2011 Sixth International Conference on Availability, Reliability and Security

Information security automation: how far can we go?

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 is a very complex task which involves the implementation and monitoring of more than 130 security controls. To achieve greater efficiency in this process it is necessary to automate as many controls as possible. This paper provides an analysis of how many controls can be automated, based on the standards ISO 27001 and NIST SP800-53. Furthermore, we take the automation potential of controls included in the Consensus Audit Guidelines into account. Finally, we provide an overview of security applications that support automation in the operation of information security controls to increase the efficiency of information security management.**

Keywords - automation; security; management; standards; controls

I. INTRODUCTION

The technological advances of recent years have greatly developed the information society. Mobile communication technologies and the rapid development of the Internet enable people and enterprises to connect to each other everywhere at any time. Because of this massive interconnection, data and information systems are constantly exposed to a wide range of threats. The occurrence of disasters, operation errors and oversights, further increase the risks associated to information systems. It's therefore extremely important to run an information security management system that ensures the confidentiality, integrity and availability of business crucial data.

The management of information security is a very complex issue. If we look at the ISO 27001 standard, which is the international standard for security management, it could be seen that 133 controls have to be implemented, operated and monitored to achieve ISO 27001 compliance. If we add the facts (i) that technology advances at a great speed, (ii) that we usually have equipment from different manufacturers in our institutions, and (iii) a variety of operating systems and applications are used; then the task of security management becomes even more complicated. Taking this into account, it is extremely necessary to achieve a certain level of automation in managing information security, in order to increase the efficiency of the process.

But how far can we go in information security automation? Which approaches exist in this field? What tools or applications exist for supporting security automation?

In Section II we provide a brief overview of existing security automation efforts. In Section III this paper provides an analysis of security controls that can be automated. The analysis results are used to show how far we can automate the management of information security controls. In Section IV, we provide a brief description of some applications that can be used for automating the deployment, operation and monitoring of security controls.

II. RELATED WORK

Existing work related to information security automation is mainly focused on defining standards that allow interoperability among different applications. These efforts resulted in the definition of Security Content Automation Protocol (SCAP). Papers related to SCAP are [1], [2] and [3]. The scope of this protocol is primarily intended to patch, configuration, vulnerability and compliance management. SCAP is still under development and is gradually being adopted by security applications. At the moment of writing this paper only 30 security software development companies have SCAP validated products. A complete list of these applications can be found in [4].

On the other hand the Consensus Audit Guidelines [5] address the issue of automation by defining a group of 20 critical controls, of which 15 controls can be automated. However, the Consensus Audit Guidelines only focus on technical controls and ignore organizational security controls.

An analysis about the limits of automation in end-user security decision making and policy setting can be seen in [6]. In that paper, the authors have argued that although automation is often touted as a means to achieving better security by taking the user out of the security decision process, there are inherent limits to automation, based on human and social factors. In this case, only the information security controls related to the end-user are taken into account.

With this paper we contribute to the security automation field by analyzing the automation potential of widely used information security standards and best practice guidelines controls. Furthermore, we analyze which existing tools can be used to support the automation of these controls.

978-0-7695-4485-4/11 $26.00 © 2011 IEEE
DOI 10.1109/ARES.2011.48

III. ASSESSING THE AUTOMATION POTENTIAL OF INFORMATION SECURITY CONTROLS

Information security is not just a matter of technology; it has to consider technology, people and processes. Therefore, it is not possible to automate every aspect of information security management. To see how far it is possible to automate information security management, it's necessary to analyze globally accepted standards, which specify the security controls that must be implemented to ensure confidentiality, integrity and availability of information. Among the best known standards and publications on this topic we have the following:

- ISO 27001: it is the most widely accepted standard worldwide, which is certifiable and defines an information security management system. The security management is defined as a cyclic process where it's necessary to deploy, operate, monitor and verify 133 security controls.
- NIST SP 800-53: it is a publication of the well known National Institute of Standards and Technology (US), which specifies a set of 198 recommended security controls. This publication is used in practice mainly in the United States where federal institutions take it as a reference standard.
- Consensus Audit Guidelines - twenty critical controls for effective cyber defense: this publication involves a large number of security experts that established a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms. The consensus effort that has produced this document has identified 20 specific technical security controls that are viewed as effective in blocking currently known high-priority attacks.

For the purpose of this paper 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:

- 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 Section IV.

In the following subsections we analyze the controls of two information security standards and one best practice guideline, and check which controls can be automated.

A. ISO 27001

ISO 27001 specifies in Annex A [7] 133 security controls. These controls are divided into 11 domains, some of them are more related to human resource issues and processes, and others are related to technology. Based on the criteria defined in Section III, Table 1 shows how many controls can be automated for each domain, and provides examples for these 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	-
Organization of information security	0	11	0	-
Asset management	1	5	20%	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%	Unattended user equipment
				Network connection control
Information systems acquisition, development and maintenance	4	16	25%	Key management
				Control of technical vulnerabilities
Information security incident management	0	5	0	-
Business continuity management	0	5	0	-
Compliance	1	10	10%	Technical compliance checking

Based on our analysis and the criteria defined in Section III, 37 controls can be automated, which represent a 27.8% of the total of security controls that are defined in the ISO 27001 standard.

B. NIST SP 800-53

A similar analysis can be done for the NIST SP 800-53 standard [8], which recommends a total of 198 security controls. The controls are divided into 18 families and are classified in three general classes: technical, operational and management. Based on the criteria defined in Section III, Table II shows how many controls can be automated for each family, and provides examples for these controls.

As it can be seen there are 62 controls that can be automated, which represent a 31.3% of the total of security controls that are defined in the NIST SP 800-53 standard. Fig. 1 shows the automation potential of each information security area.

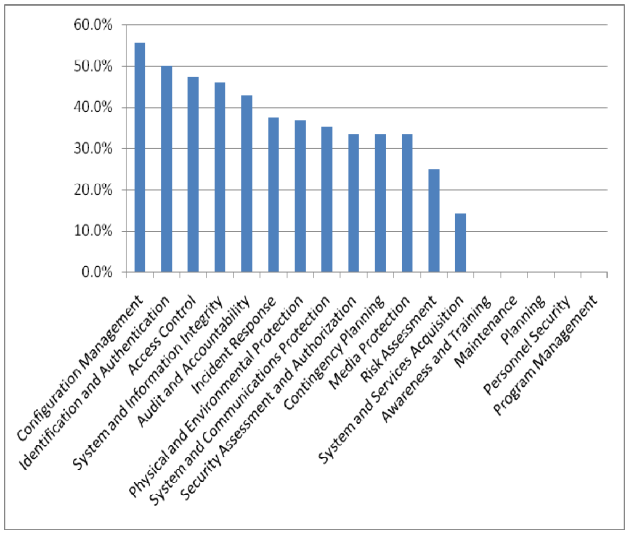

Figure 1. Percent of automatable controls in the different families of NIST SP 800-53.

TABLE II. NIST SP 800-53 CONTROLS THAT CAN BE AUTOMATED

Family	**Information Security Controls**			
	Controls that can be automated	***Total controls***	***Percent***	***Examples of controls***
Access Control (AC)	9	19	47.4%	AC-7 Unsuccessful login attempts
Awareness and Training (AT)	0	5	0	-
Audit and Accountability (AU)	6	14	42.9%	AU-6 Audit review, analysis, and reporting
Security Assessment and Authorization (CA)	2	6	33.3%	CA-7 Continuous monitoring
Configuration Management (CM)	5	9	55.6%	CM-2 Baseline configuration
Contingency Planning (CP)	3	9	33.3%	CP-9 Information system backup
Identification and Authentication (IA)	4	8	50.0%	IA-5 Authenticator management
Incident Response (IR)	3	8	37.5%	IR-4 Incident handling
Maintenance (MA)	0	6	0	-
Media Protection (MP)	2	6	33.3%	MP-2 Media access
Physical and Environmental Protection (PE)	7	19	36.8%	PE-6 Monitoring physical access
Planning (PL)	0	5	0	-
Personnel Security (PS)	0	8	0	-
Risk Assessment (RA)	1	4	25.0%	RA-5 Vulnerability scanning
System and Services Acquisition (SA)	2	14	14.3%	SA-7 User-installed software
System and Communications Protection (SC)	12	34	35.3%	SC-5 Denial of service protection
System and Information Integrity (SI)	6	13	46.1%	SI-4 Information system monitoring
Program Management (PM)	0	11	0	-

C. Consensus Audit Guidelines

The publication "Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines" contains 20 specific technical security controls that are viewed as effective in blocking currently known high-priority attacks.

According to the Consensus Audit Guidelines, 15 of the controls that are recommended can be managed, at least in part, in an automatic way; and many of these controls can be implemented and measured using existing tools found in many enterprises. Other controls can be fulfilled using commercial or, in some cases, free, open-source software [5].

It can also be seen that the 20 critical controls map directly to about one third of the priority one (P1) controls identified in NIST SP 800-53. The authors state that these controls are the most critical subset of the NIST SP 800-53 control catalog. The controls that are subject to automated collection, measurement and validation are the following:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

A complete mapping for each of the 20 Critical Controls to the specific set of 800-53 controls is included in Appendix A of the Consensus Audit Guidelines. The 15 automatable controls map directly to 56 controls of the NIST SP 800-53 standard, which represents a 28.3% of the total number of security controls.

Our overall analysis results show that about 30% of the security controls included in ISO 27001 and NIST SP 800-53 can be automated. In the following section we show how existing tools can support the automation of the identified information security controls.

IV. Soft- and Hardware for Security Automation

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:

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). The following components were taken into account: Snort, OCS, OSSEC, Ntop, NAGIOS, OpenVAS, Nmap.
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 systems, Access control systems and Intrusion detection systems.

Table III shows how many controls of the NIST SP 800-53 standard can be automated by using the listed security tools. Column 1 of Table III refers to the NIST SP 800-53 control family (see Table II for the full family name). For each security tool and each NIST SP 800-53 control, we evaluated if it can be used to automate the operation of the control.

TABLE III. Matrix of automatable controls vs. existing hard- and software

Family	Hard- and Software Tools							
	Microsoft SMS&AD	***nCircle IP360&CCM***	***OSSIM***	***Symantec Protection Suite ED, Netbackup and VCS***	***pfSense***	***APC Infrastruxure***	***VMware vSphere***	***Honeywell***
AC	8	1	-	-	3	-	-	-
AU	1	-	5	-	1	-	-	-
CA	-	2	1	-	-	-	1	-
CM	4	4	1	-	-	-	-	-
CP	-	-	-	3	-	-	3	-
IA	4	1	-	-	-	-	-	-
IR	-	-	3	-	-	-	-	-

Family	Hard- and Software Tools							
	Microsoft SMS&AD	*nCircle IP360&CCM*	*OSSIM*	*Symantec Protection Suite ED, Netbackup and VCS*	*pfSense*	*APC Infrastruxure*	*VMware vSphere*	*Honeywell*
MP	-	-	-	2	-	-	-	-
PE	-	-	-	-	-	2	-	5
RA	-	1	1	-	-	-	-	-
SA	1	2	-	-	-	-	-	-
SC	5	1	3	-	6	-	1	-
SI	1	3	5	3	-	-	1	-
∑	**24**	**15**	**19**	**8**	**10**	**2**	**6**	**5**

The following examples show how the tools can be used to automate three exemplary controls:

1. Control ISO 27001 A.7.1.1: Inventory of assets

Control: All assets should be clearly identified and an inventory of all important assets drawn up and maintained.

Implementation guidance: An organization should identify all assets and document the importance of these assets. The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The inventory should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned. In addition, ownership and information classification should be agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets should be identified [9].

Automation solution: The software nCircle IP360 can be used to produce an automated, complete inventory of systems on the network. This application scans any IP-enabled device, including servers, desktops, laptops, routers, switches, printers, voice over IP telephones and firewalls. nCircle IP360 has the capabilities of using multiple ways of correlating hosts across scans, including IP address, MAC address, host name, stack fingerprinting, open port fingerprinting, and NetBIOS name. This optimizes the ability to track a host over time and identify new hardware on the network [10].

2. Control NIST SP 800-53 AU-6: Audit review, analysis, and reporting

Control: The organization:

a. Reviews and analyzes information system audit records for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information [8].

Automation solution: The OSSIM solution provides continuous collection, correlation and analysis of events from multiple, distinct data sources (e.g. audit and services logs, network traffic, IDS data), which it analyzes, prioritizes or rules out as a possible attack. Its correlation engine tracks complex patterns and includes in its analysis all the variables that define the attack context: vulnerability type, degree of anomaly, network status, service availability and inventory, and value of the equipment and assets involved. OSSIM includes a powerful reporting system where reports are generated based on all the information collected. The reports may include both historical and real time information. Users can create their own report including only those sub-reports that are of interest in terms of the user profile and the needs of the institution that is being monitored [11].

3. Control NIST SP 800-53 CP-9: Information system backup

Control: The organization:

a. Conducts backups of user-level information contained in the information system;
b. Conducts backups of system-level information contained in the information system;
c. Conducts backups of information system documentation including security-related documentation; and
d. Protects the confidentiality and integrity of backup information at the storage location [8].

Automation solution: Symantec NetBackup provides data protection for enterprise backup and recovery environments. It minimizes cost and complexity by implementing a unified data protection solution that provides desktop, remote office and data center protection across the entire enterprise. NetBackup delivers centralized and simplified real-time management to help organizations to manage all aspects of backup and recovery including disk- and tape-based data

protection. It also provides advanced and automated disaster recovery on various platforms, and granular recovery of critical applications. It offers a broad range of options to optimize backup and recovery and support for all major operating platforms [12].

Besides each tool's automation support potential, Table III also 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 efficient communication between different security tools.

It is important to clarify that the purpose of this paper is not to assess the quality of the security applications. The analysis was performed only to identify automatable controls and the applications have been used to support our selection of automatable security controls. The list of security applications mentioned in this paper is not exhaustive.

V. CONCLUSIONS

Information security management is a very complex and therefore expensive issue. While small- and medium-sized organizations do not have the financial resources to run appropriate information security programs, bigger organizations face an increasing complexity of their IT landscape. Security automation would decrease the human intervention and therefore the costs and complexity of security activities. Therefore, the research questions of this paper were:

- How far can we go in information security automation?
- What tools or applications exist for supporting security automation?

By analyzing three widely used information security standards and best practice guidelines, we showed that about 30% of the security controls included in ISO 27001 and NIST SP 800-53 can be automated by existing tools.

We analyzed several existing security tools regarding their potential to automate the security controls of the analyzed standards. The analysis has shown that no single tool exploits the full security control automation potential. Instead a combination of different tools is required to achieve the maximum automation degree (about 30% of all controls).

In this paper we focused on automating the operation and monitoring of controls. In further research we will analyze which further activities (e.g. planning and reviewing) of the information security management process can be automated.

REFERENCES

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

[2] R.A. Martin, "Making security measurable and manageable," *Military Communications Conference, 2008. MILCOM 2008. IEEE*, 2009, p. 1–9.

[3] B. Potter, "Security automation," *Network Security*, vol. 2007, 2007, pp. 18-19.

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

[5] "Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines," 2009.

[6] W.K. Edwards, E.S. Poole, and J. Stoll, "Security automation considered harmful?," *Proceedings of the 2007 Workshop on New Security Paradigms*, 2008, p. 33–42.

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

[8] "NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations," 2009.

[9] "ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management," 2005.

[10] "Vulnerability Management & Compliance Audit Solutions | nCircle" Available: http://www.ncircle.com/.

[11] "Open Source Security Information Management" Available: http://www.ossim.net.

[12] "Data Recovery Software | Symantec" Available: http://www.symantec.com/business/netbackup.