APEX ASSURANCE GROUP

Setting Expectations

Common Criteria and the SDLC

Ray Potter
Managing Director

rpotter@apexassurance.com
+1 (919) 363-6527

Topics for Discussion

- Concepts of Software Development Life Cycle
- Basic Integrity Controls for Software Assurance
- Where Common Criteria Fits
- Case Study 1: Fortune 500 Organization(s)
- Case Study 2: Venture-Backed Startup(s)
- Case Study 3: Fortune 50 Aerospace Vendor
- Case Study 4: Fortune 100 Defense Contractor
- Summary

Why Give This Talk?

- Address some misconceptions about Common Criteria
- Introduce some interesting case studies
- Discuss where the Common Criteria can fit within the SDLC

- A summary of experiences from the following services
  - Common Criteria and FIPS 140 Consulting
  - Systems-Level Certification and Accreditation Consulting
  - SDLC consulting
  - Whitepaper Authorship
  - End-user training/workshops in various areas of information security

A Dedicated Common Criteria Professional?

- Just a strange coincidence!

Software Development Life Cycle Overview

- A process for developing software
- Common areas of SDLC
  - Concept
  - Requirements
  - Design and Documentation
  - Programming
  - Testing
  - Release
- Different implementation models exist
  - Their use depends on environment, architecture, customer need, time to market, etc.

Integrity Control Summary

- Processes and activities that contribute to developing code which is reliable and fault-tolerant
- Address security functions in a rigorous, focused, and structured manner
  - Security Training
  - Secure Design
  - Secure Programming (Coding)
  - Secure Source Code Handling
  - Security Testing
  - Security Documentation
  - Security Readiness

SDLC and Common Criteria

- Where does Common Criteria (@ EAL2-EAL4) fit?
- What did we say about the SDLC?
  - Concept, Requirements, Design and Documentation, Programming, Testing, Release
- What did we say about Integrity Controls?
  - Processes and activities that contribute to developing code which is more reliable and fault tolerant
  - Address security functions in a rigorous, focused, and structured manner
- CC provides processes and activities for the TOE
  - Structured
  - Rigorous, especially at higher levels
- CC does not provide direct implementation instructions for integrity controls

Case Study 1: Fortune 500/1000 Organizations

- **Goal:** Achieve EAL2-EAL4+ as quickly and efficiently as possible
  - Meet a procurement checkmark
- Most prolific recipients of Common Criteria evaluations
- Companies have process, design, testing documents
  - Depth of content not sufficient
  - Contradictory information, especially in processes
  - Presentation of content not "evaluator friendly"
- Results
  - Develop supplements to map existing documents to CC
  - CC does not improve, change, or affect the SDLC
  - Documents are shelved until the next evaluation

Case Study 2: Venture-Backed Startup(s)

- **Goal:** Achieve EAL2 (sometimes EAL3 or EAL4) evaluation to enter Federal marketplace
- Most process details aren't formally documented
- Sparse design documentation
- Basic testing documentation

- Results
  - Develop design and process documents
  - Augment testing documents
  - *Hope that d*ocuments are shelved until the next evaluation

Case Study 3: Fortune 50 Aerospace Vendor

- **Goal:** Prove to Federal Aviation Administration that they referenced Common Criteria in their development
- Evaluation against DO-178B
  - Certification for software avionics
  - Similar to Common Criteria, with more rigid requirements than CEM
- Results
  - Comprehensive training and mapping of DO-178B (and other guidelines) to Common Criteria
  - Security Target to address security concerns in Common Criteria language
  - CC did not improve, change, or affect the SDLC

Case Study 4: Fortune 100 Defense Contractor

- **Goal:** Pursue EAL4+ and EAL7
- Developing a new product for release in late 2009
- Following a loose Evolutionary Prototyping development model
  - Supporting documentation minimal at best

- Results
  - Use Common Criteria as a model to develop SDLC documentation
    - Design, User/Administrator Guides, Test Plans
  - Develop a maintenance plan
  - Develop a go-to-market strategy

Summary of Common Criteria in the SDLC

- Valuable to product vendors
  - Make the sale
  - Improve internal process (in rare cases)
- Valuable to end users as part of Systems Development Life Cycle
  - Fulfill procurement requirements
  - Use Protection Profiles to define requirements for specific environments
- Provides a model for addressing integrity controls in the SDLC
- Serves as a subset of SDLC

APEXASSURANCE
GROUP

Ray Potter
rpotter@apexassurance.com
+1 (919) 363-6527

www.apexassurance.com