A Comprehensive Quantified Approach for Security Risk Management in e-Health Systems

Sondes Ksibi, Faouzi Jaidi and Adel Bouhoula
Digital Security Research Lab, Higher School of Communications of Tunis, University of Carthage, Tunisia

Keywords: e-Health, IoT, Risk Management, Trust, Security.

Abstract: As a major advancement technology in healthcare industry, e-health contributes to setting up efficient and highly automated healthcare infrastructures. Internet of things (IoT) holds great promise for healthcare providers as well as for its end users. Internet of Medical Things (IoMT) applications are among the major trends of the moment. Nonetheless, numerous security features remain as main issues towards secure, reliable and privacy-preserving e-health systems. Indeed, the participating nodes in IoMT networking for e-health service delivery; which are heterogeneous and resource-constrained; generate, collect and exchange huge amounts of private and extremely sensitive data. These facts, among others, expand the attack surface and decrease the trustworthiness in e-health systems. In this research work, we propose a framework to enhance trust and help with making decisions based on a quantified risk assessment approach. This framework relies on a novel approach/model for improving trust and risk management in an e-health context.

1 INTRODUCTION

Networking of smart electronic devices, commonly called Internet of Things (IoT) is gaining a rising focus from business developers and end users. Things are interconnected and exchanging data to perform a programmed task with reduced human exertion, improved efficiency and increased economic benefits. One of the most attractive opportunities seems to be healthcare. As per statistics, according to *Meticulous Research Report*, IoT healthcare market is expected to grow from 55.5 Billion USD in 2019 to 322.2 Billion USD by 2025 (Research, 2019). IoMT applications are among the main trends of the moment. Indeed, from simple diagnostics to complex surgical procedures, connected things with computing and networking advancements led to create the new concept of modern medicine. IoT is transforming the way patients are treated to more efficient, helping healthcare industry workers and improving research results.

Despite this advancement, e-health is still facing several challenges such as ubiquity, cost, complexity of data manipulation, resources constraints and definitely the most important are security and privacy issues. Indeed, worries about protecting and preserving privacy in e-health systems do not only concern these systems themselves but also their increasingly open, heterogeneous and scalable eco-systems. The ability to confidentially and reliably transmit highly sensitive data between connected devices seems to be a complex challenge since: (i) medical connected devices can be located in un-trusted areas that may be under attacker's control; this may threaten patient's lives; (ii) in IoMT industry, the main occupation is providing required functionality at a reasonable cost. So, security is an after-thought, often placed at the bottom of the priority list in the development life cycle; (iii) traditional security solutions are not pretty suitable with resource-constrained IoT and medical devices; and (iv) last but not least, e-health systems require simultaneously rigorous (sufficiently robust controls to prevent unauthorized accesses) and flexible (smoothly and transparently weaving flexible controls to allow emergency accesses) security solutions. It has been proved that this irregular balance between flexibility and robustness has a wide impact on the compliance of deployed solutions (Jaïdi et al., 2016).

The aim of this paper is to carry on a relevant analysis of security risk management aspects. This analysis will mainly help us in setting up our solution to address the security risks within an e-healthcare context. As a main contribution, we define a framework to enhance trust and help with making decisions based on a quantified risk assessment approach. Our proposal is based on a novel approach for improving trust and managing security risk in e-healthcare.

Ksibi, S., Jaidi, F. and Bouhoula, A.
A Comprehensive Quantified Approach for Security Risk Management in e-Health Systems.
DOI: 10.5220/0009893806520657
In *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020) - SECRYPT*, pages 652-657
ISBN: 978-989-758-446-6

The reminder of the paper is organized as follows. In section 2, we introduce the security risk concept and review related works. In section 3, we outline the idea of our proposal. We introduce the main concepts of our approach for security trust-risk management within e-health contexts, work on case of study and highlight guidelines and perspectives. Finally, we conclude the paper and present ongoing works.

2 SECURITY RISK MANAGEMENT IN E-HEALTH

2.1 Terminologies and Definitions

Risk: According to the International Standardization Organization (ISO) [ISO 31000; ISO 27005], risk is the effect (positive and/or negative) of uncertainty on objectives (financial, health, safety, etc.) (ISO, 2009). Concretely, it is often expressed as a combination of the consequences (costs) of an event and the corresponding likelihood of occurrence.
Security Risk: It is, in Information Systems (IS), the risk that occurs due to loss of data or system confidentiality, integrity, or availability. It considers potential adverse impacts to the organization (assets, mission, functions, image, or reputation), users, other organizations, and the country (Force, 2018).
Risk Assessment: The risk assessment is an overall process that consists of risk identification (recognition and description of risks), risk analysis and risk evaluation. The assessment may be based on qualitative or quantitative approaches.
Risk Management: Security and cyber security risk management consist of a range of activities undertaken for protecting information and systems from cyber threats such as unauthorized access, in order to: (i) maintain awareness of security and cyber threats; (ii) identify anomalies, misconfigurations and incidents adversely affecting the system and/or data; and (iii) mitigate the impact of, respond to, and recover from incidents. The ISO 31000 risk management process consists of systematic application of policies, procedures and practices to the activities of: communication and consulting; context establishment, risk assessment (identification, analysis and evaluation), risk treatment, risk monitoring and review.

2.2 The Trust-risk Awareness Context

In a risk awareness context, addressing risk management, like illustrated by figure 1, deals mainly with two basic concepts: risk and trust. It is important

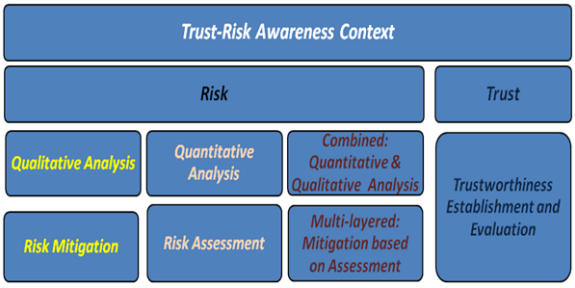

Figure 1: The Trust-Risk awareness context.

to notify that the risk concept is highly coupled with the trust concept. Indeed, a system with a low level of risk is seen with a high level of trust and vice versa. Incorporating risk awareness in IS may pursue one of the following analysis approaches: qualitative approach, quantitative approach and a combination of them. Qualitative approaches use qualifying attributes to describe potential consequences as well as their occurrence probability. In practice, via a qualitative approach, we generally focus on how to mitigate a risk without evaluating its value. Quantitative approaches use numerical values, instead of descriptive attributes, for consequences and corresponding likelihoods. In practice, via a quantitative approach, we generally focus on how to assess the value of a risk. In case of combining both approaches, qualitative analysis is often used first to obtain a general indication of the level of risks and to highlight the main risks.

2.3 Summary of Security Risk Management Solutions for e-Health

Trust-risk Awareness Methods and Models: Several methods, models and frameworks for trust-risk awareness are defined in literature. The OCTAVE (Caralli et al., 2007) method allows investigating recovery impact areas based on a questionnaire. The TARA method defined in (Wynn et al., 2011), as a predictive framework for defending vulnerabilities, allows targeting only most critical exposures. The CVSS defined in (CVSS, 2018) computes scores of vulnerabilities severity based on simple mathematical approximations that translate expert's opinions to numerical scores. Exostar (Shaw et al., 2017) is a system that deals with cyber-security of supply chains (it does not evaluate the enterprise stand-alone risk) and regulatory conformity of providers partners. A complementary approach to Exostar is CMMI (CMMI, 2017) that deals with stand-alone enterprise risk and risk associated to products development life cycle. The ISO model (ISO, 2009) addresses the standardization (based on consensus) of risk management and assessment. It offers guidelines and standards to help set-

ting up risk management systems but it does not provide mechanisms to guarantee their compliance. The NIST model (Force, 2018) defines effective and documented processes (as a set of standards and guidelines addressing risk assessment and risk management) that require automation tools and software development to make it usable. The FAIR model (FAIR, 2017) is based on a quantitative approach for the assessment of risk impact. It aims to establish a standard which is not based on consensus, but it promotes commercial software. As example of software promoted by FAIR, RiskLens (RiskLens, 2017) and CyVaR (Cyber Value at Risk) (Sanna, 2016) are black box tools that may engender standard deviation, consistence and trustworthiness problems.

Trust-risk Awareness for IoT, IoMT and e-Health: Several research works addressed the trust-risk assessment in e-health. Authors in (Radanliev et al., 2018) proposed a quantitative model, based on the coupling of the Cyber Value-at-Risk (CyVaR) and the MicroMort (MM) models, for the economic impact assessment of IoT cyber risk. In (Nurse et al., 2017), authors studied the application of existent security risk assessment approaches in an IoT context. They demonstrated that current solutions are not adequate for IoT context due to: shortcomings of periodic assessment, changing systems boundaries, yet limited system knowledge, challenge of understanding the glue, and failure to consider assets as an attack platform. They highlighted the need of new approaches to assess IoT system risk. Authors in (Malik and Singh, 2019), dealt with security vulnerabilities identification and mitigation in IoT based on a smart software vendor that lists common vulnerabilities (stored in its database) and provides a possible mitigating solution. In (Radanliev et al., 2019), authors focused on a transformation roadmap for standardizing IoT risk impact assessment (based on functional dependency) and calculating the economic impact of cyber risk (based on a goal oriented approach). Authors in (Akinrolabu et al., 2019) proposed a quantitative model, called CSCCRA, to assess the risk of a SaaS application and its supply chain mapping.

Trust-risk Awareness for Access Control: integrating risk awareness in role based access control (RBAC) systems concerns four main concepts: (i) enhancing trustworthiness relationships; (ii) defining mitigation strategies based on constraints; (iii) managing accesses based on quantified approaches; or (iv) assessing policies critical breaches for a secure and efficient policy management. Several works proposed integrating trust relationships in RBAC model (Chakraborty and Ray, 2006), (Feng et al., 2008). This allows evaluating trust levels of policy components and only trusted accesses are authorized. The risk mitigation concept deals particularly with imposing hard constraints on the policy components in order to tone down associated risks. Different constraint-based risk mitigation approaches and models have been proposed to formally specify Static Separation of Duty (SSoD) and Dynamic Separation of Duty (DSoD) policies (Simon and Zurko, 1997), (Gligor et al., 1998), (Jaeger, 1999). Authors in (Chen and Crampton, 2011) proposed to use a strategy of mitigation based on risk thresholds and an associated obligation pairs. As for access risk quantification, proposed approaches deal mainly with risk assessment of access requests. Several authors have focused on risk quantification approaches and proposed different frameworks (Ni et al., 2010), (Molloy et al., 2012), (Ma et al., 2010). Finally, concerning the monitoring of policies compliance based on risk assessment/management approaches, few works addressed this important thematic. Contributions deals mainly with the assessment of the risk associated to the policy defects and anomalies (Jaïdi et al., 2018) as well as the management of policies against attack scenarios in a correlated anomalies context (Evina et al., 2018).

2.4 Discussion

The thematic of security in e-health and particularly IoMT applications is still a challenging task. Among the concerned security concepts that need to be enhanced for ensuring the security and preserving the privacy in e-healthcare, we address the theme of security risk management in IoMT. The application of well established risk assessment approaches and methodologies in an IoMT context fails due to several constraints (such as context specificities, resource constraints, context dynamism, no standards established yet, high level of surety required, shortcomings of periodic assessment, changing systems boundaries yet limited system knowledge, the challenge of understanding the glue, failure to consider assets as an attack platform, continuous evolution of new and advanced threats, etc.). Hence, we need new approaches to assess IoMT system risk. Recent works in IoT risk assessment addressed mainly the evaluation of the economic impact of IoT cyber-security threats. From the perspective of access control, current solutions failed to manage end-to-end risk and to combine both aspects simultaneously: assessing risks associated to access requests and risks of policies critical breaches anomalies and attacks. In the next section we introduce a novel approach that aims to address the discussed limitations of current solutions.

3 THE SECURITY RISK MANAGEMENT APPROACH

3.1 Objectives

E-health applications involve a variety of contexts for managing security risks as well as strategies for risk mitigation which may suit particular cases and do not in other cases. To ensure effectiveness and efficiency of the risk management method/strategy, we propose a dynamic quantified risk-based approach. As a fine-grained approach, the risk zone is divided to three main areas of focus: data acquisition area (devices), data gathering and transmission area (PAN, WiFi, Bluetooth, 2G/3G/4G, etc.) and finally data processing and storage area (typically databases).The main purposes of the proposed approach are:

- Evaluating the cumulative risk for a global e-health service delivery process.
- Establishing a fine-grained risk management process based on context specific risk metrics, qualifiers, thresholds, factors, etc.
- Automating the update procedure for risk mitigation response.

3.2 Principle

Our approach, illustrated by figure 2, consists of three basic sub-systems and a centralized module, an orchestrator called core risk manager. These subsystems can either: (i) make decisions based on identified and assessed risk metrics autonomously regarding specific pre-defined risk thresholds; or (ii) delegate the decision making to the orchestrator.

Device Risk Manager (DRM): as a first level decision-maker, this module performs risk management in the context of data acquisition layer. The DRM analyzes data generated by devices in order to evaluate the inherent risks, then, it compares obtained risk values with predefined thresholds. In case of a risky behavior, the DRM interrupts the data transfer. Otherwise, the quantified risk value is stored and transmitted to the core manager for a deeper analysis.

Network Risk Manager (NRM): its role is to identify risks related to communication channels used within the e-health system. The NRM applies the quantification function to the specific risk factors related to the applied protocols. Risk values are assessed and compared to predefined thresholds. Results are then communicated to the CRM.

Storage and Processing Risk Manager (SPRM): it is related to the data storage and processing subsystem. It performs the same process as the other modules taking into account specific risk factors related to the databases as inputs.

Core Risk Manager (CRM): it performs end-to-end risk management, via collecting information from other subsystems. Collected data is stored in a global repository; classifications, prioritization and correlation between results are done to refine decisions and update thresholds. Other risk factors related to the environment or specific use cases can be analyzed here. The CRM updates the elementary databases of other units if optimized metrics are obtained.

3.3 Case of Application (SPRM)

The SPRM allows computing the risk values associated to non-compliance anomalies or attacks scenarios in RBAC policies. It is defined to deal with relational databases as storage entities and also with cloud databases (as a main extension of our previous approach discussed in (Jaïdi et al., 2018). The SPRM disposes of the following principal components. A RAE (Risk Assessment Engine) in charge of the assessment of risk values related to identified anomalies and threats as well as the estimation/re-estimation of the risk thresholds and rating, taking into account a set of risk factors. A RM (Response Monitor) responsible for analyzing and classifying obtained risk values with respect to corresponding thresholds and rating. Based on this classification and other parameters, the RM may react autonomously vis-à-vis risky situations via blocking access, desactivating privileges, while in normal cases it simply delegates the decision to CRM for a global decision. A RD (Risk Depository) stores, for each case, all the required metrics (risk values, ratings, thresholds, etc.). A RFD (Risk Factors Depository) stores a collection of established risk factors, such as context factors, historical events, etc., used for a dynamic evaluation of the risk metrics and for a dynamic analysis and classification of the defects and attacks. A RFM (Risk Factors Monitor) responsible for managing the risk factors collection. As an illustrative example of the assessment model, we consider a first risk rating (Extremely High: $\geq 80\%$; High: $\geq 60\%$ and $< 80\%$; Moderate: $\geq 40\%$ and $< 60\%$; Low: $\geq 20\%$ and $< 40\%$; Minor: $\geq 0\%$ and $< 20\%$). The RAE evaluates the risk of the permission Pi according to formula (1), where $Pr(k)$ denotes the probability of occurrence of a particular malicious usage k, $k = 1, ..., m$; $C(k)$ is the cost associated to this malicious usage, and CM is the value associated to existing countermeasures.

$$R(Pi) = \sum_{(k=1)}^{m} P(k) * C(k) - CM. \quad (1)$$

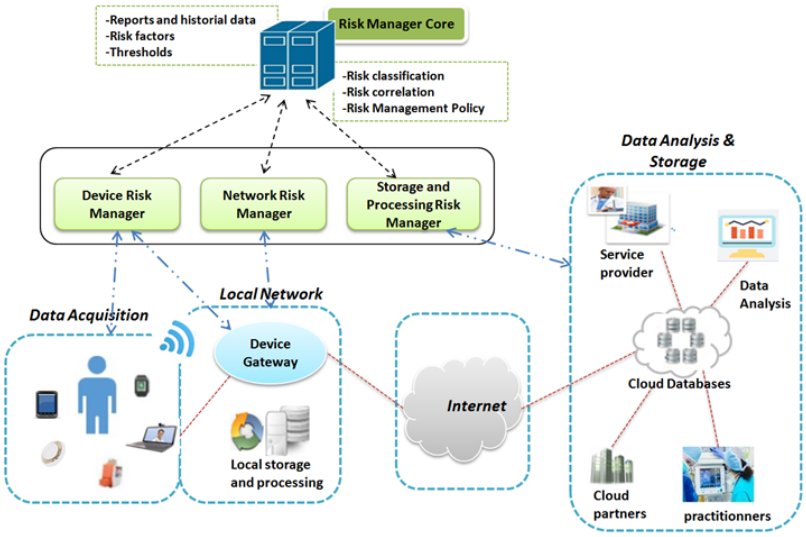

Figure 2: Dynamic-Quantified risk management approach.

Therefore, the risk of the role Rj is evaluated, according to formula (2), as the sum of the risk values of all permissions assigned to it, where $APR(Rj)$ is the set of permissions assigned to Rj. The risk of the user Ui is computed, via formula (3), as the sum of the risk values of roles assigned to that user noted $AUR(Ui)$.

$$R(Rj) = \sum_{(i=1)}^{n} R(Pi) | Pi \in APR(Rj). \quad (2)$$

$$R(Ui) = \sum_{(j=1)}^{n} R(Rj) | Rj \in AUR(Ui). \quad (3)$$

To assess the risk of the policy defects, we determine the impact/effect of each abnormality on the system, in other words we worked to quantify the influence of identified breaches on the system. For this, we assess the anomaly risk, according to formula (4), as the ratio between the anomaly sub-elements risk values and the system elements risk values where the selected elements are from the same type.

$$R(Anomaly) = \frac{\sum_{(j=1)}^{n} R(x) | x \in \{Anomaly\}}{\sum_{(l=1)}^{m} R(y) | y \in System} * 100\%. \quad (4)$$

Obtained results from application in a real world context (a medical system application) highlight the effectiveness as well as the usefulness of the SPRM.

3.4 Discussion and Perspectives

E-health systems still offer neither clear controls for patients security and privacy preservation nor documentation to inform a user about risks introduced when specific applications are deployed. Several research works addressed the problem of security in these constrained systems.The issue is about re-architecting security solutions to suit the emerging applications in e-health paradigms. We believe that the proposed approach may significantly improve the security of IoMT infrastructures and minimize the costs associated with the collateral damage that would affect the system users. The objective of this innovative dynamic-quantified security risk management framework are to predict and evaluate risk damages, identify new or unseen threats within IoMT applications and help security architects implementing countermeasures for mitigating risks. This framework is based on a cyclical risk management process and fine-grained automatic decision-making. We worked on the SPRM subsystem and we plan setting up the rest of the risk management subsystems. As a primary case of application, we addressed access control violations and threats as basic security issues.

4 CONCLUSIONS

Security solutions for e-health in the emerging IoT landscape offer exciting opportunities to the industry. Risk management frameworks are one of the promising solutions to minimize costs of eventual damages that would affect e-health system users and threaten their private data and their safety. We studied risk management methods and models in literature and highlighted some proposed frameworks by the research community. We proposed a novel approach based on a quantified risk management method com-

posed of three distributed and chained subsystems and an orchestrator module. The proposal aims to evaluate risks related to three vulnerable zones of the e-health system: devices landscape, network part and storage infrastructure. Ongoing work deals with the formalization of the approach and setting up the interactions between the different subsystems.

REFERENCES

Akinrolabu, O., New, S., and Martin, A. (2019). Csccra: A novel quantitative risk assessment model for saas cloud service providers. *Computers*, 8(3):66.

Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007). Improving the information security risk assessment process–.

Chakraborty, S. and Ray, I. (2006). Trustbac: integrating trust relationships into the rbac model for access control in open systems. In *Proceedings of the eleventh ACM symposium on Access control models and technologies*, pages 49–58.

Chen, L. and Crampton, J. (2011). Risk-aware role-based access control. In *International Workshop on Security and Trust Management*, pages 140–156. Springer.

CMMI (2017). What is capability maturity model integration (cmmi). http://cmmiinstitute.com/capability-maturity-model-integration. Accessed: 2020-04-30.

CVSS (2018). Common vulnerability scoring system sig. https://www.first.org/cvss/. Accessed: 2020-04-30.

Evina, P. A., Ayachi, F. L., Jaidi, F., and Bouhoula, A. (2018). Anomalies correlation for risk-aware access control enhancement. In *ENASE*, pages 299–304.

FAIR (2017). Quantitative information risk management - the fair institute, factor analysis of information risk. http://www.fairinstitute.org. Accessed: 2020-04-30.

Feng, F., Lin, C., Peng, D., and Li, J. (2008). A trust and context based access control model for distributed systems. In *2008 10th IEEE International Conference on High Performance Computing and Communications*, pages 629–634. IEEE.

Force, J. T. (2018). Risk management framework for information systems and organizations. *NIST Special Publication*, 800:37.

Gligor, V. D., Gavrila, S. I., and Ferraiolo, D. (1998). On the formal definition of separation-of-duty policies and their composition. In *Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No. 98CB36186)*, pages 172–183. IEEE.

ISO (2009). *Risk Management: Principles and Guidelines*. International Standardization Organization.

Jaeger, T. (1999). On the increasing importance of constraints. In *Proceedings of the fourth ACM workshop on Role-based access control*, pages 33–42.

Jaïdi, F., Labbene-Ayachi, F., and Bouhoula, A. (2016). Advanced techniques for deploying reliable and efficient access control: Application to e-healthcare. *Journal of medical systems*, 40(12):262.

Jaïdi, F., Labbene Ayachi, F., and Bouhoula, A. (2018). A methodology and toolkit for deploying reliable security policies in critical infrastructures. *Security and Communication Networks*, 2018.

Ma, J., Adi, K., Mejri, M., and Logrippo, L. (2010). Risk analysis in access control systems. In *2010 Eighth International Conference on Privacy, Security and Trust*, pages 160–166. IEEE.

Malik, V. and Singh, S. (2019). Security risk management in iot environment. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(4):697–709.

Molloy, I., Dickens, L., Morisset, C., Cheng, P.-C., Lobo, J., and Russo, A. (2012). Risk-based security decisions under uncertainty. In *Proceedings of the second ACM conference on Data and Application Security and Privacy*, pages 157–168.

Ni, Q., Bertino, E., and Lobo, J. (2010). Risk-based access control systems built on fuzzy inferences. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pages 250–260.

Nurse, J. R., Creese, S., and De Roure, D. (2017). Security risk assessment in internet of things systems. *IT professional*, 19(5):20–26.

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., and Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, 102:14–22.

Radanliev, P., De Roure, D. C., Nurse, J. R., Burnap, P., Anthi, E., Uchenna, A., Santos, O., Montalvo, R. M., et al. (2019). Cyber risk management for the internet of things.

Research, M. (2019). Internet of things (iot) in healthcare market - global opportunity analysis and industry forecast (2018-2025). https://meticulousresearch.com/product/healthcare-iot-market/. Accessed: 2020-04-30.

RiskLens (2017). Risk analytics platform, fair platform management. https://www.risklens.com/platform. Accessed: 2020-04-30.

Sanna, N. N. (2016). What is a cyber value-at-risk model? www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model. Accessed: 2020-04-30.

Shaw, R., Takanti, V., Zullo, T., Director, M., and Llc, E. (2017). Best practices in cyber supply chain risk management boeing and exostar cyber security supply chain risk management interviews.

Simon, R. T. and Zurko, M. E. (1997). Separation of duty in role-based environments. In *Proceedings 10th Computer Security Foundations Workshop*, pages 183–194. IEEE.

Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., Graubart, R., and Clausen, L. (2011). Threat assessment & remediation analysis (tara): Methodology description version 1.0. Technical report, MITRE CORP BEDFORD MA.