Secure Adaptive Response Potential (SARP): A System Security Metric

Joseph J Simpson
Missouri University of Science and Technology
6400 32nd Avenue N.W., #9
Seattle, WA 98107
(253) 773-3941
jjs-sbw@eskimo.com

Dr. Ann Miller
Missouri University of Science and Technology
Department of Electrical and Computer Engineering
Rolla, MO 65409-0040
(573) 341-6339
annmiller@ieee.org

Dr. Cihan H Dagli
Missouri University of Science and Technology
229 Engineering Management and Systems Engineering Department
Rolla, MO 65409-0370
(573) 341-4374
dagli@umr.edu

Abstract. System design, development and operational activities are monitored and evaluated to facilitate proper system security management in all phases of the system life-cycle. Effective system security metrics must address all phases of the system life-cycle as well as the associated organizational elements that interact during the system life-cycle to produce and operate the system of interest. A single system security metric, built from multiple components, is presented here as a fundamental system management security metric. This single technical security metric is used to support and evaluate the allocation of corporate and program resources, including time and budget.

Introduction. The current state of the international information technology (IT) infrastructure is an artifact of over twenty five years of explosive system and infrastructure growth. This phenomenal growth was based, in the beginning, on a few architectural and operational principles relating to open systems interconnection and open network interfaces. As the systems developed, the original system architectural principles were augmented with commercial and business decisions aimed at market dominance, “first-mover” status and system ease-of-use features. These factors, taken as a collective whole, created an IT infrastructure of physical components, software products and computing services that are not naturally secure (Schneier 2007). The value added by network-enabled capabilities must now be evaluated and balanced against the expected value loss from the existing, insecure, IT infrastructure.

The daily challenge facing current system and organizational managers is the balancing of the great value gained from network-centric and network-enabled systems with the increasing security threats associated with network components that are fundamentally insecure. Assisting and guiding IT and corporate managers in the journey from high-value, high-threat IT networks to a future of high-value, highly secure IT networks is the primary purpose of the secure adaptive response potential (SARP) system security metric.

Standard Systems Development and Operational Evaluation Processes

Standardization of network components, operations, specifications and interfaces is a primary enabler in the development, deployment and operation of large-scale systems and systems-of-systems. Important international standardization work has been evolving since the International Communications Union was founded in 1865. Today, corporate decision makers have access to a wide range of systems engineering and network operational standards. Many large corporate organizations as well as governmental agencies have used these standards as the basis for company specific policies, practices and standards. The “Standard for the Application and Management of Systems Engineering Processes”, IEEE 1220 and “Processes for Engineering a System”, EIA 632, are two examples of systems engineering standards that are currently in use in industry and corporate IT organizations (Coallier 2007).

The United States Department of Defense (DOD) and the Federal Aviation Administration (FAA) sponsored an activity to incorporate safety and security standards into the current Integrated Capability Maturity Model (iCMM). These extensions to the current iCMM are designed to be used in four basic contexts: evaluation of supplier components and products, operational and production environment evaluation, program level audits, and strategic planning evaluation in the areas of safety and security. The extensions are organized into a security and safety application area which contains a group of standard safety and security goals with associated application practices and processes.

Four new safety and security goals were introduced in this set of iCMM extensions:

- Goal 1: An infrastructure for safety and security is established and maintained.
- Goal 2: Safety and security risks are identified and managed.
- Goal 3: Safety and security requirements are satisfied.
- Goal 4: Activities and products are managed to achieve safety and security requirements and objectives.

These four goals are further defined and developed by assigning standard practices that are used to achieve each of the goals. There are sixteen practices that are used to achieve the goals, approximately four practices per goal (Ibrahim 2007).

The international security research community has also produced a variety of approaches to the system security audit and measurement problem. These approaches include the INFOSEC Assessment Capability Maturity Model (IA-CMM) and the Systems Security Engineering Capability Maturity Model (SSE-CMM). Specific system security monitoring and metric production is accomplished in an environment where an organization may be moving up the capability maturity scale while at the same time engaging in a wide range of network-centric activities. This dynamic, network-enabled, capability development requires an adaptive component in its overall, system security metric. In these cases, the system security metric and metric application process should be handled in the same manner as all other system technical performance metrics (Kanava 2007).

Security Measurements, Metrics and Requirements Structure

The functional, structural and operational similarities and differences between security measurements, security metrics and security evaluation frameworks must be clearly defined and communicated. Security measurements are a one-time evaluation of individual measurable system security parameters. Security metrics are composed of two primary parts. The first part is a set of measurements that have been collected over a period of time. The second part is a standard method used to evaluate and communicate the meaning of the collected measurements. A security evaluation framework establishes a standard structure that is used to relate the established system security metrics to each other as well as other types of system management metrics and practices.

System security measurements are the foundation for both the security metrics and security framework. Effective system security measurements are based on three general aspects of the system under evaluation: the system or object to be measured, the measurement method, and the security requirements for the system or object. There is a natural relationship between measurement methods and the system and/or operation being measured. For example, organizations will collect organizational measurements while operations will collect operational measurements. As a result, subsystems or subcomponents of a larger system are measured by one measurement technique while a different measurement technique is applied to the larger system or system-of-systems. The natural structural hierarchy of operations and system aggregation must be considered in the development of system security metrics and frameworks.

System security requirements can generally be viewed as either information security requirements or system operational requirements with some requirements appearing in both areas. Information security requirements categories include confidentiality, integrity, availability, authentication and non-repudiation. System operational requirements categories include stability, reliability, safety, maintainability, confidentiality, integrity and availability. Specific system security requirements associated with an individual system or component must be evaluated and considered in the context of the complete system of interest. When the total system of interest is viewed in a hierarchical form, the security requirements, measurements and metrics can be mapped directly onto the hierarchical, system structure. This type of mapping facilitates the identification of areas that lack essential requirements, measurements and metrics.

The complex nature of network-centric systems and network-enabled capabilities provides a rich conceptual ecology that encourages a wide variety of system views, analytical interpretations and system representations. While each of the system representations may highlight and provide emphasis for the conditions in local subsystems and/or constrained, system-operational threads, these representations must be aggregated and normalized to provide insight and guidance to the global network system level of interaction. Executive-level managers desire a single, management metric, based on component metrics, that provides a meaningful representation of the organizational system state. The process of developing and communicating both a top-level metric and its component metrics is used to identify and organize the controlling organizational relationships and value set. The output from this process is a negotiated, normalized metric set that executive management understands and will use in their decision making process (Jones 1995).

System Security Framework and Evaluation Structure

A system security evaluation framework establishes the basis for clear definition and communication of system security attributes, values, and events. The general SARP metric is constructed from a compilation of system views, each of which has been evaluated to determine its contribution to the integrated SARP system metric. At the most fundamental level, the SARP metric is organized around a classical system model used in structured, systems analysis. The system model has six components: two that address the system boundary, two that address the system problem statement, and two that address the system solution statement. The system boundary is described by the context component and the concept component. The context component focuses on the view external to the system while the concept component focuses on the view internal to the system. Taken together these two views describe the complete system boundary. The system problem statement is detailed by a combination of the function component and the requirement component. The function component fully describes the system functions, while the requirement component fully describes how well each of the system functions must be performed. The system architecture component describes the mechanism that performs the systems functions and the system test component details the process used to determine that the system architecture component performs the system functions to the degree specified by the system requirement component. The model is named CCFRAT after the six components: context, concept, function, requirement, and test (CCFRAT) (Simpson 2005).

The SARP is composed of four general categories of subsidiary metrics: organizational, technical, operational and context-specific metrics. The structure and organization of the SARP is shown in Figure 1. Each of the scales in the SARP are organized and represented as fuzzy number scales. This approach provides flexibility and adaptability allowing the specific values on each scale to be adjusted to fit the specific system context. This feature of the SARP metric allows the metric to be adjusted as experience and information is gained during the system design, development and operational phases.

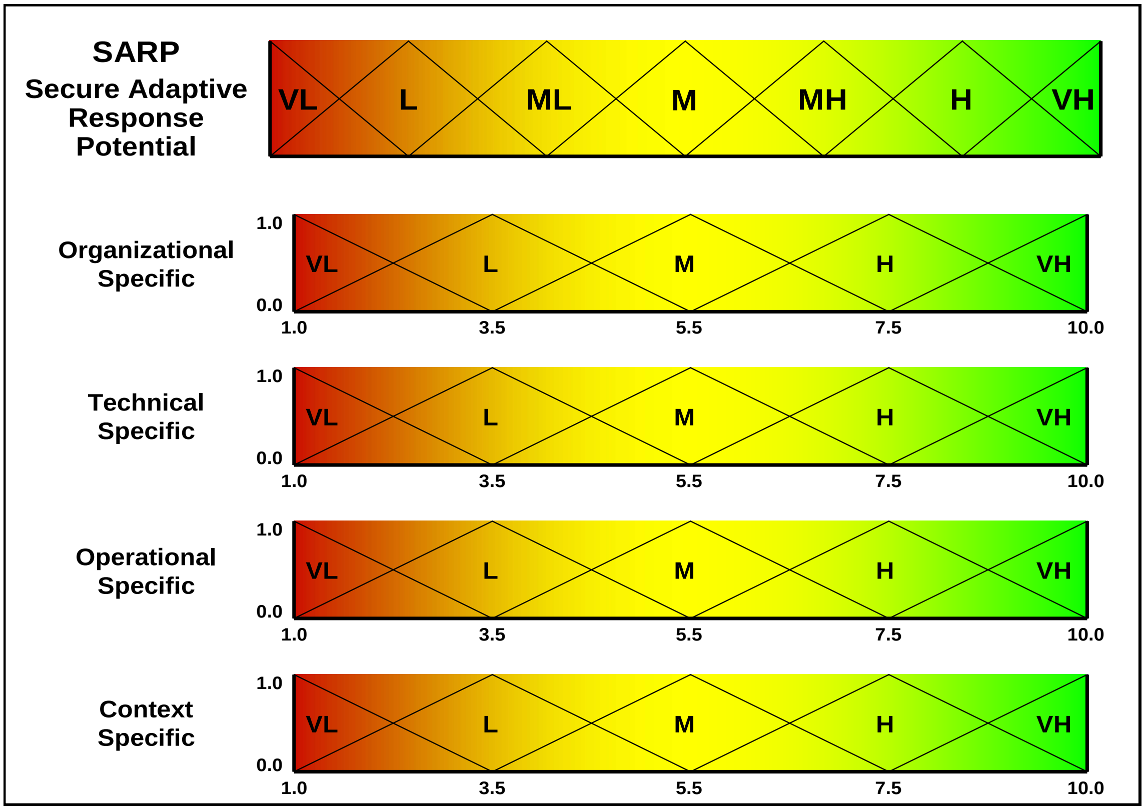


Figure 1. Secure Adaptive Response Potential Structure.

Each of the four component metric values can be determined using a variety of structured analysis and evaluation techniques. Three specific techniques that can be used to develop specific subsidiary metric values are expert judgment and opinion, analytical hierarchical process

(AHP) and the decision metrics matrix process. Each of these techniques will be discussed next in the context of the CCFRAT system model. Figure 2 outlines a generic system example.

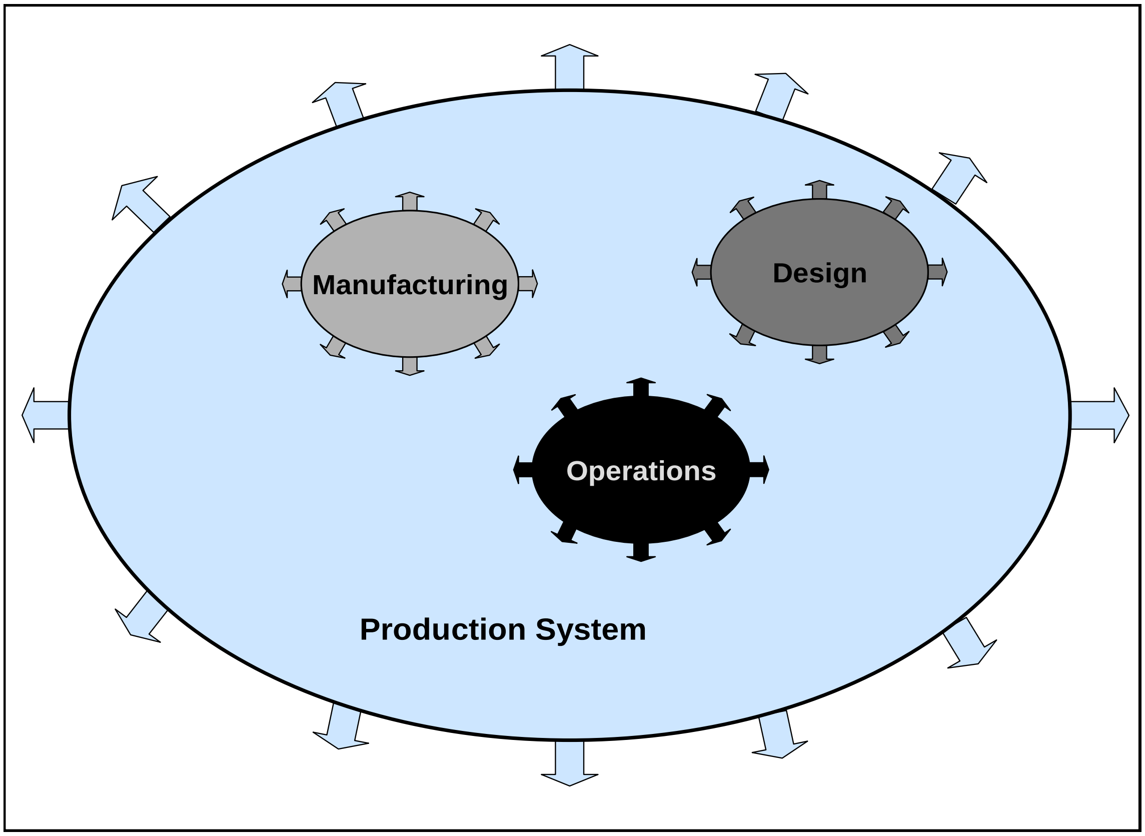


Figure 2. Generic Product Production System.

Given the production system outlined in Figure 2, there are four places where a SARP metric may be used. These four places are the complete production system, the operations subsystem, the manufacturing subsystem and the design subsystem. Each of the SARP component metrics can be evaluated using expert judgment guided by standard system security evaluation frameworks and audit processes. This evaluation approach would be applicable in cases where an organization is operating at a low capability maturity level and/or there is a lack of documented, controlled process and security measurements and metrics. This type of evaluation would point to a low SARP metric value due to the lack of a well-defined, management decision response model as well as the lack of an organized database of system security metrics upon which the SARP metric is evaluated and determined.

The AHP is a well known multi-objective, decision making process. This technique facilitates the organization of decision tasks into a hierarchal form as well as the incorporation of expert evaluation and ranking of all solution alternatives. The formal mathematical operations combined with a well-defined, solution process provides the decision maker with a tool that is more rigorous than structured audits while at the same time using similar input information (Saaty 1980). Figure 3 presents the AHP structure for the first two tiers of the SARP decision hierarchy. Combining the hierarchy from Figure 2 with the hierarchy given in Figure 3 creates a different context for each SARP evaluation.

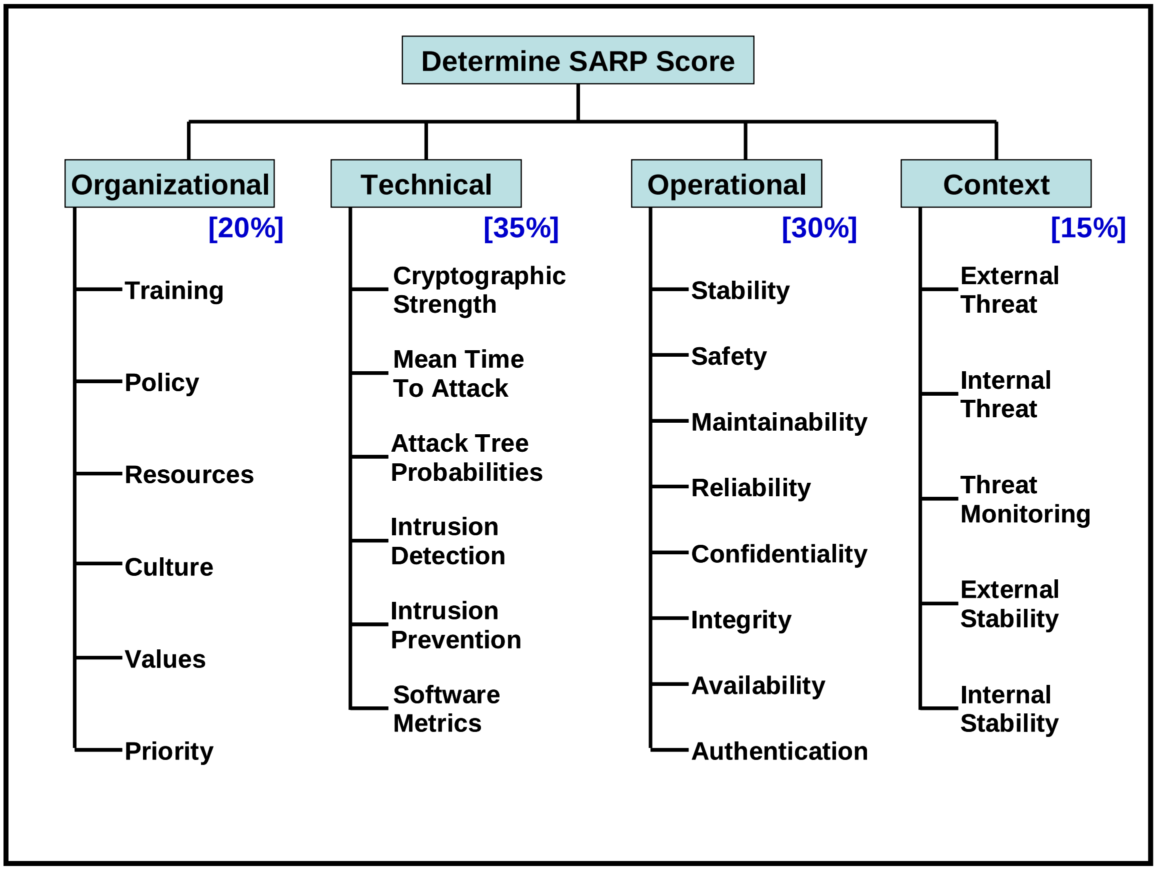


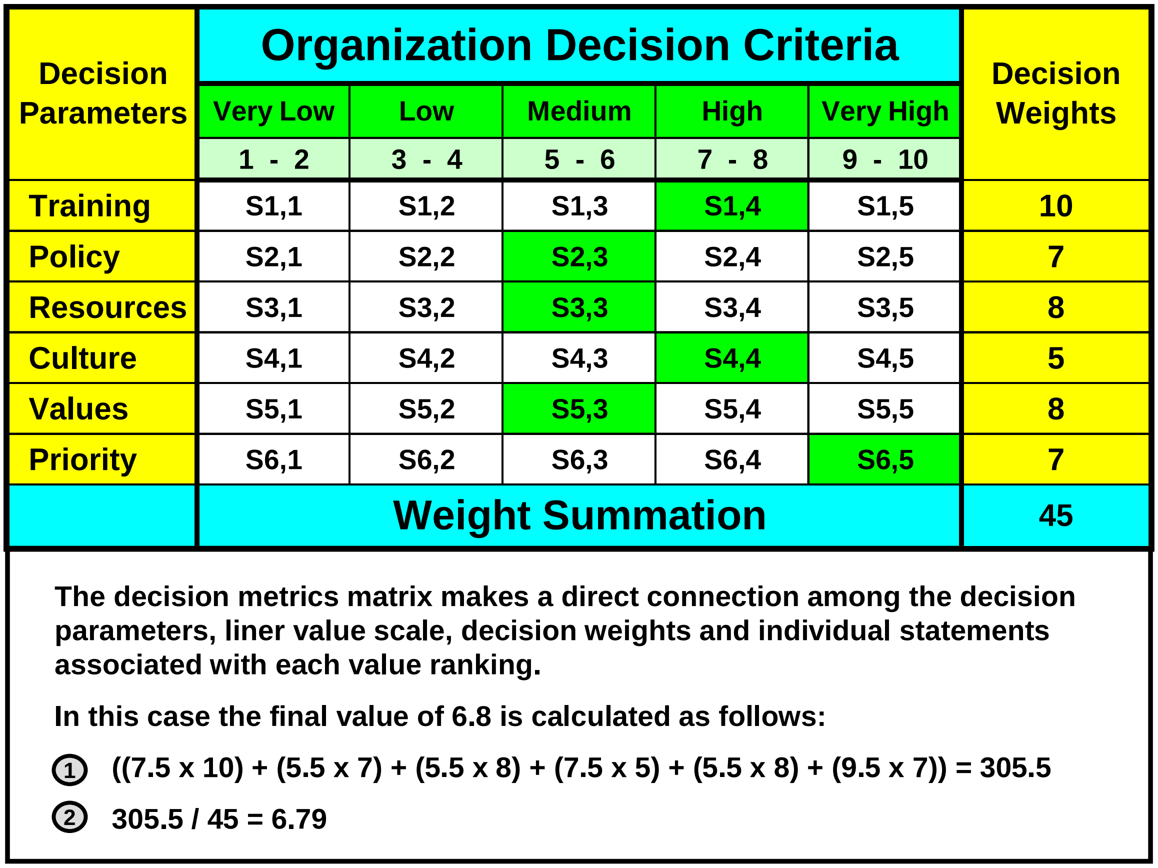
Figure 3. Analytical Hierarchy Process Top Two Tiers.

Expert knowledge and experience can be incorporated into the AHP process and problem specific structure in many ways. Only two methods for AHP knowledge incorporation will be considered in this paper. The first method used to incorporate expert knowledge into the AHP process is the evaluation of the hierarchal structure. Alternative AHP structural hierarchies are prepared for the system security problem space. These alternative structures are then circulated to known security experts for their evaluation. The result from expert evaluation is then used to establish highest-value, hierarchal structure. After the problem space hierarchal structure is established, this structure is again circulated to known security experts for the assignment of relative importance values. The selected hierarchal structure and its associated relative importance values are then used to establish the baseline SARP metric (Fisher 1998).

Metrics Development

Organizational Metric Development. Starting with the baseline SARP metric as the key system security evaluation factor, the necessary security measurements are performed with the measurement data collected and evaluated using the structured AHP and audit techniques developed for the system of interest. The dynamic nature of network-enabled capabilities and network-centric systems require a flexible, management decision structure based on automated or semi-automated system measurements. As more experience is gained and more data is collected in a given system context, standard evaluation techniques can be effectively developed and deployed.

The decision metrics matrix process is a system evaluation technique that can be used to establish and catalog effective system security response mechanisms after sufficient data and experience are generated. [9] Figure 4 provides an example decision metric matrix for the organizational component of the SARP metric.



Decision Parameters	Organization Decision Criteria					Decision Weights
	Very Low	Low	Medium	High	Very High	
	1 - 2	3 - 4	5 - 6	7 - 8	9 - 10	
Training	S1,1	S1,2	S1,3	S1,4	S1,5	10
Policy	S2,1	S2,2	S2,3	S2,4	S2,5	7
Resources	S3,1	S3,2	S3,3	S3,4	S3,5	8
Culture	S4,1	S4,2	S4,3	S4,4	S4,5	5
Values	S5,1	S5,2	S5,3	S5,4	S5,5	8
Priority	S6,1	S6,2	S6,3	S6,4	S6,5	7
	Weight Summation					45

The decision metrics matrix makes a direct connection among the decision parameters, liner value scale, decision weights and individual statements associated with each value ranking.

In this case the final value of 6.8 is calculated as follows:

① ((7.5 x 10) + (5.5 x 7) + (5.5 x 8) + (7.5 x 5) + (5.5 x 8) + (9.5 x 7)) = 305.5

② 305.5 / 45 = 6.79

Figure 4. Organization Decision Metrics Matrix.

A key feature of the decision metrics matrix is the specific encoding of value statements that describe the system state associated with a specific value rating on the linear ranking metric scale. Example statements describing the system organizational state associated with each value on the ranking scale are presented next.

The organizational training states are given as:

S1,1: No organized system or security training is planned or provided.
S1,2: Training is provided on an ad hoc basis.
S1,3: Training is planned, provided and tracked.
S1,4: Real time training is provided to address observed needs
S1,5: Training is optimized using real time feedback and targeted to specific individuals

The organizational policy states are given as:

S2,1: No organized system or security policies are available
S2,2: System and security policies are ad hoc and uncoordinated.
S2,3: System and security polices are established and effectively communicated.
S2,4: System and security polices are updated on a regular schedule.
S2,5: System and security policies are evaluated using real time feedback.

The organizational resource states are given as:

S3,1: No committed resources for system and security operations are provided.
S3,2: System and security resources are committed in an ad hoc basis.
S3,3: System and security resources are planned, budgeted and adequate.
S3,4: System and security resources are continually evaluated and monitored.
S3,5: System and security resources are optimized using real time feedback.

The organizational culture states are given as:

S4,1: No established organizational security culture is present.
S4,2: Ad hoc organizational security culture is used.
S4,3: Established organizational security culture is practiced
S4,4: Security culture is reinforced by all members of the organization.
S4,5: Security is one of the most valued company assets.

The organizational value states are given as:

S5,1: No organizational value is assigned to security operations
S5,2: Limited organizational value is assigned to security operations.
S5,3: Security operations are recognized as adding organizational value.
S5,4: Security operations are used as a key discriminator in new business development.
S5,5: Security operations are optimized to generate optimum business value.

The organizational priority states are:

S6,1: No organizational priority assigned to system and security operations.
S6,2: Ad hoc priority assigned to system and security operations
S6,3: Clear, appropriate priority levels are assigned to system and security.
S6,4: System and security priority levels are monitored and adjusted.
S6,5: System and security priority levels are optimized for highest effect.

These system state descriptions are excellent tools for the organization and communication of expert knowledge and judgment that is associated with the SARP metric. There is a wide range of standard systems engineering tools and techniques available for application to the system security measurement and metrics development activity (Grady 2006).

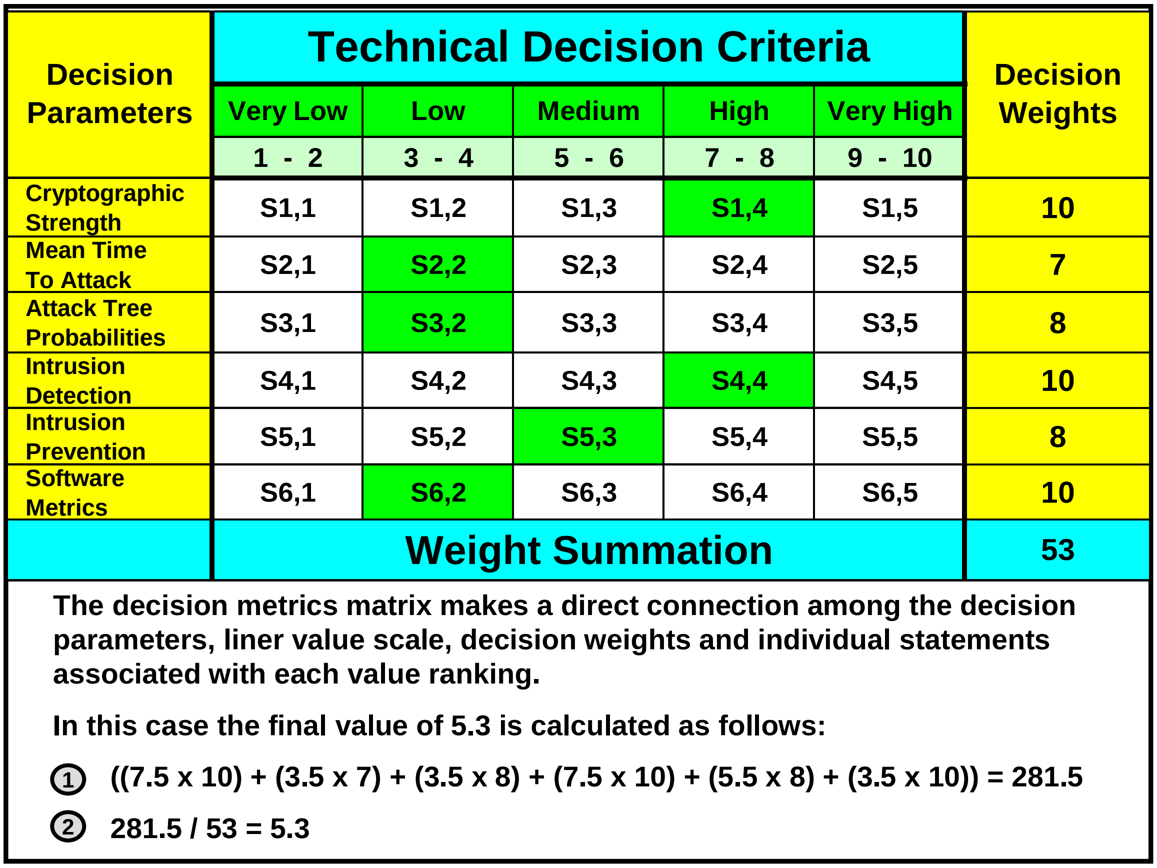
Technical Metric Development. The top-level technical metric components are given as cryptographic strength, mean time-to-attack, attack tree probability, intrusion detection, intrusion prevention and software metrics. For any given specific system these technical metrics would be based on security measurement data collected from the system of interest.

The cryptographic strength metric could be based on an aggregation of system measurements including key length, encryption algorithm type, and encryption application type. These security parameters can be determined by a system evaluation and audit, while expert knowledge can be used to assign a ranking metric value of the collected security measurements (Almerhag 2007).

The mean-time-to-attack metric is closely tied with the attack tree probability security metric. The current system configuration and operational state is surveyed, inventoried and documented. These system configurations are compared to known attack vectors and processes to determine the final metric value.

The intrusion detection and intrusion prevention metrics are based on the system operational records and event logs associated with security event auditing. The specific number of events that would be associated with the metric scale would be developed based on operational experience and expert knowledge.

Software metrics are closely tied to the type of system and the type of software application. In general the system should be designed to focus security relevant software in a few system components that have redundant physical locations and high levels of protection from tampering and other attacks. This value is assigned using expert judgment. The technical metric calculation example is given in Figure 5 with a final technical metric value of 5.3 based on expert knowledge and the matrix process.



Decision Parameters	Technical Decision Criteria					Decision Weights
	Very Low	Low	Medium	High	Very High	
	1 - 2	3 - 4	5 - 6	7 - 8	9 - 10	
Cryptographic Strength	S1,1	S1,2	S1,3	🟩 S1,4	S1,5	10
Mean Time To Attack	S2,1	🟩 S2,2	S2,3	S2,4	S2,5	7
Attack Tree Probabilities	S3,1	🟩 S3,2	S3,3	S3,4	S3,5	8
Intrusion Detection	S4,1	S4,2	S4,3	🟩 S4,4	S4,5	10
Intrusion Prevention	S5,1	S5,2	🟩 S5,3	S5,4	S5,5	8
Software Metrics	S6,1	🟩 S6,2	S6,3	S6,4	S6,5	10
	Weight Summation					53

The decision metrics matrix makes a direct connection among the decision parameters, liner value scale, decision weights and individual statements associated with each value ranking.

In this case the final value of 5.3 is calculated as follows:

① **((7.5 x 10) + (3.5 x 7) + (3.5 x 8) + (7.5 x 10) + (5.5 x 8) + (3.5 x 10)) = 281.5**

② **281.5 / 53 = 5.3**

Figure 5. Technical Decision Metrics Matrix.

Operational Metric Development. The top level operational metric components are given as stability, safety, maintainability, reliability, confidentiality, integrity, availability and authentication. For any given specific system operational mode and configuration, these technical metric values are based on security measurement data collected from the system of interest. These metrics are not independent, and in some areas there may be significant overlap in the application and evaluation of system security operational measurements. However, the base security operational measurements are combined with different logic and security goals to produce each specific operational security metric. Figure 6 details the operational decision metrics matrix.

The stability operational metric is a measure of how fast the operational demands on the system are changing. Systems that have a constant operational task set may be less susceptible to certain types of security attacks but they are also more difficult to change when the security threat demands an operational change. Expert judgment is used to evaluate the system operational modes and states in combination with other security measurement data to arrive at a score for the stability metric.

Decision Parameters	Operational Decision Criteria					Decision Weights
	Very Low	Low	Medium	High	Very High	
	1 - 2	3 - 4	5 - 6	7 - 8	9 - 10	
Stability	S1,1	S1,2	S1,3	S1,4	S1,5	5
Safety	S2,1	S2,2	S2,3	S2,4	S2,5	8
Maintainability	S3,1	S3,2	S3,3	S3,4	S3,5	7
Reliability	S4,1	S4,2	S4,3	S4,4	S4,5	8
Confidentiality	S5,1	S5,2	S5,3	S5,4	S5,5	10
Integrity	S6,1	S6,2	S6,3	S6,4	S6,5	10
Availability	S7,1	S7,2	S7,3	S7,4	S7,5	10
Authentication	S8,1	S8,2	S8,3	S8,4	S8,5	7
	Weight Summation					65

The decision metrics matrix makes a direct connection among the decision parameters, liner value scale, decision weights and individual statements associated with each value ranking.

In this case the final value of 5.2 is calculated as follows:

① ((3.5 x 5) + (5.5 x 8) + (3.5 x 7) + (3.5 x 8) + (5.5 x 10) + (7.5 x 10) + (5.5 x 10) + (5.5 x 7)) = 337.5

② 337 / 65 = 5.2

Figure 6. Operational Decision Metrics Matrix.

The safety operational metric is closely associated with the stability, reliability and maintainability security metrics. Expert knowledge from both safety experts and security experts need to be combined to properly evaluate and rank the safety metric. Similar to the safety metric, the maintainability and reliability metrics must be evaluated in terms of the complete system operational task set. Historical data, operational measurements and expert knowledge is used with standard evaluation approaches to calculate the final maintainability and reliability metrics.

The confidentiality, integrity and availability metrics are the subject of many evaluation procedures and audit checklists. Depending on the system task and role these metrics can have a wide range of values. Therefore, the value of these metrics is very sensitive to the system operational tasks, goals and roles. Expert security knowledge is required to properly generate the values for these metrics. The authentication system security metric is closely tied to the system mode, state and operational role. Operational data combined with expert system security knowledge is required to properly evaluate this metric.

Context Metric Development. The top level system context metric components are given as external threat, internal threat, threat monitoring, external stability, and internal stability. For any given specific system these system context metrics are based on security measurement data collected from the system of interest and the environmental context that encompasses the system of interest. As with some of the other metrics presented in this paper, these metrics are not independent. The specific security goals and requirements under evaluation will impact the determination of the system context metric. . Figure 7 details the context decision metrics matrix.

Decision Parameters	Context Decision Criteria					Decision Weights
	Very Low	Low	Medium	High	Very High	
	1 - 2	3 - 4	5 - 6	7 - 8	9 - 10	
External Threat	S1,1	S1,2	S1,3	S1,4	S1,5	10
Internal Threat	S2,1	S2,2	S2,3	S2,4	S2,5	8
Threat Monitoring	S3,1	S3,2	S3,3	S3,4	S3,5	6
External Stability	S4,1	S4,2	S4,3	S4,4	S4,5	7
Internal Stability	S5,1	S5,2	S5,3	S5,4	S5,5	9
	Weight Summation					40

The decision metrics matrix makes a direct connection among the decision parameters, liner value scale, decision weights and individual statements associated with each value ranking.

In this case the final value of 6.8 is calculated as follows:

① **((3.5 x 10) + (7.5 x 8) + (5.5 x 6) + (3.5 x 7) + (5.5 x 9)) = 202**

② **202 / 40 = 5.0**

Figure 7. Context Decision Metrics Matrix.

The external threat metric is based on security measurements that are taken across the external environment. Specific focus areas in the external environment are selected as required by the system operation roles and tasks. The internal threat metric is based on information value and process access. Expert knowledge and judgment is required to properly assign values to both the external and internal threat metrics.

The threat monitoring metric is based on the systems capability to monitor, log and report security events of interest. The external stability and internal stability metrics are used to analyze and evaluate the rate of organizational, technical and process change occurring in the system environment. The higher the rate of system and process change the greater the opportunity for a security event to occur.

Determination of the SARP Value

The SARP is a multifaceted system security metric designed to operate over a wide range of system states and environments. The numerical foundation of the SARP metric is based on fuzzy numbers which allow the ranking and quantification of natural language statements as well as the production of crisp numerical values using transformation techniques. The AHP, as well as the decision metrics matrix, has been used in this paper to provide structure to the evaluation and analysis process.

Using the hierarchy given in Figure 3, expert knowledge and judgment was used to assign weights to the four SARP subcomponents. This assignment was:

- Organizational, 20 percent
- Technical, 35 percent
- Operational, 30 percent
- Context, 15 percent.

The subcomponents now have two metric values, one weighted and one un-weighted. These subcomponent scores are:

Subcomponent	Un-weighted	Weighted
Organizational	6.8	5.0
Technical	5.3	3.9
Operational	5.2	3.3
Context	5.0	6.6

The un-weighted value is used to determine the total SARP score which is rated as medium. This relative score may be good or bad depending on the system that was evaluated. The weighted score is used to determine what specific areas should be addressed first when the organization starts to improve their system security capability. Using the weighted score, the technical and operational areas had the lowest values; therefore they should be evaluated and given the resources to improve the scores.

In the technical area a quick review of the metric matrix shows that the software metric, mean-time-to-attack and attack probabilities areas need the greatest improvement. In the operational area the stability, reliability and maintainability areas are the ones that need the greatest improvement.

Summary and Conclusions

Three basic techniques from classical systems engineering have been applied to the development of system security metrics. These techniques are capability maturity model audits, analytic hierarchy process, and structured system analysis using the CCFRAT system model. The proper application of these techniques facilitates management decisions associated with the sequential development of highly-secure, adaptive system security responses. An adaptive security response is necessary to counteract a system threat environment that is constantly changing and adapting.

References

Almerhag, I. A., and Woodard M. E., "Quality of Service Routing Metrics on Selected Aspects of Network Security," April 22nd, 2007. http://www.comp.brad.ac.uk/het-net/HET-NETs05/ReadCamera05/WP05.pdf .

Coallier, Francois, "International Standardization in Systems Engineering," INCOSE Insight, Vol. 10, Issue 2, April 2007, p 7-8.

Fisher, Gerard H., "An Application of the Analytic Hierarchy Process to System Engineering and Project Management," Proceedings of the Eight Annual International Symposium of the International Council on Systems Engineering, (Vancouver, BC, 1998)

Grady, Jeffrey, O., *System Requirements Analysis*. Elsevier, New York, 2006.

Helm, James C., "Decision Metrics Matrix Process," Proceedings of the Twelfth Annual

International Symposium of the International Council on Systems Engineering, (Las Vegas, Nevada, 2002)

Ibrahim, Linda, “Harmonization of Safety and Security Standards,” INCOSE Insight, Vol. 10, Issue 2, April 2007, p 37-39.

Jones, James, H., “Developing a Single Performance Indicator from Hierarchical Metrics,” Proceedings of the Fifth Annual International Symposium of the International Council on Systems Engineering, St. Louis MO, 1995.

Kanava, Jorma and Savola, Reijo, “Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes,” May 2, 2007. http://iplu.vtt.fi/workshop-06.html .

Saaty, Thomas L., *The Analytic Hierarchy Process*. McGraw-Hill, New York, 1980.

Schneier, Bruce, “Do We Really Need a Security Industry?” April 26, 2007. http://www.wired.com/politics/security/commentary/securitymatters/2007/05/securitymatters_0503 .

Simpson, J., Dagli C., Miller A., Grasman S., “A Generic, Adaptive Systems Engineering Information Model”, Proceedings of the 15th Annual International Symposium of the International Council on Systems Engineering, Rochester, NY, July, 2005.

Biography

Joseph J. Simpson’s interests are centered in the area of complex systems including system description, design, control and management. Joseph has professional experience in several domain areas including environmental restoration, commercial aerospace and information systems In the aerospace domain, Joseph has participated in a number of system development activities including; satellite based IP network design and deployment, real-time synchronous computing network test and evaluation, as well as future combat systems communications network design. Joseph Simpson has a BSCE and MSCE from the University of Washington, an MSSE from the Missouri University of Science and Technology, is a member of INCOSE, IEEE, and ACM. Currently Joseph is enrolled in a system engineering doctorate program at the Missouri University of Science and Technology.

Dr. Ann Miller is the Cynthia Tang Missouri Distinguished Professor of Computer Engineering at the Missouri University of Science and Technology. Previously, she was the Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computing, Intelligence, Electronic Warfare, and Space for the U. S. Department of the Navy. For a portion of that time, she had additional responsibilities as Department of the Navy Chief Information Officer (CIO). She also served as Director for Information Technologies, Department of Defense Research and Engineering. Prior to that, Dr. Miller served for over 12 years with Motorola, Inc. where she held a variety of technical and managerial positions. She holds one U. S. patent in satellite communications, has co-authored three books on the programming language Pascal, and is the author of more than five dozen journal articles and monographs. Dr. Miller chairs the NATO Information Systems Technology Panel and is a Senior Member of IEEE. Dr. Miller’s research areas include reliability and security of computer-based systems, with an emphasis on networked large-scale systems.

Dr. Cihan H Dagli is a Professor of Engineering Management and Systems Engineering and director of the System Engineering graduate program at the Missouri University of Science and Technology. He received BS and MS degrees in Industrial Engineering from Middle East Technical University and a Ph.D. from the School of Manufacturing and Mechanical

Engineering at the University of Birmingham, United Kingdom, where from 1976 to 1979 he was a British Council Fellow. His research interests are in the areas of Systems Architecting, Systems Engineering, and Smart Engineering Systems Design through the use of Artificial Neural Networks, Fuzzy Logic, and Evolutionary Programming. He is the founder of the Artificial Neural Networks in Engineering (ANNIE) conference being held in St. Louis, Missouri since 1991. He provided the conduit to the dissemination of neural networks applications in engineering and decision making through these conferences for the last fourteen years. He is the Area editor for Intelligent Systems of the International Journal of General Systems, published by Taylor and Francis, and Informa Inc.