Metrics and Measurement of Trustworthy Systems

Jin-Hee Cho
US Army Research Laboratory
Adelphi, MD
Email: jinhee.cho@us.army.mil

Patrick M. Hurley
US Air Force Research Laboratory
Rome, NY
Email: patrick.hurley.4@us.af.mil

Shouhuai Xu
University of Texas at San Antonio
San Antonio, TX
Email: shxu@cs.utsa.edu

***Abstract*—Accurate measurement of the quality of systems is crucial to building trustworthy systems. Such a measurement indicates whether a system is working properly and meeting its requirements. Although security and dependability metrics are regarded as key metrics for measuring the quality of systems, they are not sufficient for measuring the quality of systems that are placed in a multi-domain environment including hardware, software, network, human factors, and physical environments. In order to embrace multidimensional aspects of the quality of a system, we introduce a trustworthiness metric framework that supports three key submetrics of trust, resilience, and agility, and propose an ontology-based framework with three corresponding sub-ontologies. We also discuss how the key metrics are related to the severity of threats and the quality of assessment tools. This work is part of the cyber defense effort conducted by the Trustworthy Systems Working Group (TSWG) under the Cyber Strategic Challenge Group (CSCG) of The Technical Cooperation Program (TTCP), which is an international cooperation organization for enhancing defense science and technology.**

***Index Terms*—metrics, measurement, trustworthy systems, trustworthiness, agility, resilience, threat, vulnerability**

I. Introduction

Accurate measurement of the quality of systems and development of metrics are crucial to building trustworthy systems. Such a measurement is an objective indicator representing the trustworthiness of a system's ability to meet its requirements. Although security and dependability metrics have been previously discussed as system metrics [1, 2, 3], they cannot adequately accommodate the multidimensional aspects of systems, especially for computer-based systems with human-machine interactions. To address this shortfall, we undertake measuring a system's trustworthiness. Up to now, our understanding of trustworthiness is in its embryonic stage.

Under the Cyber Strategic Challenge Group (CSCG) of The Technical Cooperation Program (TTCP)[1], the *Trustworthy Systems Working Group* (TSWG) was formed in 2014 with the following four key activities to share and conduct collaborative research: (1) vulnerability assessment, (2) red teaming, (3) building mixed levels of trust systems, and (4) development of metrics and measurement of trustworthy systems. Through sharing and exchanging defense research and technology of each member nation and conducting collaborative research, TSGW aims to build a cyber-hardened system which is highly trustable, resilient and agile under high dynamics of system and threat conditions. In this paper, the members in the TSWG aim to develop metrics for measuring the multidimensional quality of systems.

In order to embrace a more comprehensive set of aspects of the quality of a system, the so called *trustworthiness of a system*, we propose a metric framework called `TRAM` (Trust, Resilience, and Agility Metrics). We choose the three key metrics in support of the mission of the TSWG. The present work makes the following contributions:

- `TRAM` leverages ontology methodologies, such as Protégé [5], to create a generic metric framework that describes the hierarchical structure of metrics to measure trustworthiness of a system and represents the relationships between them.
- We augment `TRAM` to measure the quality of a system embracing both security and performance of: hardware; software; the network; the effect of human factors (i.e., users or system designers / analysts); and physical environments.
- We offer insights for understanding the relationships between assessment tools, such as red teaming and vulnerability assessment, and metric attributes. We consider how the interplay between assessment tools can affect the trustworthiness of a system.
- We choose the key metrics of `TRAM` in order to support the goal of the TSWG, building cyber-hardened trustworthy systems that ensure trust, resilience, and agility of systems.

The rest of this paper is organized as follows. Section II discusses the existing metrics, measurements, and metric ontologies. Section III discusses the key components for measuring trustworthiness. Section IV describes the proposed ontology-based metric framework, namely `TRAM`. Section IV discusses how the attributes of trust, resilience, and agility are related to each other. Section V concludes the paper and discusses future research directions.

II. Background and Related Work

A. Metrics and Measurement of Quality of a System

"To measure" means assigning an element of a scale (e.g., number scale, nominal scale, ordinals scale) to an object for quantifying an attribute of the object [6]. A measurement is

[1] TTCP is an international organization aiming to collaborate and exchange defense scientific and technical research and information, harmonize and align defense research programs by sharing or exchanging research activities between the five nations, Australia, Canada, United Kingdom, United States, and New Zealand [4].

related to attributes of a system, and there could be many different attributes of a system that are measurable. Therefore, an abstraction is used to cover such forms of measurable attributes.

As a closely related term, a “metric” is used to indicate “a precisely defined method which is used to associate an element of an (ordered) set V to a system S” [6]. Avižienis *et al.* [2] discuss how metrics (or measurements) can be valid with the following criteria: (1) *objectivity* based on certainty, (2) *efficiency* based on quantification, and (3) *control* based on feedback or means of controlling decisions. Slayton *et al.* [7] observe that metrics lead to ‘learning’ for improvement.

To measure the quality of a system, many attributes have been discussed in the literature. Avižienis *et al.* [2] claim that the fundamental attributes of metrics reflecting the quality of a system are functionality, performance, dependability, coupled with security, and cost. “Usability, manageability, and adaptability” are discussed as the factors affecting dependability and security. Moreover, they discuss security to consider availability, integrity, and confidentiality, and use dependability to embrace reliability, availability, integrity, safety, and maintainability. Hasselbring and Reussner [8] define the key attributes of software trustworthiness in terms of correctness, safety, quality of service (i.e., availability, reliability, performance), security (i.e., availability, integrity, confidentiality), and privacy. Trustworthiness has been explored in socio-technical systems [9] and cyber sensing [10]. There have been some studies on using provenance to evaluate trustworthy information sharing [11, 12, 13].

However, the studies mentioned above [2, 8, 9, 10, 11, 12, 13] do not address: (1) how each attribute is related to other attributes; (2) how an attribute’s meaning overlaps with that of the other attributes’; (3) how attributes are hierarchically structured with a full-fledged granularity of sub-attributes representing the quality of multidimensional system domains.

B. Metric Ontologies

An ontology is “a formal specification of a *shared* conceptualization” [14]. Guarino [15] elaborates the term ‘conceptualization’ as “a language-independent view of the world, a set of conceptual relations defined on a domain space.” An ontology can be seen as a language-dependent cognitive artifact committed to *a certain* conceptualization of the world [15].

There have been efforts to develop metric ontologies. Paul *et al.* [16] develop an ontology-based assessment framework of trustworthiness including dependability and other attributes. The framework provides automated assessment of trustworthiness for individual system entities and integrates them into an overall integrated system. Ontology-based definitions and models of trust have been studied in various domains [17]. Chang *et al.* [18] propose generic trust ontologies comprising three components in service-oriented network environments: agent trust, service trust, and product trust. Dokoohaki and Matskin [19] propose a trust ontology to improve the semantics of trust network structure of social institutions and ecosystems on Semantic Web. Valacheas *et al.* [20] develop a resilience ontology with several subontologies such as a domain ontology, a threats ontology, a threat agent ontology, a means ontology, and a metrics ontology. The metrics ontology proposed in [2], including the attributes of dependability and security (i.e., availability, integrity, confidentiality, safety, reliability, maintainability), represents the relationship between metrics and resilience

III. Key Components of Trustworthiness

The key components to measure trustworthiness of systems include: (1) a system of concern and its features, states and behavior; (2) threats, including faults, errors, and failures caused by deliberate actions (i.e., attacks) or non-deliberate actions; (3) key metrics of trustworthiness; (4) means to build trustworthy systems; (5) relationships between assessment (e.g., red teaming, vulnerability assessment, penetration testing) and submetrics (or attributes) of a trustworthiness metric.

A. Scope of Systems

In this paper, a ‘system’ refers to a set of interacting entities in the context of computing and communication [2]. A system can be composed of multiple components, including hardware, software, network, human factors, physical environments, and the effect of the components’ behavior on the system’s overall behavior (i.e., a *service*) [2]. Quality of Service (QoS) is affected by threats against the system, including errors, faults, and failures as we elaborate below.

B. Threats

The dictionary definition of *threat* [28] is (1) “someone or something that could cause trouble, harm, etc.”; and (2) “the possibility that something bad or harmful could happen.” Threat against a system refers to anything that can or may bring harmful effects to the state of the system and lead to improper service states (e.g., erroneous behavior, unavailable service, system shutdown due to a critical failure).

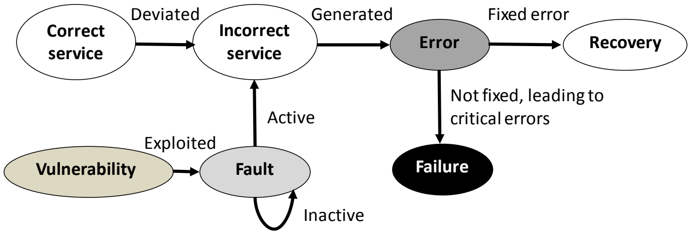

Fig. 1: Relationships between service, threats (fault, error, failure), vulnerability, and recovery of a system [2].

As highlighted in Fig. 1, Avizienis *et al.* [2] classify threats according to the assumption that an active *fault* introduces incorrect service, which generates system *error(s)*. If the error is not detected and treated with a proper response, it will cause a system *failure*. This means that any vulnerability that can lead to a fault or error can be considered as a threat. Thus, a threat includes not only an actual harm but also the

Main attributes of trustworthiness	Equivalent or sub-attribute(s) to the main attributes	Trust [1, 2, 21, 22]	Resilience [23, 24]	Agility [25, 26, 27]
reliability	an attribute of dependability; predictability; competence; consistency; stability; certainty; fault-forecasting; high-confidence; assurance; survivability	✓	✓	✓
availability	an attribute of dependability; an attribute of security	✓	✓	✓
safety	an attribute of dependability	✓	✓	
confidentiality	an attribute of security	✓		
integrity	an attribute of security; accuracy; credibility	✓		
robustness	fault-tolerance; performability; accountability; authenticity; nonrepudiability	✓	✓	✓
maintainability	recoverability; retainability; correctability; self-healing; self-repair		✓	
adaptability	autonomy; learning; extensibility; reconfigurability		✓	✓
usability	automatability; flexibility; learnability; satisfaction; compatibility; reusability; complexity			✓
timeliness	quickness; decisiveness			✓
leanness	efficiency; simplicity; scalability			✓
reactiveness	readiness; fault-removal		✓	✓
proactiveness	preparedness; fault-prevention			✓

TABLE I: Main attributes of trustworthiness in terms of trust, resilience, and agility.

potential of any harm that may cause a system failure. When a system vulnerability is exposed by unexpected operations or misconduct of users (or system operators) or is exploited by inside or outside attackers, it leads to a fault and an active fault can trigger an incorrect service. If the incorrect service is not fixed, an error is generated. If the error is critical but not fixed, it causes a system failure [2].

C. Key Metrics

As reviewed in Section II-A, security and dependability have been considered as key system metrics. However, the metrics defined in the literature do not address human factors, including subjective opinions such as trust. Moreover, the existing metrics do not explore attributes such as *agility*, which is important for modern computing and communication systems that are highly dynamic in multi-genre domains dealing with information, communication, and/or social-cognitive technologies. Trustworthiness is defined as "the assurance that the system will perform as expected" [29]. The notion includes the attributes [2] [2], where Avizienis *et al.* [2] define dependability as the same meaning of trustworthiness, assurance, high confidence, or survivability. Trustworthiness is distinguished from trust in that trustworthiness is represented as an objective aspect of trust estimated based on evidences or observations; whereas trust includes subjective aspects of a cognitive entity's opinion such as a human [21]. In this work, we propose a *trustworthiness metrics framework* based on the following submetrics:

1) Trust: Trust has been defined with many different meanings; its concept with multidimensional characteristics are well summarized as "the willingness to take risk based on a subjective belief that a trustee (evaluatee) will exhibit reliable behavior to maximize a trustor's (evaluator's) interest under uncertainty (or ignorance) of a given situation based on the cognitive assessment of past experience with the trustee" [21]. Trust is often defined in our everyday lives by a situation that a trustor trusts a trustee by accepting any vulnerability the trustee introduces. Similarly, trust between systems is defined as the *accepted dependence* where system A's dependability relies on system B's dependability [2].

2) Resilience: It means "the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks" [23]. Resilience has been considered as a synonym for fault-tolerance, which can be a means for achieving system security and dependability [2].

3) Agility: It is defined as "the ability of an entity to be effective in the face of a dynamic situation, unexpected circumstances, or sustaining damage" by emphasizing "the synergistic combination of robustness, resilience, responsiveness, flexibility, innovation, and adaptation" [26]. Agility also means the continual readiness of an entity to respond rapidly, accurately, proactively, and economically by providing high QoS [27]. An agile system is highly proactive, responsive, and recoverable quickly to sudden threats or errors introduced to the system. Note that agility is not orthogonal to resilience. We discuss the overlapping aspects of agility and resilience in the `TRAM` ontology framework presented in Fig. 2.

Table I summarizes the main attributes of trustworthiness in terms of trust, resilience, and agility. It shows that *reliability*, *availability* and *robustness* are common attributes of the submetrics of trust, resilience, and agility. We note that security attributes (i.e., availability, confidentiality, and integrity) are considered as dimensions of trust, meaning that *trust* is more than security encompassing both dimensions of security and performance of a system. *Resilience* is often considered the same as recoverability or maintenability (including fault-tolerance), and that some dimensions of *agility* are different from those of trust and resilience because agility focuses on measuring how quickly and adaptively a system is functioning under sudden changes or attacks, requiring a learning capability under high dynamics. Notice that agility and resilience have many common attributes as described in Table I.

[2] In this paper, we use a 'metric' to mean a goal to achieve while an 'attribute' is used to indicate a 'submetric' or 'objectives' to achieve an upper level metric or goal. For example, while 'security' can be called as a metric, 'confidentiality, integrity, and availability' are called 'attributes' to achieve security. Although trust, resilience, and agility can be called as metrics (or submetrics), they can be called as attributes to measure trustworthiness.

D. Means to Trustworthiness

The question of "how to achieve trustworthiness" is closely related to finding the answer for what makes systems trustworthy. Avizienis *et al.* [2] discuss the means to security and dependability in terms of fault prevention, fault tolerance, fault removal, and fault forecasting. Although they are useful for building secure and dependable systems, it is not clear how they are associated with the quality of procedures / tools for assessing the quality of systems. The quality of assessment, testing, or verification (e.g., vulnerability / risk assessment or red teaming / penetration testing) significantly affects the level of uncertainty [30]. This is an important matter because uncertainty from unknown attacks, unknown vulnerabilities or unknown risk can often hinder proper actions to prevent, tolerate, remove, or forecast faults, which are the main causes of errors or failures of a system.

E. Relationships between Assessment and Metrics

Now we discuss how the key attributes of trustworthiness, namely trust, resilience and agility, are related to the degree of threat, uncertainty, asset importance, and risk appetite (e.g. risk-seeking, risk-neutral, risk-averse). The severity of threats can enhance the effectiveness of red teaming exercises, by tailoring their design and implementation to test a system's resilience against attacks or faults. The type of threats considered significantly affects the level of assessed trustworthiness because it determines the degree of difficulty of mission completion in a highly dynamic, hostile environment.

Red teaming (RT) is an assessment process for identifying vulnerabilities or weaknesses in various aspects of a system, aiming to improve the quality of a system throughout its development process and even during its use [31]. *Vulnerability assessment* (VA) refers to the process for examining a system to identify its weaknesses and loopholes that may open back-doors for adversarial entities to perform attacks [32]. *Penetration testing* (PT) is an evaluation / verification process that tests various features of operations / functionalities of a system for finding vulnerabilities exploitable by attackers. PT is sometimes interchangeably used with VA. Although PT and VA overlap in identifying vulnerabilities, PT is a more specific, goal-oriented testing process, whereas VA provides a list of vulnerabilities of a system as well as their priorities to be fixed. Unlike VA, PT has a clear goal of determining the exploitability of identified vulnerabilities based on the already performed VA (e.g., an unauthorized user tries to gain access to a system by penetrating system security and defense mechanisms) [32]. On the other hand, RT is more than PT because RT is designed to enhance security by identifying vulnerabilities and improving defense strategies (e.g., countermeasures against attacks or prevention mechanisms for vulnerabilities) [31].

Fig. 2 is a Petri Net representation of the relationships between the aforementioned trustworthiness attributes, threat, vulnerability, risk assessment, and any other system features including asset importance and risk appetite, where an *oval* represents a state of a system and a *bar* indicates a transition of a system changing from one state (one oval) to another state (another oval). We highlight how each transition can be realized via metrics, threat, and other system features. The quality of assessment tools, such as RT, PT, and VA, can significantly reduce the number of unknown attacks or vulnerabilities (i.e., uncertainty). Accordingly, the quality of assessment impacts the validity of the measurements and metrics that help provide an objective standard for judging the quality of a system. Note that the colored ovals (i.e., perceived risk, vulnerability, and impact of failure) indicate the key factors to be considered in the process of risk assessment.

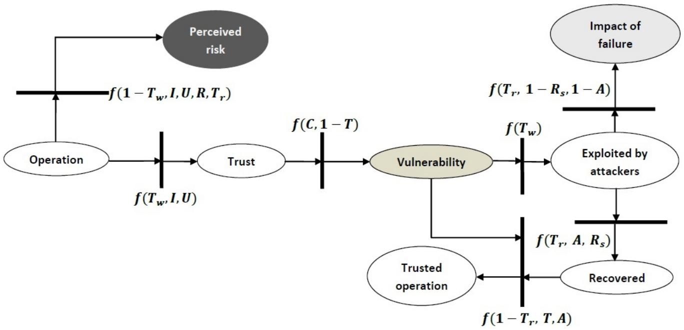

Fig. 2: A Petri Net representation of the relationships between metric attributes, assessments, and threats. T_w refers to trustworthiness of a system with $T_w = (T_r, T, R_s, A)$ where T_r is the degree of threat, T is perceived trust, R_s is resilience, and A is agility of the system. Uncertainty, U, is derived from unknown vulnerabilities / attacks. I indicates importance of an asset and R refers to risk appetite for a given system. Each metric or measurement x is scaled in $[0, 1]$ where $1 - x$ indicates its complement.

IV. Ontology-based TRAM Framework

For the TTCP project, we plan to develop ontologies for red teaming, vulnerability assessment, metric criteria, and trustworthiness metric framework. Due to the space constraint, this paper focuses on the `TRAM` ontology of trustworthiness metrics including trust, resilience, and agility metrics. We will report the comprehensive framework in the extended version of the present work for a future journal submission. Fig. 3 describes the current version of the `TRAM` framework using an ontology tool, Protégé [5]. The current `TRAM` framework only considered well-known attributes of trustworthiness. One ongoing research is to make it as comprehensive as possible.

The *trust ontology* focuses on measuring the security and performance aspects of a system as well as the predictability such as 'data predictability' derived from objective evidences and 'human judgment' based on subjective opinions (e.g., users, system analysts, or administrators).

The *resilience ontology* focuses on fault-tolerance, recoverability, and reconfigurability. Fault-tolerance measures the maximum degree of resistance against system errors, insider attacks, or outsider attacks. Recoverability indicates whether

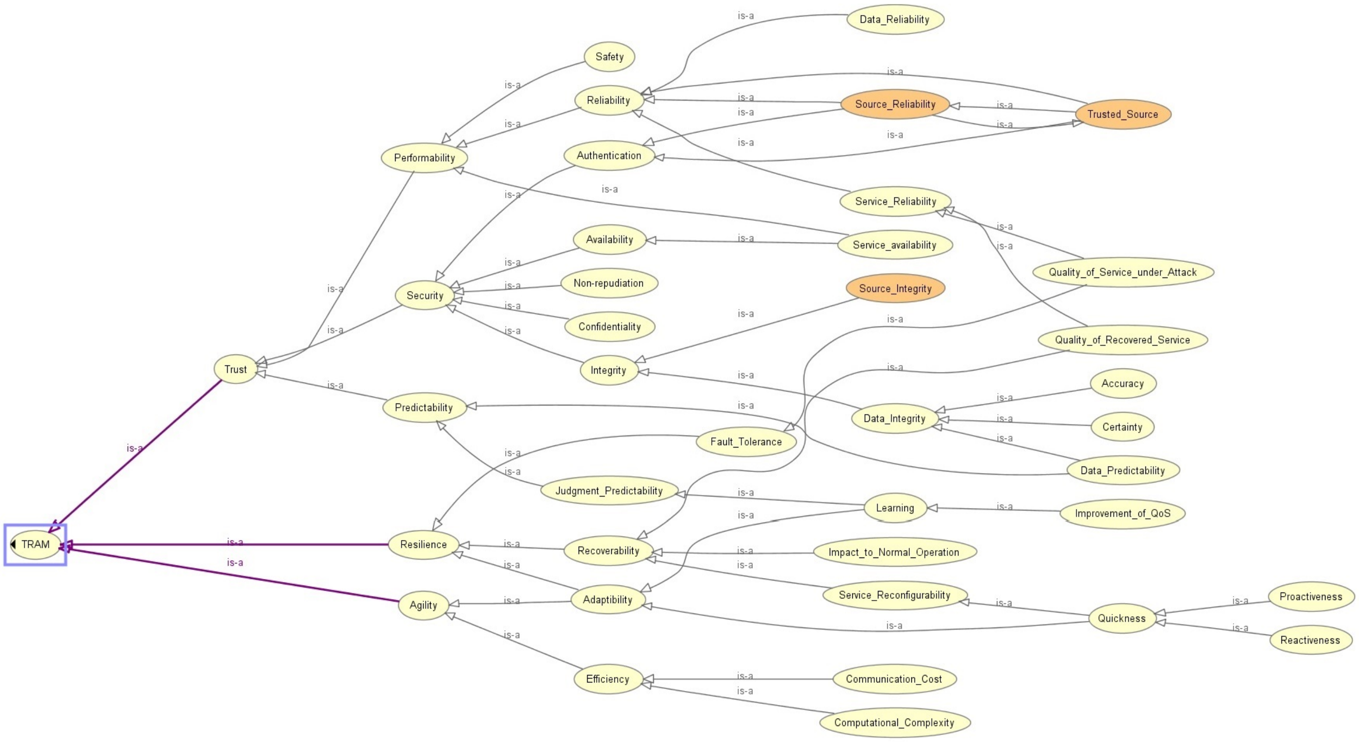

Fig. 3: Ontology-based TRAM framework: an attribute B points to an attribute A, it means that A is a superclass of B implying B is part of A expressed by the 'is-a' relationship. Items colored by orange represent equivalent attributes; i.e., Source_Reliability, Trusted_Source, and Source_Integrity are considered equivalent to each other.

a system or service is repairable (e.g., by restoring original services), and measures the quality of the restored service. Reconfigurability provides the original service requested in highly dynamic environments and hostile conditions when normal operations are interrupted. Note that reconfigurability is closely related to the adaptability aspect of agility as shown in Fig. 3.

The *agility ontology* focuses on timely service(s) with a simple solution as required by a user, emphasizing adaptability, efficiency, and usability. Adaptability is related to how quickly a requested service is provided under sudden changes based on timely response and a high learning capability. Efficiency indicates how effective the system can provide a requested service under unexpected changes or attacks by consuming minimum resource, implying cost-effectiveness. Usability is related to how easily a user can contribute to receiving a requested service or restoring the service.

V. Conclusion

We have examined metrics for measuring the quality of trustworthy systems in terms of: (1) the key metrics consisting of trustworthiness in terms of trust, resilience, and agility, which go beyond traditional metrics of security and dependability; (2) the identified key aspects of a vulnerability and its resulting faults, errors, and failures; (3) the relationships between the key metrics, threats, vulnerability, and risk; (4) an ontology-based trustworthiness metric framework called TRAM. Developing a generic metric framework to measure the quality of a system is highly valuable because it can offer an objective indicator to provide a certain level of confidence towards a developed system based on a comprehensive and critical set of metrics based on high consensus in the research community of metrics development.

Our future research plan includes the following: (1) developing ontologies of red teaming and vulnerability assessment and investigating their relationship to TRAM; (2) defining the types of evidences that can be used to evaluate the trustworthiness of systems and designing methods for aggregating evidences (e.g., an *evidence aggregation engine* based on belief models or machine learning); (3) considering multi-objective optimization techniques to obtain an overall score of metric attributes in the TRAM framework.

Acknowledgement

We thank other TTCP TSWG members, Trevor Benjamin (Dstl, UK), Chris North (DSTO, Australia), and Brad Hopkins (DSTO, Australia) for their precious comments to enhance the quality of this paper. This research was in part supported by the Department of Defense (DoD) through the office of the Assistant Secretary of Defense for Research and Engineering (ASD (R&E)) and ARO Grant #W911NF-13-1-0141. The views and opinions of the author(s) do not reflect those of the DoD, ASD (R&E), or Army.

References

[1] D. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation: From dependability to security," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 48–65, Jan.–Mar. 2004.

[2] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 11–33, Jan–Mar. 2004.

[3] M. Pendleton, R. Garcia-Lebron, J.-H. Cho, and S. Xu, "A survey on security metrics," *manuscript*, 2016.

[4] TTCP, "The technical cooperation program," 2014. http://www.acq.osd.mil/ttcp/index.html.

[5] Stanford Center for Biomedical Informatics Research, "Webprotégé," 2015. http://protege.stanford.edu/.

[6] R. Böhme and F. C. Freiling, *Dependability Metrics*, vol. 4909, ch. On Metrics and Measurements, pp. 7–13. Springer-Verlag Lecture Notes in Computer Science, 2008.

[7] R. Slayton, "Measuring risk: Computer security metrics, automation, and learning," *IEEE Annals of the History of Computing*, vol. 37, pp. 32–45, April-June 2015.

[8] W. Hasselbring and R. Reussner, "Toward trustworthy software systems," *IEEE Computer*, vol. 39, pp. 91–92, April 2006.

[9] N. G. Mohammadi et al., *Cloud Computing and Services Science*, ch. Trustworthiness Attributes and Metrics for Engineering Trusted Internet-Based Software Systems.

[10] S. Xu, "Toward a theoretical framework for trustworthy cyber sensing," in *Proc. of SPIE Defense, Security, and Sensing*, 2010.

[11] S. Xu, R. S. Sandhu, and E. Bertino, "TIUPAM: A framework for trustworthiness-centric information sharing," in *Proceedings of International Conference on Trust Management (IFIPTM'09)*, pp. 164–175, 2009.

[12] S. Xu, H. Qian, F. Wang, Z. Zhan, E. Bertino, and R. S. Sandhu, "Trustworthy information: Concepts and mechanisms," in *Proceedings of 11th International Conference on Web-Age Information Management (WAIM'10)*, pp. 398–404, 2010.

[13] W. Dai, T. P. Parker, H. Jin, and S. Xu, "Enhancing data trustworthiness via assured digital signing," *IEEE Trans. Dependable Sec. Comput.*, vol. 9, no. 6, pp. 838–851, 2012.

[14] W. Borst, *Construction of Engineering Ontologies*. University of Tweente, Eschede: Centre for Telematica and Information Technology, 1997.

[15] N. Guarino, "Formal ontology in information systems," pp. 3–15, Amsterdam: IOS Press, 1998.

[16] R. Paul et al., "An ontology-based integrated assessment framework for high-assurance systems," in *IEEE International Conference on Semantic Computing*, pp. 386–393, 2008.

[17] L. Viljanen, *Trust, Privacy, and Security in Digital Business*, vol. 3592, ch. Towards an Ontology of Trust, pp. 175–184. Springer-Verlag Berlin Heidelberg, Lecture Notes in Computer Science, 2005.

[18] E. Chang, T. S. Dillon, and F. Hussain, "Trust ontologies for e-service environments," *International Journal of Intelligent Systems*, vol. 22, pp. 519–545, 2007.

[19] N. Dokoohaki and M. Matskin, "Structural determination of ontology-driven trust networks in semantic social institutions and ecosystems," in *International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, (Papeete, France), pp. 263–268, Nov. 2007.

[20] P. T. Vlacheas et al., "Ontology and taxonomies of resilience," tech. rep., European Network and Information Security Agency, Oct. 2011.

[21] J.-H. Cho, K. S. Chan, and S. Adali, "A survey on trust modeling," *ACM Computing Surveys*, vol. 48, p. Article No. 28, Nov. 2015.

[22] M. H. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein, "Towards a standardized terminology for network performance," *IEEE Transactions on Reliability*, vol. 57, pp. 267–271, June 2008.

[23] Y. Y. Haimes, "Perspective on the definition of resilience in systems," *Risk Analysis*, vol. 29, no. 4, pp. 498–501, 2009.

[24] P. Cholda, J. Tapolcai, T. Cinkler, K. Wajda, and A. Jajszczyk, "Quality of resilience as a network reliability characterization tool," *IEEE Networks*, vol. 23, pp. 11–19, March/April 2009.

[25] A. H. Dekker, "Measuring the agility of networked military forces," *Journal of Battlefield Technology*, vol. 9, pp. 1–6, March 2006.

[26] D. S. Alberts, "Agility, focus, and convergence: The future of command and control," *The International C2 Journal*, vol. 1, no. 1, pp. 1–30, 2007.

[27] K. Conboy, "Agility from first principles: Reconstructing the concept of agility in information systems development," *Information Systems Research*, vol. 20, pp. 329–354, Sept. 2009.

[28] Marriam-Webster Dictionary, "Definition of threat," 2016.

[29] Merriam-Webster Dictionary, "Definition of trust," 2015.

[30] R. B. V. Jr., R. Henning, and A. Siraj, "Information assurance measures and metrics - state of practice and proposed taxonomy," in *Proceedings of the 36th Hawaii International Conference on System Sciences*, 2003.

[31] B. J. Wood and R. A. Duggan, "Red teaming of advanced information assurance concepts," in *Proc. of DARPA Information Survivability Conference and Exposition*, vol. 2, pp. 112–118, 2000.

[32] J. Goel and B. Mehtre, "Vulnerability assessment and penetration testing as a cyber defence technology," *Procedia Computer Science*, vol. 57, pp. 710–715, 2015.