Assurance Cases

Robert A. Martin
Sean Barnum

May 2011
### Assurance Cases

**Report Documentation Page**

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

<table>
<thead>
<tr>
<th>1. REPORT DATE</th>
<th>MAY 2011</th>
<th>2. REPORT TYPE</th>
<th>3. DATES COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>00-00-2011 to 00-00-2011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
<th>Assurance Cases</th>
<th>5a. CONTRACT NUMBER</th>
<th>5b. GRANT NUMBER</th>
<th>5c. PROGRAM ELEMENT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
<th></th>
<th>5d. PROJECT NUMBER</th>
<th>5e. TASK NUMBER</th>
<th>5f. WORK UNIT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</th>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitre Corporation, 202 Burlington Rd, Bedford, MA, 01730-1420</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</th>
<th>10. SPONSOR/MONITOR’S ACRONYM(S)</th>
<th>11. SPONSOR/MONITOR’S REPORT NUMBER(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

Approved for public release; distribution unlimited

**13. SUPPLEMENTARY NOTES**

Presented at the 23rd Systems and Software Technology Conference (SSTC), 16-19 May 2011, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License

**14. ABSTRACT**

**15. SUBJECT TERMS**

**16. SECURITY CLASSIFICATION OF:**

<table>
<thead>
<tr>
<th>a. REPORT</th>
<th>b. ABSTRACT</th>
<th>c. THIS PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

**17. LIMITATION OF ABSTRACT**

Same as Report (SAR)

**18. NUMBER OF PAGES**

21

**19a. NAME OF RESPONSIBLE PERSON**

Approved for public release; distribution unlimited

Standard Form 298 (Rev. 8-98)

Prescribed by ANSI Std Z39-18
Agenda

8:00-8:45am  Software Security Knowledge about Applications Weaknesses

9:00-9:45am  Software Security Knowledge about Attack Patterns Against Applications
              Training in Software Security

10:15-11:00am  Software Security Practice

11:15-12:00am  Supporting Capabilities
                Assurance Cases
                Secure Development & Secure Operations
Today Everything’s Connected

Your System is attackable…

When this Other System gets subverted through an un-patched vulnerability, a mis-configuration, or an application weakness…
What Is an Assurance Case?
History of Assurance Cases

- Originally Only Safety Cases
  - Aerospace
  - Railways, automated passenger
  - Nuclear power
  - Off-shore oil
  - Defense
- Security Cases
  - Use compliance rules more than an assurance case
- Cases for Business Critical Systems
Definition of Safety Case

- From Adelard’s ASCE manual:

“A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment.”
Definition of Assurance Case

- Generalizing that definition

A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system’s properties are adequately justified for a given application in a given environment.
Structured Assurance Cases

- Structure is required to make the creation, sharing, analysis, maintenance and automation of such an assurance case practical

- Structured Assurance Cases are composed of structured sets of Claims, Arguments and Evidence
  - A Claim is a proposition to be assured about the system of concern
  - An Argument is a reasoning of why a claim is true
  - Evidence is either a fact, a datum, an object, a claim or [recursively] an assurance case which supports an Argument against a Claim
Extremely Simplified Overview of Structured Assurance Case Content

Claim = assertion to be proven

Argument = reasoning supporting a claim

Evidence = data supporting an Argument
Need for Standards

- While several different notations exist for safety cases and generalized assurance cases, no widely accepted standard currently exists for specifying structured assurance cases within a systems & software assurance domain.
- Standards are needed before structured assurance cases can be widely leveraged or made practical through automated tooling.
- Coordinated efforts are currently underway in the International Standards Organization (ISO) and the Object Management Group (OMG) to develop these needed standards.
  - ISO 15026 Part 2 (currently published) is a very simple high-level standard outlining the context and basic requirements for structured assurance cases.
  - The OMG SACM (under development) and supporting OMG standards are targeted at providing an automatable level of detail for structured assurance case specification.
ISO/IEC 15026: A Four-Part Standard

- Planned parts:
  15026-1: Concepts and vocabulary (initially a TR2 and then revised to be an IS)
  15026-2: Assurance case (including planning for the assurance case itself)
  15026-3: System integrity levels (a revision of the 1998 standard)
  15026-4: Assurance in the life cycle (including project planning for assurance considerations)

- Possible additional parts as demand requires and resources permit, e.g.
  Assurance analyses and techniques
  Guidance documents
ISO/IEC 15026: Systems & Software Assurance
15026 Part 2: The Assurance Case (Claims-Evidence-Argument)
ISO/IEC 15026: Systems & Software Assurance
15026 Part 2: The Assurance Case (Claims-Evidence-Argument)

Claim
Conclusion & its Uncertainty

Conditionality

Related Consequences & Uncertainty Limitations

Argument
Combines Subordinates Yielding Conclusion & Uncertainty

Justification of Kind & Validity of Reasoning in Argument

Sub-Claim

Evidence

Meaning, validity, integrity, coverage, significance, relevance, & meaningfulness

Assumption & Probability True

Rationale for Assumption, Probability & its Uncertainty

Evidence, etc.
ISO/IEC/IEEE 15026 Assurance Case

- Set of structured assurance claims, supported by evidence and reasoning (arguments), that demonstrates how assurance needs have been satisfied.
  - Shows compliance with assurance objectives
  - Provides an argument for the safety and security of the product or service.
  - Built, collected, and maintained throughout the life cycle
  - Derived from multiple sources

- Sub-parts
  - A high level summary
  - Justification that product or service is acceptably safe, secure, or dependable
  - Rationale for claiming a specified level of safety and security
  - Conformance with relevant standards & regulatory requirements
  - The configuration baseline
  - Identified hazards and threats and residual risk of each hazard / threat
  - Operational & support assumptions

**Attributes**
- Clear
- Consistent
- Complete
- Comprehensible
- Defensible
- Bounded
- Addresses all life cycle stages

©2010 MITRE
Structured Assurance Case Efforts at the OMG

- There are efforts underway within the Object Management Group (OMG) to leverage existing standards and develop new standards for specifying ISO 15026 structured assurance cases in such a way that they will fully support automation
  - Currently working to integrate two draft standards (the Argumentation Metamodel (ARM) and the Software Assurance Evidence Metamodel (SAEM)) into a single standard (Structured Assurance Case Metamodel (SACM)) for structured assurance case specification
  - SACM will also likely leverage the existing OMG Knowledge Discovery Metamodel (KDM) and Semantic Business Vocabulary & Rules (SBVR) standards
Structured Safety Assurance tools are commercially available
Use Cases

- Unambiguous specification of security requirements along with clear identification of what evidence will be acceptable to prove them
  - Unambiguously bound scope of effort
  - Focus training and resource management on skills that are actually needed for a given context
  - Acquire the appropriate tools and services that are actually needed for a given context
  - Enable Acquisition to clearly communicate required assurance and what evidence will be required along with the delivered product
  - Guide Security Engineering
  - Guide Assurance Analysis
  - Guide Testing
  - Guide Independent Assessment & Evaluation
  - Empower accountability and liability
- Structured Assurance Cases are composable and reusable
Common Criteria v4 CCDB
- TOE to leverage CAPEC & CWE
- Also investigating how to leverage ISO/IEC 15026 and OMG’s Structured Assurance Case Metamodel (SACM)

NIAP (U.S.) Evaluation Scheme
- Above plus
- Also investigating how to leverage SCAP
Questions?
ramartin@mitre.org