Standards Based Security Testing

Claire L. Lohr, CSQE, CSDP, CTAL
clohr@computer.org

F. Scot Anderson, CISSP
scot@securixx.com

Topics

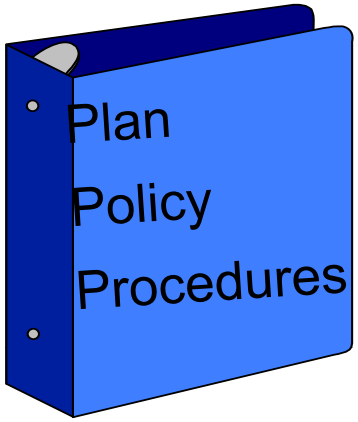
- Why use standards?
- Secure systems' component parts (1st level taxonomy)
- Available types of testing (taxonomy)
- Security requirements standards (for validation test)
- Security test standards (final, draft, planned, and guidelines)
- Relevant traditional standards
- Tracing from the standards to the taxonomies
- How to use this information
- ?'s

Why Use Standards?

- Impress stakeholders
  - Some require it
  - “Outside” authority
- Built by consensus
  - Balanced perspectives
  - Expensive consulting advice virtually for free
  - Mitigation of risk by including the perspectives of many vs. just one opinion
- If stakeholders permit, only use what is relevant

Secure Systems' Component Parts

1. ISMS Processes

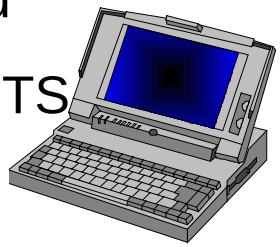


2. Software

- Custom
- COTS/GOTS

3. Hardware

- Developed
- COTS/GOTS



4. Site

5. Human resources

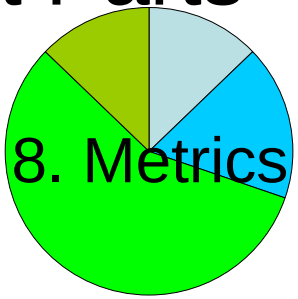
- Developers
- Assessors
- Operations
- Users
- Consultants (SMEs)

6. Data (information)

- Stored
- Transmitted

7. Communications

- Developed
- COTS/GOTS



9. Risk Mgm't

10. Training

11. Containment

- Disaster recovery
- COOP

12. Industry specific

- Government (C&A)
- Telecom
- Healthcare
- Financial services

Types of Testing

1. Static

1.1 Reviews
- 1.1.1 Code (including tool scans)
- 1.1.2 Design
- 1.1.3 Requirements
  - 1.1.3.1 Functional
  - 1.1.3.2 Non-functional
- 1.1.4 Security documentation
- 1.1.5 Retention of log data

1.2 Tracing (verification)

1.3 Audits
- 1.3.1 Credentials of individuals
- 1.3.2 Security procedure implementation

3. Vulnerability Assessment (for certification and accreditation)

3.1 Internal

3.2 External

2. Dynamic

2.1 Verification
- 2.1.1 Unit
- 2.1.2 Integration
- 2.1.3 System

2.2 Validation
- 2.2.1 System
- 2.2.2 Integrated systems
- 2.2.3 Penetration testing
  - 2.2.3.1 Overt
  - 2.2.3.2 Covert

Security Requirements

R1. ISO/IEC

27000 series

R1.1 ISO/IEC 27000 DRAFT Information technology -- Security techniques -- Information security management systems --Overview and vocabulary

R1.2 ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

R1.3 ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management

R1.4 ISO/IEC 27003 Information technology — Security techniques — Information security management system implementation guidance

R1.5 ISO/IEC 27004 Information technology — Security techniques — Information security management measurement

R1.6 ISO/IEC 27005 Information technology — Security techniques — Information security risk management

R1.7 ISO/IEC 27006 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

R1.8 ISO/IEC 27007 Information technology — Security techniques — Guidelines for information security management systems auditing

R1.9 ISO/IEC 27011 Information technology — Security techniques — Information security management guidelines for Telecommunications

Security Requirements

R1. ISO/IEC

Adoption and evolution of the Common Criteria

R1.10 ISO/IEC 15408-1 Information technology — Security techniques - Evaluation Criteria for IT Security - PART 1: Introduction and general model

R1.11 ISO/IEC 15408-2 Information technology — Security techniques — Evaluation Criteria for IT Security - PART 2: Security Functional Components

R1.12 ISO/IEC Information technology — Security techniques - Evaluation Criteria for IT Security - PART 3: Security Assurance Components

Security Requirements

R2. Common Criteria www.commoncriteriaportal.org (see ISO 15408 series and 18045) *free*

Basic

- R2.1 Part 1: Introduction and general model
- R2.2 Part 2: Security functional requirements
- R2.3 Part 3: Security assurance requirements

Supporting

- For Smart Cards or similar devices
  - R2.4 Guidance
  - R2.5 Mandatory requirements
- For maintenance and re-evaluation
  - R2.6 Reuse of Evaluation Results and Evidence
  - R2.7 Assurance continuity
- R2.8 Sanitizing reports for publication
- R2.9 Integrated circuits
- R2.10 (Development) site certification

Evaluations (see ISO 18045)

- R2.11 CEM (Common Evaluation Methodology) v3.1

Security Requirements

R3. OWASP *free*

R3.1 OWASP Guide to Building Secure Web Applications v2 (v3 Draft available)

R3.2 OWASP CLASP (Comprehensive, Lightweight Application Security Process)

R4. Build Security In *free* www.buildsecurityin.us-cert.gov

R4.1 Enhancing the Development Life Cycle to Produce Secure Software Version 2.0

R4.2 Many articles

R5. DIACAP www.diacap.net *free*

R5.1 DoD Instruction 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP)

Security Requirements

R6. NIST www.nist.gov *free* FISMA

R6.1 SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems

R6.2 SP 800-39 (Draft) Managing Risk from Information Systems: An Organizational Perspective

R6.3 SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems

R6.4 SP 800-30 Risk Management Guide for Information Technology Systems

R6.5 SP 800-18 Guide for Developing Security Plans for Federal Information Systems

Security Requirements

R7. HIPPA http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/index.html

R7.1 Privacy and Security Framework (numerous documents)

R8. Sarbanes-Oxley http://sec.gov/spotlight/sarbanes-oxley.htm

R8.1 numerous documents

R9. NSA www.nsa.gov *free*

R9.1 Net Centric Enterprise Services (NCES)

R9.2 NSTISSAM TEMPEST/1-92, Compromising Emanations Laboratory Test Standard, Electromagnetics

R10. NIACAP http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf *free*

R10.1 National Information Assurance Certification and Accreditation Process (NIACAP)

Security Requirements

R11. Certification of professionals

- R11.1 www.cissp.com security
- R11.2 www.isaca.org security and governance
- R11.3 www.giac.org security
- R11.4 www.astqb.org testing
- R11.5 IEEE CSDP http://www2.computer.org/portal/web/getcertified development

R12. IEEE supporting standards www.ieee.org

- R12.1 IEEE Std 830™-1998 IEEE Recommended Practice for Software Requirements Specifications
- R12.2 IEEE Std 1540™-2001 (see ISO 16085-2006) IEEE Standard for Software Life Cycle Processes—Risk Management
- R12.3 IEEE Std 828™-2005 IEEE Standard for Software Configuration Management
- R12.4 IEEE Std 982.1™-2005 IEEE Standard Dictionary of Measures of the Software Aspects of Dependability

Security Requirements

R13. ISO supporting standards

- R13.1 ISO/IEC 15026 Information technology - system and software integrity levels
- R13.2 ISO/IEC 15939 Systems and software engineering - measurement process
- R13.3 ISO/IEC 16085 Systems and software engineering - life cycle processes - risk management
- R13.4 ISO/IEC 12207:2008 Systems and software engineering--Software life cycle processes

Security Requirements

Secure System Components	Standards for Requirements
1. ISMS processes	R1.1 R1.2 R1.3 R1.4
2. Software	R1.11
2.1 Developed	R3.1 R3.2 R4.1
2.2 COTS/GOTS	T2.1

Full tables available from web site (forward and backward tracing)

Security Requirements

Standard	Requirements	Testing
R1. ISO 27000 series		
R1.2 ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements	1. ISMS processes	**1. Static** (section A.12.5.2) technical review after changes **1.1 Reviews** (section A.12.5.2) review of applications after operating system changes **1.1.4 Security documentation (review)** (section 4.2.3 d)) review risk assessments (section 4.3.2) review documents **1.3 Audits** (section 10.6.2) audit security of network services (section 12.3.1) audit of key management **1.3.1 Credentials of individuals** (section A.8.1.2) verification of background checks

Security Test Standards

S1. NIST www.nist.gov

S1.1 SP 800-115 Technical Guide to Information Security Testing and Assessment

S1.2 SP 800-84 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

S1.3 SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems

S2. OWASP www.owasp.org

S2.1 OWASP Testing Guide V 3.0

S2.2 OWASP Code Review Guide V1.1

S3. ISO

S3.1 ISO/IEC 18045 Information technology — Security techniques - Methodology for IT security evaluation

S4. ISECOM www.isecom.org *free*

S4.1 OSSTMM - Open Source Security Testing Methodology Manual

Security Test Standards

S5. NSA www.nsa.gov *free*

S5.1 Certified TEMPEST Test Services List (CTTSL)

S6. Build Security In *free* www.buildsecurityin.us-cert.gov *free*

S6.1 (also R4.1) Enhancing the Development Life Cycle to Produce Secure Software Version 2.0 (Chapter 8)

S6.2 Code analysis (article)

S6.3 Many articles

S7. DISA www.iase.disa.mil *free*

S7.1 Gold Disk Version 2 (tools; only available for military)

S7.2 Gold Disk User Guide Basic Operations Version 2.0

Security Test Standards

Types of Testing	Standards for Test
1. Static	R1.2 (section A.12.5.2) technical review after operating system changes R1.3 (section 10.1.2) testing of changes (section 12.5.2) technical review after operating system changes S6.3
1.1 Reviews	R1.2 (section A.12.5.2) review of applications after operating system changes R1.3 (section 6.2.3) due diligence reviews of third party agreements (section 7.1.2) review asset access restrictions (section 12.5.1) reviewing changes (section 12.5.2) review after operating system changes R1.12 (section 10.6) evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (section 10.9) evaluation assurance level 7 (EAL7) - formally verified design and tested (section 18.2.6) analysis (of documentation) and testing for insecure states T1.4

Traditional Test Standards

T1. IEEE www.ieee.org

- T1.1 Std 829™-2008 IEEE Standard for Software and System Test Documentation
- T1.2 Std 1012™-2004 IEEE Standard for Software Verification and Validation
- T1.3 Std 1008™-1987 IEEE Standard for Software Unit Testing
- T1.4 Std 1028™-2008 IEEE Standard for Software Reviews and Audits
- T1.5 IEEE Std 1044™-1993 IEEE Standard Classification for Software Anomalies

T2. ISO

- T2.1 ISO/IEC 12119:1994 Packages: Requirements/Testing
- T2.2 ISO 29119 Part 1: Software Testing Concepts
- T2.2 ISO 29119 Part 2: Test Process
- T2.3 ISO 29119 Part 3: Test Documentation
- T2.4 ISO 29119 Part 4: Test Techniques

How to Use This Information

1. Download presentation and tables from www.ivvgroup.org
2. Choose either a requirements or test topic
3. Look up the relevant standards
4. Provide feedback for improvement

Obtain Updates Online

This presentation is available online (and will continue to be updated) at:

www.ivvgroup.com

Please provide feedback to:

clohr@computer.org

Questions?

Biographies of the Authors

Claire Lohr, CSQE, CSDP, CTFL, CTAL

Ms. Lohr has been an active professional in the computer field for 40 years, with the last twenty years focused on Software Process Improvement. She has provided these services to notable firms such as GTE, Motorola, Westinghouse, SAIC, MITRE, Boeing, the American Red Cross, Aetna, Dowty Controls (England), and Europe Combined Terminals (Holland). Ms. Lohr currently provides training and consulting services for both Government and commercial clients. She chaired the IEEE Std 829-2008 Working Group, and has served on both the IEEE Computer Society's Software and Systems Engineering Standards Committee (S2ESC) and the IEEE Computer Society's Standards Advisory Board (SAB; as Vitality Chair). Ms. Lohr obtained her degree in Engineering at Case Institute of Technology in 1968.

F. Scot Anderson, CISSP

A 27-year seasoned executive, senior manager, entrepreneur, and systems developer, Mr. Anderson is an Information Security subject matter practitioner and expert since 1993, including penetration and vulnerability testing, C&A, policy and implementation documentation. He is also a BSI trained ISO 27001 Lead Auditor, with extensive experience in ITIL, ISO, NIST, FIPS standards, DIACAP C&A, FISMA, Sarbanes Oxley, and CMM principles and standards. He develops and deploys infrastructure architectures to provide and enhance FISMA reporting capabilities. He is an articulate contributor providing instruction, publication (IEEE) and documentation.

Acronyms

ASTQB American Software Testing Qualifications Board
CEM (Common Evaluation Methodology
CISSP Certified Information Security Systems Professional
COOP Continuity of Operations
COTS Commercial Off The Shelf
CSDP Certified Software Development Professional
CTTSL Certified TEMPEST Test Services List
DIACAP DoD Information Assurance Certification and Accreditation Process
DISA Defense Information Systems Agency
FISMA Federal Information Security Management Act
GIAC Global Information Assurance Certification
GOTS Government Off The Shelf
HIPPA Health Insurance Portability and Accountability Act

Acronyms (continued)

IEC International Electrotechnical Commission
IEEE Institute of Electrical and Electronics Engineers
ISACA Information Systems Audit and Control Association
ISO International Organization for Standardization
NIACAP National Information Assurance Certification and Accreditation Process
NIST National Institute for Standards and Technology
NSA National Security Agency
OWASP Open Web Application Security Project
SME Subject Matter Expert
TEMPEST (not an acronym)