecture has traditionally evolved via application of standards and best practices using a system-wide approach. This is at least in part because systems engineers consider security a non-functional requirement. However, as security increasingly becomes a core component of system survivability, stakeholders have become more explicit about articulating expected system security features. Stakeholders also have expectations that security feature capabilities will be maintained throughout the system lifecycle, despite changes in system subfunctions and context of operations. This paper presents a framework whereby security features may be matched with system architecture.

Though the field of systems architecture patterns itself is still evolving, it is possible to produce architecture patterns that may be used to illustrate the concept of a security architecture framework. Security architecture frameworks extend and enhance systems architecture patterns to produce system security metrics that correspond to the architecture pattern. The framework approach enables system owners and operators to:

- Identify security features that correspond to system functions.
- Identify security features required to maintain integrity over system interfaces.
- Evaluate the extent to which their systems are protected from known threats.

Due to the possibility of threats that are unknown, no system will ever be 100% secure. The framework will provide value in its ability to measure the security of a given system compared other systems with similar function and purpose.

SERC Security Roadmap

This work builds on the foundation created in the System Engineering Research Center (SERC) Systems Security Research Roadmap [18]. In that effort, it was emphasized that progress in

system security research must follow a scientific process that includes clear problem statements, thorough problem background descriptions including a full literature review, clearly defined solution criteria, and proposed hypothesis formulated to shed light on a solution and how it may be proven or disproven.

The roadmap acknowledges that simply challenging the systems engineer to put aside security standards and start afresh will not resolve systemic security problems. The existing standards came about because security is a difficult problem to address. Current standards and models have been embraced by a generation of practitioners who entered the systems security field over the past forty years because those practitioners found common solutions to diverse security problems and shared them. This work is significant and should be leveraged by integrating it with a fresh look at the mission of the systems engineer with respect to security.

The fresh look should start with a concept of security that allows it to be understood as a tangible systems attribute. Security provides safeguards that contribute to a system's ability to achieve its mission and purpose in the face of changing threats. By this definition, it may be included in requirements as a system capability with a clear and measurable goal, albeit one that is customized in context. A clear understanding of the definition of security in the context of a given system mission should allow the design of alternative security architectures, as well as metrics that can be applied to those architectures in order to determine their effectiveness in maintaining system security.

Security architecture frameworks following this methodology extend and enhance systems architecture to produce security requirements at the system rather than at the security technology level [19]. This allows for security V&V to be designed at the system level rather than as a build-to specification. The security metrics that result from these efforts are expected to play a key role in the development of new tools for use by systems security engineers. Of course, due to the possibility of threats that are unknown, no system will ever be 100% secure. Nevertheless, this approach should enable system owners and operators to:

- Identify security features that require system-level functions.
- Evaluate the extent to which security features protect systems from deliberate damage that would cause system failure.
- Devise V&V metrics at the system level that show security requirements are met.

Figure 1 illustrates the approach. By extracting the definition of security from the system mission and the context within which it operates, security architecture can be integrated into systems architecture, customized rather than bolted-on. Architecture metrics may be devised that measure whether security functional requirements are met by security features. Systems exhibiting similar architecture patterns may then benefit from common security architecture models. The existence of common security architecture models should make it possible to develop tools that may be developed to guide future engineering efforts toward more secure solutions.

Security Models

As George Box is often quoted, “All models are wrong, some models are useful.” Models that are useful in formulating security requirements are available. They include technical descriptions of operating system security features, network-centric defense-in-depth strategies, data-centric digital rights management, security services, and software security patterns [20-23]. Figure 2 summarizes these approaches. The models are designed to assist engineering in selecting the right set of security controls from a list of those available to secure a system. However, they provide no guidance on what actually should be secured, nor do more the more official industry standards [24]. Current model and standards based approaches assume that needs for security have been identified and the decisions are at the level of the cost/benefit utility of alternative sets of security mechanisms. Where cost/benefits are quantified, they proceed on a case-by-case basis rather than at a holistic system or mission level [25]. These approaches appropriately form the basis for security verification strategies, but lack the overall security goal-oriented guidance that would provide a formal basis for a validation strategy.

A validation strategy for security would entail measures that a system is resilient in the face of changing threats. In order to formalize a validation strategy, once must have a clear sense of system mission or purpose as well as a definition of security as an attribute of a system that thwarts perpetrators who enact threats to exploit vulnerabilities that permit system disruption. This means security metrics are measures useful in assessing the extent to which a system is invulnerable to disruption via perpetrators. It does not provide a definition of absolute security, but this compromise may be acceptable. As Ross points out, even ambitious goals for system feature availability are six-sigma [26], and a six-sigma level of security is not secure for five minutes a year [27], during which time, it could be completely compromised. He concludes that it is foolish to make absolute statements about information security.

We attempt to model security by examining a system or enterprise through a security lens, one in which security is used as a measure applied to system structure and process [28]. This concept of security can be used to explore the state (secure or insecure) of the structure and process of a system or enterprise. Seen through this lens, an enterprise already includes many functions that would typically be viewed as security-specific. But in fact, these functions were designed in response to enterprise goals that are not security-specific. Figure 3 is a list of systems architecture categories and corresponding built-in mission requirements that overlap with security measures. The overlap column identifies measures that will be assumed to be part of any system in the given category. The last column identifies a security measure that would typically be considered an add-on due to a security-specific requirement. Such security measures are seen as add-ons because it is not clear to stakeholder how they support the system or enterprise mission (and in some cases, they may not).

The concept of security as an attribute of enterprise mission is illustrated in the systemigram of Figure 4. The concepts are depicted using a systems engineering job aid, a *systemigram* [29]. A

systemigram describes a system succinctly by way of a "mainstay" thread, which is conventionally placed in the systemigram illustration from left to right, top to bottom, and appears in bold. The mainstay may be viewed as the main thing a system must do in order to be the system named. This is a high level process that is generally agreed by those who best understand the system. The example in Figure 4 is a generic enterprise. Other threads describe actions taken by the system that, though not central to its purpose, are nevertheless associated with any system so named. A systemigram does not produce a single paragraph of text, many of its threads skirt around its subject in an effort to add dimensions to the definition. Each set of noun-verb combinations link the concept to be defined to the object of its actions. The mainstay thread may be viewed as the core definition. But there is no assumption that the mainstay can stand on its own.

Security is depicted as a support structure for the enterprise. This construct links the goals of security to the goals of the enterprise. The systemigram approach allows the development of security validation strategies using model-dependent realism. Such goal-oriented, scientific model of enterprise security is expected to use both verification and validation measurement and metrics. Scientific validation will rely on construct validity, which involves identifying relationships between theories and measurable things that correlate with those theories. As Carmines and Zeller put it, ”the extent to which a particular measure relates to the other measures consistent with theoretically derived hypotheses concerning the concepts” [30]. Theoretical concepts are by nature abstract, and therefore hard to articulate in order to establish common understanding. It is therefore helpful to be able to derive testable hypotheses that, if true, would provide evidence to support the theory. Hypotheses concerning system security will serve to test validity, and at the same time they provide a comprehensible framework for interpreting the results of the testing in a way that leads to a more thorough understanding of security itself.

To effectively use construct validity, we will have to find some indicator that security is present, and identify evidence of it. If we establish an empirical relationship between the theory that security support enterprise mission, and a substantial body of evidence, then we will have established the basis for security metrics. Of course, measures must be devised to test for the evidence of the indicators. If the indicators and the original concept have a positive correlation, then the measurement lends validity to the construct.

The model will allow the current spectrum of well-defined security measures to be mapped isomorphically to system security goals to ensure coverage for both security validation and security verification techniques. This will allow formal tracing from available security V&V metrics to security V&V requirements. Any gap in coverage between security requirements and security V&V capability may then be identified.

Conclusion and Next Steps

A key element of the systems security engineering roadmap is to provide capability for security researchers to self-assess the value of a potential contribution to the field. An engineering approach to V&V of security requirements will ipso facto provide methodology to test a research hypothesis. There are a number of feasible alternatives for a launch point from current systems engineering tools and techniques to a security design goal analysis. For example, failure modes, effects, and criticality analysis (FMECA) can be used to identify the impact of system failure on enterprise operations [31]. Black box diagrams and equivalence partitions may be used to frame state transitions between stable and unstable outcomes. Goal, Question, Metric (GQM) methodology may help enterprise stakeholders articulate infrastructure affect on process [32].

The utility of these tools in the pursuit of goals for secure design is ostensible while their applicability in the context of a systemic security metrics is yet to be determined. By using these tools in conjunction with systems thinking approaches, we hope to devise validation metrics that are consistent with current security verification techniques.

Security research employing such methods should be able to build on prior results by citing successful V&V results in similar architecture patterns. Though such an engineering approach may seem like practical application rather than research to some in our community, they may be overlooking the fact that security is not at all well understood, and so any serious investigation of its properties constitutes a research endeavor.

Figure 1: SERC Roadmap

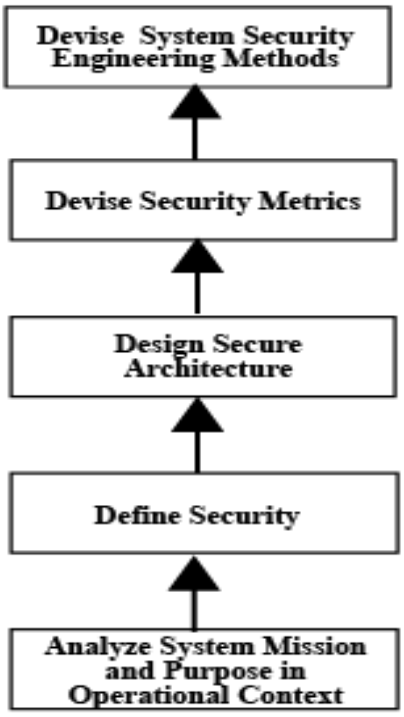


Figure 2: Security Models

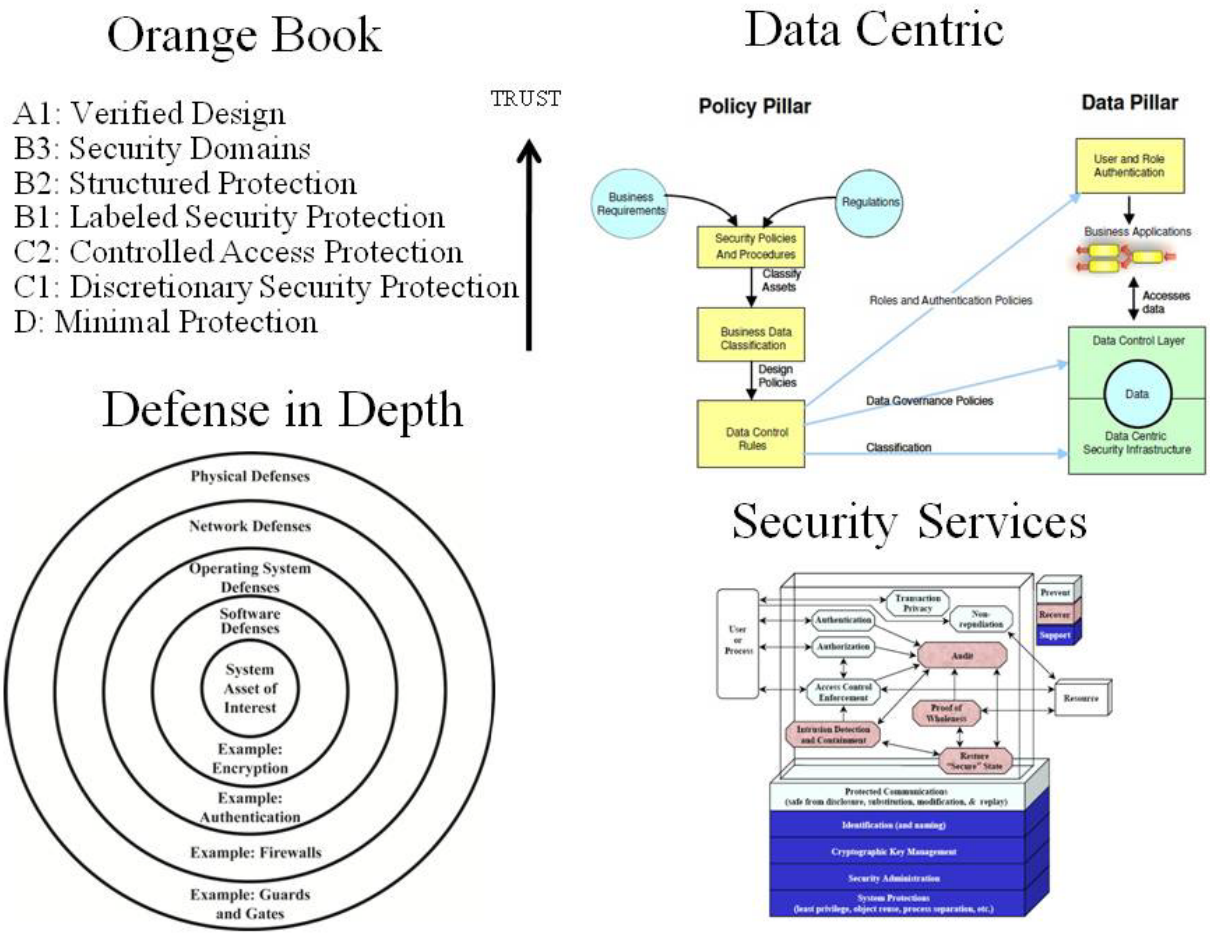
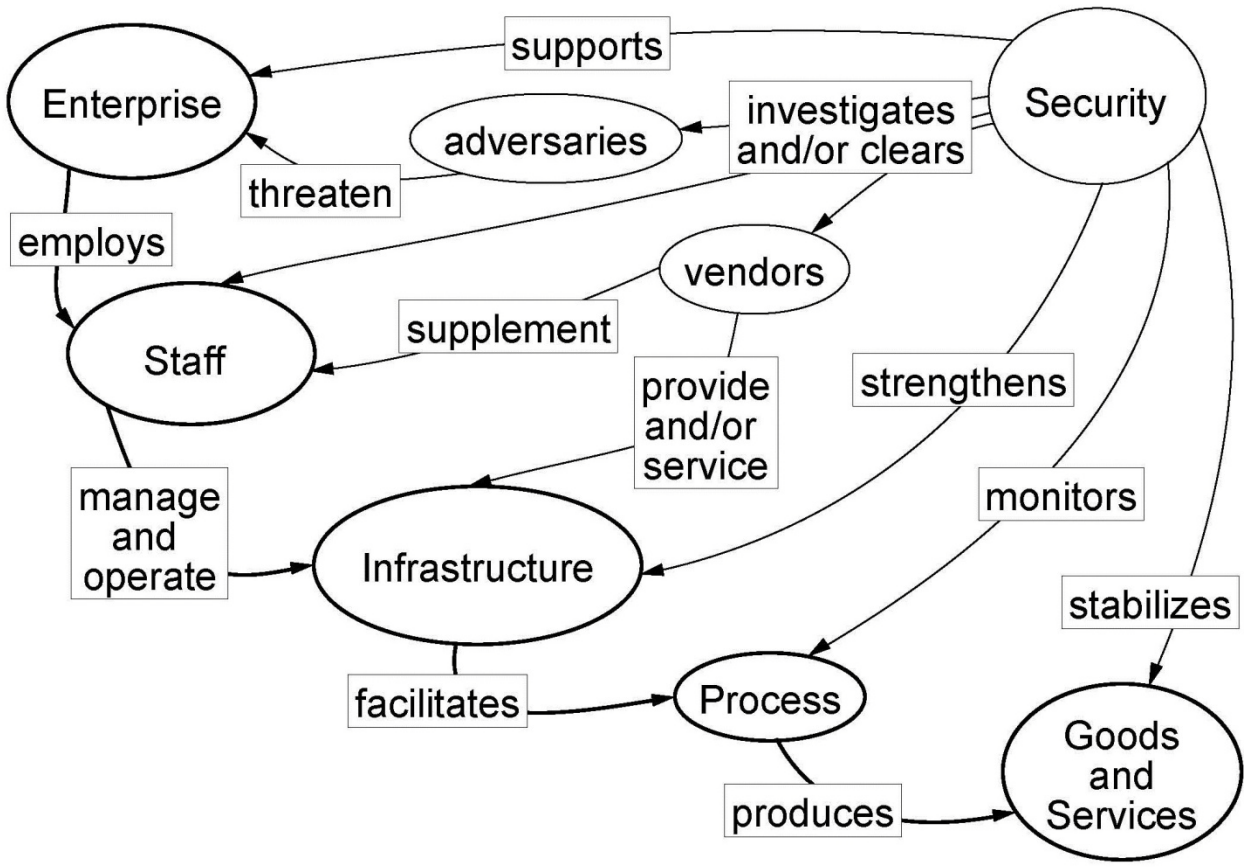


Figure 3: Systemic Security Overlap

System	Overlap	Security
Sensor-enabled Monitoring	Data Continuity	Confidentiality
Telecommunications	Protocol integrity	Bandwidth utilization forensics
Financial Services	Identity management	Transaction Audit
Military	Confidential communications	Recovery and Reconstitution
Industrial Control	Incident detection and recovery	Protection against insider threat
SmartGrid	Accountability	Theft and Fraud investigation
Airspace	Situational Awareness	Software integrity
Cyberspace	Software integrity	Privacy

Figure 4: Security Systemigram



1. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). *Information technology — Security techniques — Information security management systems —Requirements (ISO/IEC 27001)*. 2005; Available from: www.iso.org.
2. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), *Information technology — Security techniques — Code of practice for information security management (ISO/IEC 27002)*. 2005.
3. Ross, R., et al., *Recommended Security Controls for Federal Information Systems, SP 800-53 Rev 2*, National Institute of Standards and Technology, Editor. 2007.
4. Swanson, M., J. Hash, and P. Bowen, *Guide for Developing Security Plans for Federal Information Systems, SP800-18 Rev 1*, National Institute of Standards and Technology, Editor. 2006.
5. Mogull, R., *An Open Letter to Robert Carr, CEO of Heartland Payment Systems*, in *Securosis Blog*. 2009, Securosis.
6. Jansen, W., *Directions in Security Metrics Research*. 2009, National Institute of Standards and Technology Interagency Report.
7. Sherwood, J., A. Clark, and D. Lynas, *Enterprise Security Architecture*. 2005: CMP Books.
8. Anderson, R., *Security Engineering, Second Edition*. 2008: Wiley.
9. Bishop, M., *Computer Security, Art and Science*. 2003: Pearson Education.
10. McGlasson, L., *More Heartland-Related Fraud Detected*, in *Bank Information Security* 2010.
11. Fuhrmans, V., *Virus Attacks Siemens Plant-Control Systems* in *Wall Street Journal*. 2010.
12. Williams, C., *Cameron to spend £1bn+ on cyber security*, in *The Register*. 2010.
13. Cacas, M., *DHS outlines cybersecurity planning* in *Federal News Radio*. 2010.
14. Spafford, G., *Privacy and Security Remembrances of Thing Past.* Communications of the ACM, 2010. **53**(8): p. 35-37.
15. Shipley, G., *Epic Fail*, in *Information Week*. 2010, UBM Techweb. p. 26-38.
16. Axelrod, C.W., *Accounting for Value and Uncertainty in Security Metrics.* Information Systems Control Journal, 2008. **6**.
17. Gallaher, M.P., A.N. Link, and B.R. Rowe, *Cyber Security, Economic Strategies and Public Policy Alternatives*. 2008: Edward Elgar.
18. Bayuk, J., et al., *Systems Security Engineering, A Research Roadmap, Final Technical Report*. 2010, Systems Engineering Research Center (www.sercuarc.org).
19. Bayuk, J.L. and B.M. Horowitz, *An Architectural Systems Engineering Methodology for Addressing Cyber Security.* Systems Engineering, 2011. **14**(3).
20. The Orange Book, *Trusted Computer System Evaluation Criteria*, Department of Defense, Editor. 1985 (supercedes first version of 1983).
21. Stoneburner, G., *Underlying Technical Models for Information Technology Security*, National Institute of Standards and Technology, Editor. 2001.
22. Schumacher, M., et al., *Security Patterns, Integrating Security and Systems Engineering*. 2006: Wiley.
23. Grandison, T., et al., *Elevating the Discussion on Security Management, The Data Centric Paradigm*, in *International Workshop on Business-Driven IT Management*. 2007, IEEE.
24. Bayuk, J., *The Utility of Security Standards*, in *International Carnahan Conference on Security Technology (ICCST)*. 2010, IEEE.
25. Bayuk, J., *Enterprise Security for the Executive: Setting the Tone at the Top*. 2010: Praeger.
26. Pande, P., R. Neuman, and R. Cavanagh, *The Six Sigma Way*. 2001: McGraw-Hill.
27. Ross, S.J., *The Right Question.* Information Systems Control Journal, 2005. **4**.
28. Wirsbinski, J. and J. Boardman, *Establishing Security Strategy Using Systems Thinking.* INCOSE Insight, 2009. **12**(2): p. 41-43.

29. Boardman, J. and B. Sauser, *Systems Thinking: Coping with 21st century problems*. 2008: Taylor & Francis.
30. Carmines, E. and R. Zeller, *Reliability and Validity Assessment*. Quantitative Applications in the Social Sciences, ed. M.S. Lewis-Beck. 1979, Thousand Oaks, California: SAGE Publications.
31. Rausand, M. and A. Hoylan, *System Reliability Theory, Second Edition*. 2004: Wiley.
32. Basili, V.R., G.H. Caldiera, and D. Rombach, *The Goal Question Metric Approach*. 1994, University Of Maryland.

April 2011
Security Verification & Validation
Conference on Systems Engineering Technology (CSER)
An INCOSE Conference. http://www.incose.org