Delivering the Right Assurance

Requirements-Driven Development for IT Security Products

Erin Connor, Mark Gauvreau, and Samuel E. Moore
EWA-Canada
21 September 2006

Presenter: Mark Gauvreau (mgauvreau@ewa-canada.com)

Your Trusted Partner

Overview

- Introduction to EWA-Canada
- Purpose (Focus) of Presentation
- Introduction to Automated Techniques/Tools
- Use of Automated Techniques/Tools
- Criteria (Critical Features/Capabilities) for All-purpose Tool
- Cost/Benefit Considerations for Tool Use
- Summary

Introduction to EWA-Canada

- Who we are
  - EWA-Canada
- What we do
  - Common Criteria Evaluation Lab – Canadian Scheme
  - FIPS 140-2 Cryptographic Module Test Lab – CMVP
  - Point of Sale & Bank Machine PIN Pad Certifications
    - Interac Financial Services Network
    - Payment Card Industry
  - Documentation development assistance to vendors
  - Managed Security Services and Consulting

Purpose (focus) of Presentation

- Use/application of systems engineering automated tools during:
  - the system/requirements analysis, system design and integration & test phases of product development, and
  - the production of the required CC development documentation (ADV, ATE).

Purpose (focus) of Presentation (cont'd)

Systems and software engineering disciplines and applicable automated tools offer mature engineering processes and a structured approach that can be applied to CC Information Technology Security evaluations.

Introduction to Automated Techniques/Tools

Applying Systems Engineering (SE) to Common Criteria

Tools can be used by the developer and/or consultant/lab to:

- ease steep learning curve when introducing CC into new environments
- better integrate existing product specifications and TOE Security Target
- lead to better integration with engineering processes,
- maintain the evaluation evidence throughout assurance continuity
- maintain traceability data for RCR purposes

Introduction to Automated Techniques/Tools (cont'd)

Applying Systems Engineering (SE) to Common Criteria

Tools can be used during the system life cycle and SE process:

- system/requirements analysis *
- system design *
- integration & test *
- production & customer support

* Focus of presentation

Introduction to Automated Techniques/Tools (cont'd)

Finding A Systems Engineering (SE) Tool

- International Council on System Engineering (INCOSE)
- INCOSE Tools Database Working Group
- Requirements Management Tools
- Systems Architecture Tools

Introduction to Automated Techniques/Tools (cont'd)

International Council on System Engineering (INCOSE) < http://www.incose.org/ >

– INCOSE Efforts to Improve System Engineering through Modeling & Tools

– INCOSE Tools Database Working Group

- INCOSE Object Management Group - Systems Modeling Language (OMG SysML™).

- Tools Database. The INCOSE Tools Database Working Group (TDWG) makes information on commercial-of-the-shelf (COTS) and government-off-the-shelf (GOTS) tools of interest to systems engineers available via this website.

Use of Automated Techniques/Tools

Sample Tools

- DOORS Telelogic (was QSS) Requirements traceability tool. http://www.telelogic.com/ *
- CORE Vitech Corporation Full life-cycle systems engineering CASE tool. http://www.vitechcorp.com
- RTM (Requirements Traceability Management) Requirements traceability software. http://www.serena.com

* Focus of presentation

Use of Automated Techniques/Tools

Telelogic Tools < http://www.telelogic.com >

- Telelogic FOCAL POINT
- Telelogic DOORS
- Telelogic SYSTEM ARCHITECT
- Telelogic TAU
- Telelogic SYNERGY
- Telelogic DASHBOARD
- Telelogic LOGISCOPE
- Telelogic DocExpress
- Telelogic Rhapsody
- Telelogic Statemate

* Although Telelogic tools are the focus of this presentation, tool suite integration and compatibility with other vendors' products are important considerations in tool selection.

Use of Automated Techniques/Tools

Telelogic Tools applications for CC Development evidence requirements

ADV_FSP Functional Specification

- Import TSFs (F.DOTS) defined in the Security Target TOE Summary Specification (ST/TSS).
- Import Security Functions (SFs) defined by the Functional Specification (FSP).
- Requirements Management with Telelogic DOORS
- Automated Documentation Generation with Telelogic DocExpress

Use of Automated Techniques/Tools

Telelogic Tools applications for CC Development evidence requirements

ADV_HLD High level design

- Characterize TOE Subsystems as defined by the High Level Design (HLD).
- Define FSP to HLD Subsystem Mapping
- Define FSP to HLD (Interface) Mapping
- System design architecture with Telelogic SYSTEM ARCHITECT
- Systems and Software Design, Development and Testing with Telelogic TAU
- Requirements Management with Telelogic DOORS
- Automated Documentation Generation with Telelogic DocExpress

Use of Automated Techniques/Tools

Telelogic Tools applications for CC Development evidence requirements

ADV_LLD Low level design

- Characterize Subsystem LLD Modules defined by the Low Level Design (LLD)
- Define HLD Subsystem to LLD Module Mapping
- Systems and Software Design, Development and Testing with Telelogic TAU
- Model-Driven Development with UML 2.0 and SysML with Telelogic Rhapsody
- Embedded Systems Design Software with Telelogic Statemate
- Automated Documentation Generation with Telelogic DocExpress

Use of Automated Techniques/Tools

Telelogic Tools applications for CC Development evidence requirements

ADV_IMP Implementation representation

- Characterize/design/develop IMP source code modules
- Define LLD-IMP Mapping
- Systems and Software Design, Development and Testing with Telelogic TAU
- Model-Driven Development with UML 2.0 and SysML with Telelogic Rhapsody
- Embedded Systems Design Software with Telelogic Statemate
- Automated Documentation Generation with Telelogic DocExpress

Use of Automated Techniques/Tools

Telelogic Tools applications for CC Development evidence requirements

ADV_RCR Representation correspondence - Telelogic DOORS

- TSS to FSP Mapping
- FSP to HLD Subsystem Mapping
- FSP to HLD (Interface) Mapping
- HLD-LLD Mapping
- LLD-IMP Mapping

Use of Automated Techniques/Tools

Telelogic Tools applications for CC Development evidence requirements

ATE_COV Coverage - Telelogic DOORS or DOOR/Rational

- accuracy and completeness of the correspondence between the tests identified in the test documentation and the functional specification.

ATE_DPT Depth - Telelogic DOORS or DOOR/Rational

- accuracy and completeness of the correspondence between the tests identified in the test documentation and the high-level design.

Use of Automated Techniques/Tools

Telelogic Tools applications for CC Development evidence requirements

ATE_FUN Functional Tests

- Test plans, test procedures, expected results and actual results with Telelogic DOORS, or DOOR/Rational
- Software Quality Assurance with Telelogic LOGISCOPE
- Systems and Software Design, Development and Testing with Telelogic TAU
- Model-Driven Development with UML 2.0 and SysML with Telelogic Rhapsody
- Embedded Systems Design Software with Telelogic Statemate
- Automated Documentation Generation with Telelogic DocExpress

Use of Automated Techniques/Tools

Telelogic Tools applications for CC Development evidence requirements

ATE_IND Independent Testing with Telelogic DOORS or DOOR/Rational

- Evaluation Test Plan and Evaluation Test Procedures, Test results

Criteria (critical features/ capabilities) for All-purpose Tool

Key Criteria for All-purpose Tool to Support

- Requirements Management Tools

- System Architecture Design/Development

Criteria (critical features/ capabilities) for tools (cont'd)

- List of Criteria:
  - tool suite integration and compatibility with other vendors' products
  - Capturing requirements/identification
  - Capturing system element structure
  - Requirements flowdown
  - Traceability analysis
  - Configuration Management
  - Documents & other output media
  - Groupware

Criteria (critical features/ capabilities) for tools (cont'd)

- List of Criteria (Cont'd):
  - Interfaces to other tools
  - User interfaces
  - Support life cycle
  - Support Quality system design
  - Support multiple system views
  - Methodology independent
  - Computer environment
  - Resource requirements
  - Support & maintenance
  - Standards
  - Training

Criteria (critical features/ capabilities) for tools (cont'd)

- List of Criteria (cont'd):
  - Works with Legacy systems
  - Model execution
  - Production code generation
  - Code generation languages
  - Requirements
  - Analysis
  - Design
  - Test
  - Openess
  - Collaboration
  - Vendor

Cost/benefit considerations for tool use

Costs Considerations

- Tools
- Computer Environment
- Resource requirements
- Training
- Support & Maintenance

Cost/benefit analysis for tool use

Benefit Considerations

- Supports both requirements management and system/product design/test
- System development approach
- Groupware
- CC evaluation evidence
- Mature engineering processes
- Structured approach
- Multiple users (tools can be used by the developer and/or consultant/lab)

Cost/benefit analysis for tool use

Benefit Considerations (cont'd)

- Eases steep learning curve when introducing CC into new environments,
- Better integration of existing product specifications and TOE Security Target,
- Leads to better integration with engineering processes,
- Maintains the evaluation evidence throughout assurance continuity

Summary

- Introduced Automated Techniques/ Tools
- Discussed use of Automated Techniques/ Tools in CC evaluations and assurance continuity/maintenance
- Presented Criteria (features/capabilities) for all-purpose tool
- Presented Cost/benefit considerations for tool use

Questions

?

For further information:
Mark Gauvreau
(mgauvreau@ewa-canada.com)