Metrics for Security of Cooperating Systems

Roland Rieke
Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany
Philipps-Universität Marburg, Germany
roland.rieke@sit.fraunhofer.de
http://rieke.link/

Dagstuhl Seminar "Socio-technical Security Metrics", Dec. 2014

Systems of systems that collaborate for a common purpose are called *cooperating systems*. They are characterised by freedom of decision and loose coupling of their components. Typical examples of cooperating systems are electronic health systems, vehicular ad hoc networks, distributed air traffic management systems, telephone systems, and electronic money transfer systems.

In this abstract, three problems with respect to security metrics for cooperating systems are addressed, namely, (1) abstract representation of security information, (2) security information quality, and (3) elicitation, linkage, and management of security information.

Abstract representation of security information

In order to analyse cooperating systems with respect to threats originating from attackers that try to take control of the system, it is important to develop a metric that provides information on how vulnerable the system is with respect to a given network configuration and policies for the information flow between the components. Attack graphs can be used to find out if there is a combination of basic exploits that enables an attacker to reach critical network resources or block essential services. Attacker capabilities can be given by the set of exploits that the attacker knows, the strategy to select and apply them, and the cost and impact of an execution of the exploit. As it is required to analyse all possible sequences of basic exploits - so called attack paths -, this graph can be huge and complex. Depending on the attributes included in the attack graph, it represents a metric for properties such as the overall vulnerability of the system, the most likely attacker behaviour, or the most effective countermeasures [1]. However, to improve usability of such a metric it is necessary to derive an abstract representation of the graph that provides the important facts on a level a human user can work with. Thus, the ability to *derive appropriate abstract representations* is an important aim to be addressed by any attack graph based metric.

Security information quality

An important property of a security metric is its applicability at runtime. A tool-based runtime calculation of a security metric enables a timely response to attacks as well as an impact mitigation by triggering appropriate countermeasures. Security information and event management systems provide security services to collect and analyse security events and data from a wide variety of sources in order to provide a unified view of the monitored systems' security status. However, in [2] an analysis of a comprehensive set of industrial scenarios has identified several additional security requirements that are not adequately addressed by current security information and event management systems.

In order to address some of these requirements, [3] introduced a novel model-based approach for Predictive Security Analysis at Runtime (PSA@R). In particular, PSA@R widens the focus of the security analysis from a system level view to the business process level. The close-future behaviour of a process instance is predicted based on the process specification. For effective use of PSA@R, it is assumed that a process instance projection is possible for each event from the runtime environment. Unfortunately, if business processes have not been designed for this kind of measures, the necessary information is not present in the security events received. This motivates the generic requirement that systems need to be *designed for security assessment at runtime*.

Elicitation, linkage, and management of security information

In [4], an extensible meta-model has been proposed in order to drive an integrated security strategy management, through an *analysis and refinement* approach, and also through a *security measurement* approach which would enable assessment of the system's performance against the security requirements it was designed for. The overall aim is, to provide an extensible model that spans all parts of the security monitoring and decision support process, namely: (i) detecting threatening events; (ii) putting them in context of the current system state; (iii) explaining their potential impact with respect to some security- or compliance model; and (iv) taking appropriate actions. In particular, a security information meta model has been presented, consisting of: (a) high level goal setting, (b) security requirements, (c) measurement requirements, and (d) objects of measurement. By application of this model, security can be designed in such a way that it can be measured (and managed).

One important missing link in this concept is a structured method to derive measurement requirements from security and dependability requirements, and eventually identify the required objects of measurement. By using such a method in combination with existing methods to refine high-level security goals to concrete security requirements, a *goal-oriented security metric* reflecting security assessment with respect to security goals of the responsible stakeholder could be derived.

Acknowledgement. Research reported in this abstract was supported by the German Federal Ministry of Education and Research in the context of the project ACCEPT (ID 01BY1206D).

References

[1] Roland Rieke. Abstraction-based analysis of known and unknown vulnerabilities of critical information infrastructures. *International Journal of System of Systems Engineering (IJSSE)*, 1:59–77, 2008.

[2] Roland Rieke, Luigi Coppolino, Andrew Hutchison, Elsa Prieto, and Chrystel Gaber. Security and reliability requirements for advanced security event management. In Igor Kotenko and Victor Skormin, editors, *Computer Network Security*, volume 7531 of *Lecture Notes in Computer Science*, pages 171–180. Springer Berlin Heidelberg, 2012.

[3] Roland Rieke, Jürgen Repp, Maria Zhdanova, and Jörn Eichler. Monitoring security compliance of critical processes. In *Parallel, Distributed and Network-Based Processing (PDP), 2014 22th Euromicro International Conference on*, pages 525–560. IEEE Computer Society, Feb 2014.

[4] Roland Rieke, Julian Schütte, and Andrew Hutchison. Architecting a security strategy measurement and management system. In *Proceedings of the Workshop on Model-Driven Security*, MDsec '12, pages 2:1–2:6, New York, NY, USA, 2012. ACM.