

NISTIR 8011
Volume 1

Automation Support for Security Control Assessments

Volume 1: Overview

Kelley Dempsey
Paul Eavy
George Moore

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8011-1>



NISTIR 8011
Volume 1

Automation Support for Security Control Assessments

Volume 1: Overview

Kelley Dempsey
*Computer Security Division
Information Technology Laboratory*

Paul Eavy
*Federal Network Resilience Division
Department of Homeland Security*

George Moore
*Johns Hopkins University
Applied Physics Laboratory*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8011-1>

June 2017



U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency Report 8011, Volume 1
93 pages (June 2017)

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8011-1>

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST information security publications, other than the ones noted above, are available at <http://csrc.nist.gov/publications>.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sec-cert@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal systems.

Abstract

This volume introduces concepts to support automated assessment of most of the security controls in NIST Special Publication (SP) 800-53. Referencing SP 800-53A, the controls are divided into more granular parts (determination statements) to be assessed. The parts of the control assessed by each determination statement are called control items. The control items are then grouped into the appropriate security capabilities. As suggested by SP 800-53 Revision 4, *security capabilities* are groups of controls that support a common purpose. For effective automated assessment, testable *defect checks* are defined that bridge the determination statements to the broader security capabilities to be achieved and to the SP 800-53 security control items themselves. The defect checks correspond to security sub-capabilities—called sub-capabilities because each is part of a larger capability. Capabilities and sub-capabilities are both designed with the purpose of addressing a series of attack steps. Automated assessments (in the form of defect checks) are performed using the test assessment method defined in SP 800-53A by comparing a desired and actual state (or behavior).

Keywords

actual state; assessment; assessment boundary; assessment method; authorization boundary; automated security control assessment; automation; capability; continuous diagnostics and mitigation; information security continuous monitoring; dashboard; defect; defect check; desired state specification; ISCM dashboard; mitigation; ongoing assessment; root cause analysis; security automation; security capability; security control; security control assessment; security control item.

Acknowledgments

The authors, Kelley Dempsey of the National Institute of Standards and Technology (NIST), Dr. George Moore of the Applied Physics Laboratory at Johns Hopkins University, and Paul Eavy of the Department of Homeland Security, wish to thank their colleagues who reviewed drafts of this document, including Nadya Bartol, Craig Chase, Ann Dixon, Terry Fletcher, Jim Foti, Susan Hansche, Amy Heydman, Alicia Jones, Betsy Kulick, Elizabeth Lennon, Susan Pagan, Daniel Portwood, Ron Ross, Martin Stanley, Kevin Stine, Robin Walker, David Waltermire, Kimberly Watson, and Jim Wiggins. The authors also gratefully acknowledge and appreciate the comments and contributions made by government agencies, private organizations, and individuals in providing direction and assistance in the development of this document.

Table of Contents

Executive Summary	ix
1. Introduction.....	1
<i>1.1 Purpose and Scope.....</i>	<i>1</i>
<i>1.2 Target Audience.....</i>	<i>2</i>
<i>1.3 Organization of Volume 1</i>	<i>3</i>
2. Overview of an Automated Security Control Assessment Process	4
<i>2.1 Prerequisites to Automated Security Control Assessment.....</i>	<i>4</i>
<i>2.2 Automating the Test Assessment Method.....</i>	<i>5</i>
<i>2.2.1 Terms for Referring to Assessment Objects.....</i>	<i>6</i>
<i>2.3 Factors for Determining When to Trust Automated Ongoing Assessments</i>	<i>6</i>
<i>2.4 An Automated Security Control Assessment Program: ISCM.....</i>	<i>7</i>
<i>2.5 Preparing for Automated Security Control Assessments.....</i>	<i>9</i>
3. Focusing Security Control Assessments on Security Results.....	10
<i>3.1 Applying Security Capabilities to Automated Assessments</i>	<i>11</i>
<i>3.1.1 Supports Strong Systems Engineering of Security Capabilities</i>	<i>11</i>
<i>3.1.2 Supports Guidance for Control Selection</i>	<i>11</i>
<i>3.1.3 Simplifies Understanding of the Overall Protection Process</i>	<i>12</i>
<i>3.1.4 Enables Assessment of Security Results at a Higher Level than Individual Controls....</i>	<i>12</i>
<i>3.1.5 Improves Risk Management by Measuring Security Results More Closely Aligned with Desired Business Results.....</i>	<i>12</i>
<i>3.2 Attack Steps.....</i>	<i>13</i>
<i>3.2.1 Adversarial Attack Step Model</i>	<i>14</i>
<i>3.3 Security Capabilities.....</i>	<i>17</i>
<i>3.3.1 SP 800-53 Control Families and Security Capabilities.....</i>	<i>17</i>
<i>3.3.2 SP 800-137 Security Automation Domains and Security Capabilities.....</i>	<i>17</i>
<i>3.3.3 Using Security Capabilities in Security Control Assessment</i>	<i>18</i>
<i>3.3.4 Security Capabilities and ISCM.....</i>	<i>18</i>
<i>3.3.5 Example Security Capabilities Listed and Defined</i>	<i>18</i>

3.3.6 <i>Tracing Requirements: Mapping Capability to Attack Steps</i>	23
3.3.7 <i>Organization-Defined Security Capabilities</i>	23
3.4 <i>Sub-Capabilities</i>	24
3.4.1 <i>Examples of Sub-Capabilities (from HWAM)</i>	24
3.4.2 <i>Tracing Sub-Capabilities to Attack Steps</i>	26
3.5 <i>Security Control Items</i>	26
3.5.1 <i>Tracing Security Control Items to Attack Steps</i>	26
3.5.2 <i>Tracing Security Control Items to Capabilities</i>	27
3.5.3 <i>Tracing Security Control Items to Sub-Capabilities</i>	29
3.6 <i>Synergies Across Each Abstraction Level</i>	29
3.6.1 <i>Multiple Capabilities Support Addressing Each Attack Step</i>	29
3.6.2 <i>Many Controls Support Multiple Capabilities</i>	30
4. Using Actual State and Desired State Specification to Detect Defects	32
4.1 <i>Actual State and Desired State Specification</i>	32
4.2 <i>Collectors and the Collection System</i>	32
4.2.1 <i>Actual State Collectors</i>	32
4.2.2 <i>Collection of Desired State Specifications</i>	32
4.2.3 <i>The Collection System</i>	33
4.3 <i>Authorization Boundary and Assessment Boundary</i>	34
4.3.1 <i>System Authorization Boundary</i>	35
4.3.2 <i>ISCM Assessment Boundary</i>	35
4.3.3 <i>Tracing System Risk to its Sources</i>	37
4.4 <i>The Desired State Specification</i>	38
4.4.1 <i>Types of Desired State Specifications</i>	39
4.4.2 <i>Desired State Specification Reflects Policy</i>	40
4.4.3 <i>Desired State Specification Demonstrates the Existence of Policy</i>	40
4.5 <i>Using Automation to Compare Actual State and Desired State Specification</i>	41
5. Defect Checks	42
5.1 <i>Defect Checks and Determination Statements</i>	42
5.2 <i>Interpreting Defect Checks as Tests of Control Items</i>	43
5.3 <i>Interpreting Defect Checks as Tests of Sub-Capabilities and Control Items</i>	43

<i>5.4 Defect Check Documentation</i>	47
<i>5.5 Data Quality Measures.....</i>	49
<i>5.6 Assessment Criteria Device Groupings to Consider</i>	49
<i>5.7 Why Not Call Defects Vulnerabilities or Weaknesses?</i>	50
<i>5.8 Security Controls Selected/Not Selected and Defect Checks.....</i>	50
<i>5.9 Foundational and Local Defect Checks.....</i>	51
<i>5.10 Documenting Tailoring Decisions</i>	52
6. Assessment Plan Documentation	53
<i>6.1 Introduction to Security Assessment Plan Narratives</i>	53
<i>6.2 Assessment Scope.....</i>	54
<i>6.3 Determination Statements within the Narratives.....</i>	55
<i>6.4 Roles and Assessment Methods in the Narratives</i>	55
<i>6.5 Defect Check Rationale Table</i>	56
<i>6.6 Tailoring of Security Assessment Plan Narratives</i>	56
<i>6.7 Control Allocation Tables.....</i>	57
<i>6.8 Documenting Selected Controls and Tailoring Decisions.....</i>	58
7. Root Cause Analysis	60
<i>7.1 Knowing Who Is Responsible</i>	60
<i>7.2 Root Cause Analysis</i>	60
<i>7.2.1 Root Cause Analysis How-to: Controls</i>	61
<i>7.2.2 Root Cause Analysis How-to: Defect Types</i>	62
8. Roles and Responsibilities	66
<i>8.1 SP 800-37-Defined Management Responsibilities</i>	66
<i>8.2 ISCM Operational Responsibilities</i>	66
9. Relationship of Automated Security Control Assessment to the NIST Risk Management Framework	69
<i>9.1 Linking ISCM to Specific RMF Assessment Tasks.....</i>	69
Appendix A. References	A-1
Appendix B. Glossary	B-1
Appendix C. Acronyms and Abbreviations.....	C-1

List of Figures

Figure 1: Overview of an Automated Security Control Assessment Process.....	8
Figure 2: Attack Step Model.....	14
Figure 3: ISCM Security Capabilities Used in this NISTIR.....	19
Figure 4: Capabilities Work Together to Block Attack Steps	30
Figure 5: ISCM Collection System.....	34
Figure 6: Focus of Defect Checks and Determination Statements	44
Figure 7: Example of a Security Assessment Plan Narrative	54
Figure 8: Flow of Cause and Effect from Control Items to Security Results	61

List of Tables

Table 1: SP 800-53A Assessment Methods	5
Table 2: Descriptions of the Attack Steps.....	15
Table 3: ISCM Security Capabilities	20
Table 4: Tracing the HWAM Capability to Blocking Attack Steps	23
Table 5: Selected Examples of Sub-Capabilities (HWAM)	25
Table 6: Example of Tracing HWAM Security Control Items to Attack Steps	27
Table 7: Illustrative Keyword Rules to Map to Capabilities	28
Table 8: Tracing Control Items to the HWAM Capability (EXAMPLE)	28
Table 9: Tracing Control Items to the Sub-Capabilities: Selected Examples for the Prevent Authorized Devices without a Device Manager Sub-Capability	29
Table 10: Example of a Control Item Supporting Multiple Capabilities.....	31
Table 11: Types of Desired State Specifications	39
Table 12: Equivalence of Prohibited and Desired State Specification – An Example	39
Table 13: Example Control and Determination Statements	42
Table 14: Sensitivity and Specificity Notes.....	45
Table 15: Sample Rows from a Hypothetical Sub-Capability and Defect Check Description ^a	47
Table 16: Data Quality Measures	49
Table 17: Example of a Control Item and Its Determination Statements	55
Table 18: Control Allocation Table Column Explanations	58
Table 19: Notional Control Allocation Table – Example	59
Table 20: Notional Way to Look up Controls Tested by a Defect Check	64
Table 21: Impact Scenarios/Impact Analysis	65
Table 22: SO and SSO Responsibilities.....	66
Table 23: Notional Example of ISCM Operational Roles for HWAM	67