DEVELOPMENT OF SECURITY METRICS

Based on Decomposition of Security Requirements and Ontologies

Reijo M. Savola
VTT Technical Research Centre of Finland, Oulu, Finland

Keywords: Security metrics, Security requirements, Decomposition, Ontologies.

Abstract: Systematically and carefully designed information security metrics can be used to provide evidence of the security solutions of the system under development. The lack of appropriate security solutions in software-intensive systems might have serious consequences for businesses and the stakeholders. We investigate holistic development of security metrics based on security requirement decomposition and ontologies. The high-level security requirements are expressed in terms of lower-level measurable components applying a decomposition approach. Security requirement analysis of a distributed messaging system is used as an example.

1 INTRODUCTION

Information security is clearly a challenging system-level problem. One cannot accurately determine the information security requirements outside the context and environment of the target system. Building security requirements is often a process of making trade-off decisions especially between high security, high usability and low cost.

The rest of this paper is organized into the following sections. Section 2 presents the metrics development approach and different parts of it. Section 3 discusses related work and finally, Section 4 summarizes the study with some future research questions and conclusions.

2 PROPOSED APPROACH

In this study, we use the following iterative process for security metrics development, partly based on Savola (2007). The steps for the process are as follows:

1. Carry out threat and vulnerability analysis. Carry out threat analysis of the system under investigation and its use environment (use cases). Identify known or suspected vulnerabilities.
2. Define and prioritize security requirements in a holistic way based on threat analysis. The most critical security requirements should be paid the most attention. Pay attention to the coherence of requirements.
3. Identify basic measurable components from the higher-level requirements using a decomposition approach.
4. Define measurement architecture for on-line metrics and evidence collection mechanisms for off-line metrics.
5. Select basic measurable components based on e.g. feasibility and importance.
6. Apply suitable metrics ontologies to the chosen basic measurable components to plan the actual metrics development.
7. Develop appropriate off-line and on-line security metrics, and the functionalities and processes where they are used.

Note that all steps are highly iterative and the sequence of the steps can be varied. Steps 1 and 2 should be started as early as possible in the system development process and elaborated iteratively as the system design gets more mature. Steps 3 and 4 can be carried out in parallel to each other. Step 4 can also be started partially already during the architectural design phase of the system.

2.1 Threat and Vulnerability Analysis

Threat analysis is the process of determining the relevant threats to a System Under Investigation (SUI). The outcome of the threat analysis process is a description of the threat situations. In practice, there are many ways to carry out threat analysis,

M. Savola R. (2009).
DEVELOPMENT OF SECURITY METRICS - Based on Decomposition of Security Requirements and Ontologies.
In *Proceedings of the 4th International Conference on Software and Data Technologies*, pages 171-174
DOI: 10.5220/0002243501710174

from simply enumerating threats to modelling them in a rigorous way. The extent of threat analysis depends, e.g., on the criticality of the use cases in SUI. The following threat and vulnerability analysis process can be used, based on the Microsoft threat risk modelling process (Howard and LeBlanc, 2003):

1. Identify security objectives,
2. Survey the SUI architecture,
3. Decompose the SUI architecture to identify functions and entities with impact to security,
4. Identify threats, and
5. Identify vulnerabilities.

The security objectives can be decomposed, e.g., to identity, financial, reputation, privacy and regulatory and availability categories (OWASP, 2009). There are many different sources of risk guidance that can be used in developing the security objectives, such as laws, regulations, standards, legal agreements and information security policies.

Vulnerability analysis can be carried out after appropriate technological choices have been made. Vulnerabilities in the technology and implementation affect to threats of the system. In vulnerability analysis, well-known vulnerability listings and repositories such as OWASP (Open Web Application Security Project) Top 10 (OWASP, 2009) can be used.

2.2 Definition and Prioritization of Security Requirements

Security requirements derive from *threats*, *policies* and *environment properties*. Security requirements that are derived from threats are actually countermeasures. Policies are security relevant directives, objectives and design choices that are seen necessary for the system under investigation. Environment properties contribute to the security of the SUI from outside.

In general, every security risk due to a threat chosen to be cancelled or mitigated must have a countermeasure in the collection of security requirements.

A security requirement of the SUI r_i is derived from applicable threat(s) θ_i, policies p_i and the environment properties e_i:

$$r_i = (\theta_i , p_i, e_i),\\ r_i \in R, \theta_i \in \Theta, p_i \in P, e_i \in E, \tag{1}$$

where R is the collection of all security requirements of SUI, Θ is the collection of all security threats chosen to be cancelled or mitigated, P is the collection of all security policies applied to SUI, and E is the collection of all environment properties that contribute to the security of the SUI from outside.

2.3 Decomposition of Security Requirements

The core activity in the proposed security metrics development process is in decomposing the security requirements. In the following, we discuss the decomposition process and give an example of it.

The following decomposition process, based on Wang and Wulf (1997), is used to identify measurable components from the security requirements:

1. Identify successive components from each security requirement (goal) that *contribute to the success* of the goal.
2. Examine the subordinate nodes to see if further decomposition is needed. If so, repeat the process with the subordinate nodes as current goals, breaking them down to their essential components.
3. Terminate the decomposition process when none of the leaf nodes can be decomposed any further, or further analysis of these components is no longer necessary.

When the decomposition terminates, all leaf nodes should be measurable components. In the following, we decompose the requirements presented above and discuss the results. Since adaptive security contains higher-level requirements, we leave it to the last. It is easier to investigate the six lower-level requirement categories first.

In general, the model depicted in Fig. 1 can be used for the authentication decomposition (Wang and Wulf, 1997) during the process of identifying potential metrics for authentication performance.

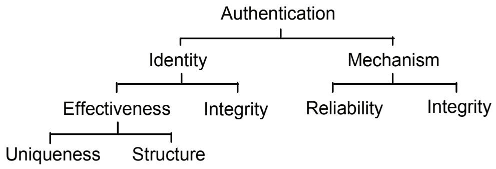

Figure 1: Decomposition of authentication.

See (Savola and Abie, 2009) for a more detailed discussion of security requirement decomposition and identification of basic measurable components.

2.4 Measurement Architecture and Evidence Collection

The next step requires *identification of measurable* *information* and the *mechanisms how to obtain and process* that data. Both on-line and off-line evidence collection should be designed. In many cases, on-line and off-line measurements can be dependent on each other.

Identification of measurable information can be carried out, e.g., from data flow diagrams and protocol descriptions. As an example, Fig. 2 shows a conceptual picture of information flows of a distributed messaging system GEMOM, Genetic Message Oriented Secure Middleware (Abie *et al.*, 2008). Security metrics of the Security Monitor module can use information from the Broker module, Audit and Logging module and Security module. In addition, the metrics get information from memory, storage and network interfaces.

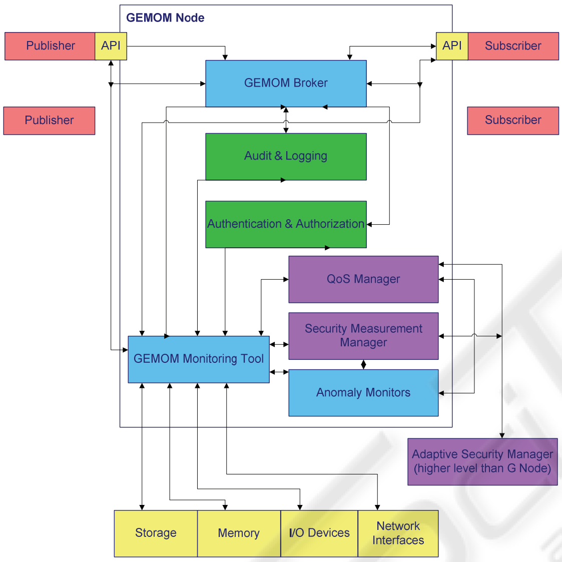

Figure 2: Example of information flows to and from the GEMOM Monitoring Tool containing security metrics.

2.5 Feasibility and Importance of Metrics

According to Jelen (2000), a good metric is Specific (well-defined, using unambiguous wording), Measurable (quantitative when feasible), Attainable (within budgetary and technical limitations), Repeatable (measurements from which metric is derived do not vary depending on the person taking them) and Time-dependent (takes into consideration measurements from multiple time slices) (“SMART”). Payne (2006) remarks that truly useful security metrics indicate the degree to which security goals, such as data confidentiality, are being met.

The feasibility of measuring security and developing security metrics to present actual security phenomena has been criticized in many contributions. In designing a security metric, one has to be conscious of the fact that the metric simplifies a complex socio-technical situation down to numbers or partial orders. McHugh (2002) is skeptical of the side effects of such simplification and the lack of scientific proof. Bellovin (2006) remarks that defining metrics is hard, if not infeasible, because an attacker’s effort is often linear, even in cases where exponential security work is needed. Another source of challenges is that luck plays a major role (Burris, 2000) especially in the weakest links of information security solutions. Those pursuing the development of a security metrics program should think of themselves as pioneers and be prepared to adjust strategies as experience dictates (Payne, 2000).

2.6 Use of Metrics Ontologies

After the decomposition of security requirements, metrics ontologies can be used to help in planning the actual metrics development process.

Fig. 3. shows an example metrics ontology for reliability metrics, see example in Fig. 3 (Niemelä *et al.*, 2008). Reliability can be seen at the leaf of the authentication taxonomy of Fig. 1. From the example reliability metrics ontology, it can be seen that there are reliability metrics that emphasize either strengths or weaknesses. Strength metrics can be divided into maturity metrics, normal case metrics and abnormal case metrics.

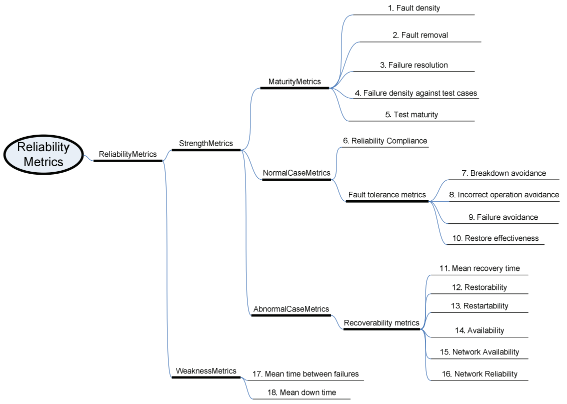

Figure 3: Example of a reliability metrics ontology (Niemelä *et al.*, 2008).

3 RELATED WORK

Wang and Wulf (1997) describe a general-level framework for measuring system security based on a decomposition approach. CVSS (Common Vulnerability Scoring System) (Schiffman, 2004) is a global initiative designed to provide an open and standardized method for rating information technology vulnerabilities from a practical point of view. NIST's Software Assurance Metrics and Tool Evaluation (SAMATE) project (Black, 2006) seeks to help answer various questions on software assurance, tools and metrics. OWASP (2009) (Open Web Application Security Project) contains an active discussion and development forum on security metrics. More security metrics approaches are surveyed in (Savola, 2007) and (Savola, 2008).

4 CONCLUSIONS

The field of developing security metrics systematically is young and the current practice of information security is still a highly diverse field, and holistic and widely accepted approaches are still missing.

We have introduced a novel methodology for security metrics development based on threats, policies, security requirements and requirement decomposition. The developed approach enables to describe and relate different types of security metrics in a systematic way.

Further work is needed in definition of the measurement architecture, evidence collection and selection of measurable components. Methods to assess the importance, feasibility and complexity of security metrics are needed. Furthermore, more detailed metrics to the system under investigation should be developed and validated in the actual system. The future work includes more thorough investigation of suitable generic decomposition models.

ACKNOWLEDGEMENTS

The work presented in this paper has been carried out in the GEMOM FP7 research project, partly funded by the European Commission.

REFERENCES

Abie, H., Dattani, I., Novkovic, M., Bigham, J., Topham, S. and Savola, R. GEMOM – Significant and Measurable Progress Beyond the State of the Art. In *ICSNC 2008*. Malta, Oct. 26-31, 2008, pp. 191-196.

Bellovin, S. M. On the Brittleness of Software and the Infeasibility of Security Metrics. In *IEEE Security & Privacy*, Jul/Aug. 2006, p. 96.

Black, P. E. SAMATE's Contribution to Information Assurance. In *IAnewsletter*, Vol. 9, No. 2, 2006.

Burris, P. and King, C. *A Few Good Security Metrics*. METAGroup, Inc. Oct. 2000.

Howard, M. and LeBlanc, D. *Writing Secure Code*, Second Edition, Microsoft Press, 2003.

Jelen, G. SSE-CMM Security Metrics. In *NIST and CSSPAB Workshop*, Washington, D.C., 2000.

McHugh, J. Quantitative Measures of Assurance: Prophecy, Process or Pipedream? In *Workshop on Information Security System Scoring and Ranking*, ACSA and MITRE, Williamsburg, Virginia, May 2001 (2002).

Niemelä, E., Evesti, A. and Savolainen, P. Modeling Quality Attribute Variability. In *3rd Int. Conf. on Evaluation of Novel Approaches to Software Engineering*. Funchal, Portugal, May 4-7, 2008, pp. 169-176.

OWASP. *Open Web Application Security Project*. http://www.owasp.org./, 2009

Payne S. C. *A Guide to Security Metrics*. SANS Institute Information Security Reading Room, 2006.

Savola, R. Requirement Centric Security Evaluation of Software Intensive Systems. In *2nd Int. Conf. on Dependability of Computer Systems DepCOS-RELCOMEX '07*, Szklarska Poreba, Poland, June 14-16, 2007, pp. 135-142.

Savola, R. A Novel Security Metrics Taxonomy for R&D Organisations. In *7th Annual Information Security South Africa (ISSA) Conference*, Johannesburg, South Africa, July 7-9, 2008, pp. 379-390.

Savola, R. and Abie, H. Identification of Basic Measurable Components for a Distributed Messaging System. In *3rd Int. Conf. on Emerging Security Information, Systems and Technologies (SECURWARE) 2009*, Athens, Greece, June 18-23, 2009.

Schiffman, M., Eschelbeck, G., Ahmad, D., Wright, A. and Romanosky, S. *CVSS: A Common Vulnerability Scoring System*, National Infrastructure Advisory Council (NIAC), 2004.

Wang, C. and Wulf, W. A. Towards a Framework for Security Measurement, *20th National Information Systems Security Conference*, Baltimore, MD, Oct. 1997, pp. 522-533.