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

National Institute of Standards and Technology
U.S. Department of Commerce

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

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

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

List of Figures

List of Tables