Automation possibilities in information security management

Raydel Montesino
Information Security Department
University of Informatics Sciences (UCI)
Havana, Cuba
raydelmp@uci.cu

Stefan Fenz
SBA Research and Vienna University of Technology
Vienna, Austria
sfenz@sba-research.org

***Abstract* — Information security management, as defined in ISO 27001, deals with establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system. This paper provides an analysis about the automation possibilities in information security management. The analysis takes into account the potential of using (i) security ontologies in risk management, (ii) hard- and software systems for the automatic operation of certain security controls, and (iii) the Security Control Automation Protocol (SCAP) for automatically checking compliance and security configurations. The analysis results support organizations and security managers at identifying systems they can use to achieve greater efficiency in the information security management process.**

Keywords - automation; security management; standards; ontologies

I. INTRODUCTION

Managing information systems' security is an expensive and challenging task. Many different and complex software components - including firmware, operating systems, and applications - must be configured securely, patched when needed, and continuously monitored for security. Most organizations have an extensive set of security requirements. For commercial firms, such requirements are established through complex interactions of business goals, governmental regulations, and insurance requirements; for government organizations, security requirements are mandated [1].

Meeting these requirements is time consuming and error prone, because organizations lack automated ways of performing the security management tasks. This paper provides an analysis about the automation possibilities in processes and controls related to information security management. The overall research question is:

- How can we increase information security management automation in the context of the ISO 27001 process model?

In Section II we provide a brief overview of information security management, as defined in the international standard ISO 27001. In Section III we analyze the automation potential of security ontologies for the risk management process. In Section IV this paper provides an analysis of security controls that can be automated using existing hard- and software security tools. In Section V we analyze the Security Content Automation Protocol (SCAP) and its possibilities to automate vulnerability checking, technical control compliance activities, and security measurement.

II. INFORMATION SECURITY MANAGEMENT

The information security management process is defined in ISO 27001[1]. This international standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) [2]. It adopts the "Plan-Do-Check-Act" (PDCA) process model, which is applied to structure all ISMS processes. The actions to be carried out in each phase are:

Plan: Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

Do: Implement and operate the ISMS policy, controls, processes and procedures.

Check: Assess and measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

Act: Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

In the following sections we discuss automation possibilities for risk management (Plan), security controls operation (Do), and compliance and security configuration checking (Check).

[1] There are other standards related to information security management, but ISO 27001 is widely used and constitutes a certifiable standard. That's why we use it as a reference for this paper.

III. RISK MANAGEMENT AUTOMATION

In [3] we demonstrated how the security ontology [4] can be used to automate information security risk management. The security ontology and corresponding AURUM risk management tool are briefly described in the following subsections.

A. *Security Ontology*

The security ontology [4] is based on the security relationship model presented in the National Institute of Standards and Technology Special Publication 800-12. Figure 1 shows the high-level concepts and relations of the security ontology, in which threats, vulnerabilities, controls, and their implementations are the pivotal elements. As soon as a threat exploits a physical, technical, or administrative weakness, it gives rise to follow-up threats, represents a potential danger to the organization's assets, and affects specific security attributes (e.g., confidentiality, integrity, and/or availability). We also use potential threat origins (human or natural origin) and sources (accidental or deliberate source) to describe each threat. Each vulnerability is assigned a severity value and the asset on which it could be exploited. Decision makers have to implement controls to mitigate an identified vulnerability and to protect the respective assets through preventive, corrective, deterrent, recovery, or detective measures (control type). Please see http://sec.sba-research.org for the latest security ontology version.

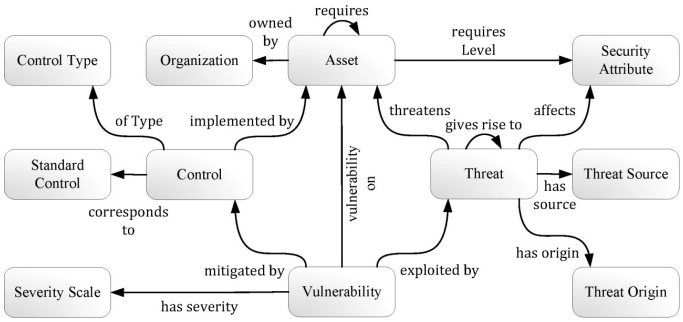

Figure 1. Security ontology - main concepts and relationships

The security ontology supports risk management automation by: (i) facilitating interoperability by providing a shared understanding of the domain in question and help to avoid heterogeneity, (ii) providing a formalization of shared understanding which allows machine processability, and (iii) allowing the reuse of information already gathered within the company. Not only can the created data be reused in future projects, independently of implemented tools, but other groups, e.g., open communities facing similar risks in the same domain or partner organizations, profit from the collected data as well.

B. *AURUM*

AURUM [3] uses the security ontology and reasoning engines to calculate current asset risk levels and to provide corresponding countermeasure implementation suggestions to decrease the risk to an acceptable level. The organization is only required to model their physical, virtual, and organizational environment in the security ontology. Based on the security ontology's threat, vulnerability, and control definitions, AURUM automatically determines which controls are fulfilled and how this influences the threat probability and subsequent risk level of business crucial assets. If the risk exceeds the acceptable level, AURUM automatically suggests appropriate controls implementations.

Compared to traditional tools, the security ontology enables AURUM to flexibly react to changed threat situations. If, for example, a new vulnerability has been identified it is only required to model it in the security ontology to reflect its existence in the risk calculation. Each security ontology control is mapped to one of the 133 ISO 27001 controls. This mapping enables AURUM to conduct automated compliance checks and to provide cost-efficient control implementation suggestions for reaching ISO 27001 compliance. Please see [5] for further details on the developed compliance calculation method.

IV. AUTOMATIC OPERATION OF SECURITY CONTROLS

After the risk assessment process and the selection of countermeasures, the information security controls have to be implemented and operated in order to mitigate the risk. ISO 27001 specifies 133 security controls, some of them are more related to human resource issues and processes, whereas others are related to technology.

In [6] we provided an analysis of how many of these controls can be automated by existing security applications that support automation in the operation of information security controls. The automatable controls and the hard- and software tools that support the automation are briefly described in the following subsections.

A. *Controls that can be automated*

A security control can be automated if the operation of the control can be done without the intervention of humans in the process. In some cases the controls can be only partially automated. The identification of controls that can be automated (partially or completely) is based on the following criteria [6]:

- The operation and monitoring of the control requires only machine-readable and -processable resources (i.e., controls such as awareness training cannot be automated as they require the training of humans)
- The control can be partially or completely implemented by at least one security application mentioned in the following sub section.

Based on these criteria, Table I shows how many ISO 27001 controls can be automated for each domain, and provides examples for these controls. The analysis results show that about 30% of the security controls can be automated. In the following section we show how existing tools can support the automation of the identified information security controls.

TABLE I. ISO 27001 CONTROLS THAT CAN BE AUTOMATED

Domain	Information Security Controls			
	Controls that can be automated	*Total controls*	*Percent*	*Examples of controls*
Security policy	0	2	0.0%	-
Organization of information security	0	11	0.0%	-
Asset management	1	5	20.0%	Inventory of assets
Human resources security	1	9	11.1%	Removal of access rights
Physical and environmental security	2	13	15.4%	Physical entry controls
Communications and operations management	15	32	46.9%	Controls against malicious code
				Information back-up
				Audit logging
Access control	13	25	52.0%	Unattended user equipment
				Network connection control
Information systems acquisition, development and maintenance	4	16	25.0%	Key management
				Control of technical vulnerabilities
Information security incident management	0	5	0.0%	-
Business continuity management	0	5	0.0%	-
Compliance	1	10	10.0%	Technical compliance checking

B. *Soft- and hardware tools*

In order to identify automatable controls, several enterprise level security soft- and hardware solutions were reviewed, especially those that allow to automate the operations of controls in a centralized way. The following soft- and hardware has been studied with regard to their potential of automating security controls [6]:

1) Microsoft: Systems Management Server (SMS) and Active Directory (AD)
2) nCircle: IP360 and Configuration Compliance Manager (CCM)
3) AlienVault: Open Source Security Information Management (OSSIM).
4) Symantec: Protection Suite Enterprise Edition (ED), NetBackup and Veritas Cluster Server (VCS).
5) PfSense.
6) APC Infrastruxure
7) VMware vSphere
8) Honeywell: NOTIFIER fire alarm systems, Access control systems and Intrusion detection systems.

It is important to clarify that the list of security applications mentioned in this paper is not exhaustive. The analysis was performed only to identify automatable controls. Please see [6] for a complete analysis of which controls can be automated by which software.

Besides each tool's automation support potential, the analysis shows that there is no single tool that supports the entire range of potentially automatable controls. Instead we need a combination of different tools to maximize security automation within organizations. Therefore, it is crucial to establish interoperability standards to support communication between different security tools. The efforts in achieving this objective will be addressed in the following section.

V. THE SECURITY CONTENT AUTOMATION PROTOCOL

The most recent work related to information security automation has focused on standardizing the format and nomenclature by which security software products communicate information about software identification, software flaws and security configurations. These efforts resulted in the definition of the Security Content Automation Protocol (SCAP). SCAP has been specified by the National Institute of Standards and Technology (US) in NIST SP 800-126 [7].

SCAP can be used in the checking phase of the information security management process in order to provide an automated way of (i) performing continuous monitoring of system security configuration settings, (ii) examining systems for signs of compromise, and (iii) having situational awareness; i.e. being able to determine the security posture of systems and the organization at any given time.

SCAP has two major elements. First, it is a protocol: a suite of open specifications that standardize the format and nomenclature by which software communicates information about software flaws and security configurations. Each specification is also known as an *SCAP component*. Second, SCAP includes software flaw and security configuration standardized reference data, also known as *SCAP content*. SCAP has several fields of application, including (i) automated checks for known vulnerabilities, (ii) automating the

verification of security configuration settings, and (iii) generating reports that link low-level settings to high-level requirements [8].

The current components of the SCAP protocol are:

- Common Platform Enumeration (CPE): nomenclature and dictionary of product names and versions.
- Common Configuration Enumeration (CCE): Nomenclature and dictionary of system configuration issues.
- Common Vulnerabilities and Exposures (CVE): Nomenclature and dictionary of security-related software flaws.
- Common Vulnerability Scoring System (CVSS): Specification for measuring the relative severity of software flaw vulnerabilities.
- Extensible Configuration Checklist Description Format (XCCDF): Language for specifying checklists and reporting checklist results.
- Open Vulnerability and Assessment Language (OVAL): Language for specifying low-level testing procedures used by checklists.

A. *Practical use of SCAP*

Organizations should use security configuration checklists that are expressed using SCAP to improve and monitor their systems' security, and to demonstrate compliance with high-level security requirements that originate from mandates, standards, and guidelines.

SCAP content is available from multiple sources. For example, the National Vulnerability Database (US) [9] hosts a dictionary of CPE entries and information on CVE entries, while the MITRE Corporation hosts an OVAL database and maintains a list of CCE entries [10]. The National Checklist Program (US) web site [11] and the Center for Internet Security (CIS) [12] are repositories for SCAP-expressed checklists. There you can find best-practice security configurations accepted for several operating systems and applications.

Organizations should also acquire and use SCAP-validated products. This protocol is gradually being adopted by security applications. At the moment of writing this paper 30 security software development companies offer SCAP validated products. A complete list of these systems can be found in [13].

VI. CONCLUSIONS

Information security management is a complex and therefore time-consuming and expensive task. Organizations face changing threat landscapes and have to address them on multiple levels. Some efforts in research and industry already concentrate on increasing the automation of some aspects in information security.

To structure and consolidate these efforts we checked which phases of the ISO 27001 process model (Plan-Do-Check-Act) can be automated. The research question was:

- How can we increase information security management automation in the context of the ISO 27001 process model?

In this paper we showed existing approaches for increasing automation in the Plan, Do, and Check phase: (i) semantic approaches such as the security ontology and the corresponding AURUM tool can be used to support the Plan phase, (ii) existing security applications can be used to automate about 30% of the 133 ISO 27001 controls in the Do phase, and (iii) the SCAP suite and its significant industry support can be used to support Check phase automation. This mapping of existing automation efforts with the different ISMS phases as defined in ISO 27001, gives an exact idea of automation possibilities in information security management and serves as a reference for security managers in order to increase the effectiveness of their ISMS. The analysis has shown that several isolated automation approaches exist. However, only by integrating these approaches organizations will be able to maximize their utility. In further research we will propose an automation framework for information security management, by studying the integration of existing approaches in this field.

REFERENCES

[1] S. Radack and R. Kuhn, "Managing Security: The Security Content Automation Protocol," *IT Professional*, 2011, p. 9–11.

[2] "ISO/IEC 27001: Information technology - Security techniques - Information security management systems – Requirements," 2005.

[3] S. Fenz, A. Ekelhart, and T. Neubauer, "Information Security Risk Management: In which security solutions is it worth investing?," *Communications of the Association for Information Systems*, vol. 28, 2011, pp. 329-356.

[4] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*, 2009, p. 183–194.

[5] S. Fenz, "Ontology-based generation of IT-security metrics," *Proceedings of the 2010 ACM Symposium on Applied Computing*, 2010, p. 1833–1839.

[6] R. Montesino and S. Fenz, "Information security automation: how far can we go?," *Sixth International Conference on Availability, Reliability and Security (ARES)*, Vienna, Austria: 2011.

[7] "NIST SP 800-126: The Technical Specification for the Security Content Automation Protocol (SCAP)," Nov. 2009.

[8] S. Quinn, K. Scarfone, M. Barrett, and C. Johnson, "NIST SP 800-117: Guide to Adopting and Using the Security Content Automation Protocol (SCAP)," Jul. 2010.

[9] "National Vulnerability Database (NVD)" Available: http://nvd.nist.gov/.

[10] "OVAL - Open Vulnerability and Assessment Language" Available: http://oval.mitre.org/.

[11] "National Checklist Program Repository" Available: http://web.nvd.nist.gov/view/ncp/repository.

[12] "Center for Internet Security (CIS)" Available: http://cisecurity.org.

[13] "Security Content Automation Protocol Validated Products" Available: http://nvd.nist.gov/scapproducts.cfm.