Common Criteria: Delta Evaluation

James Arnold/Terrie Diaz

SAIC Common Criteria Test Laboratory

Introduction

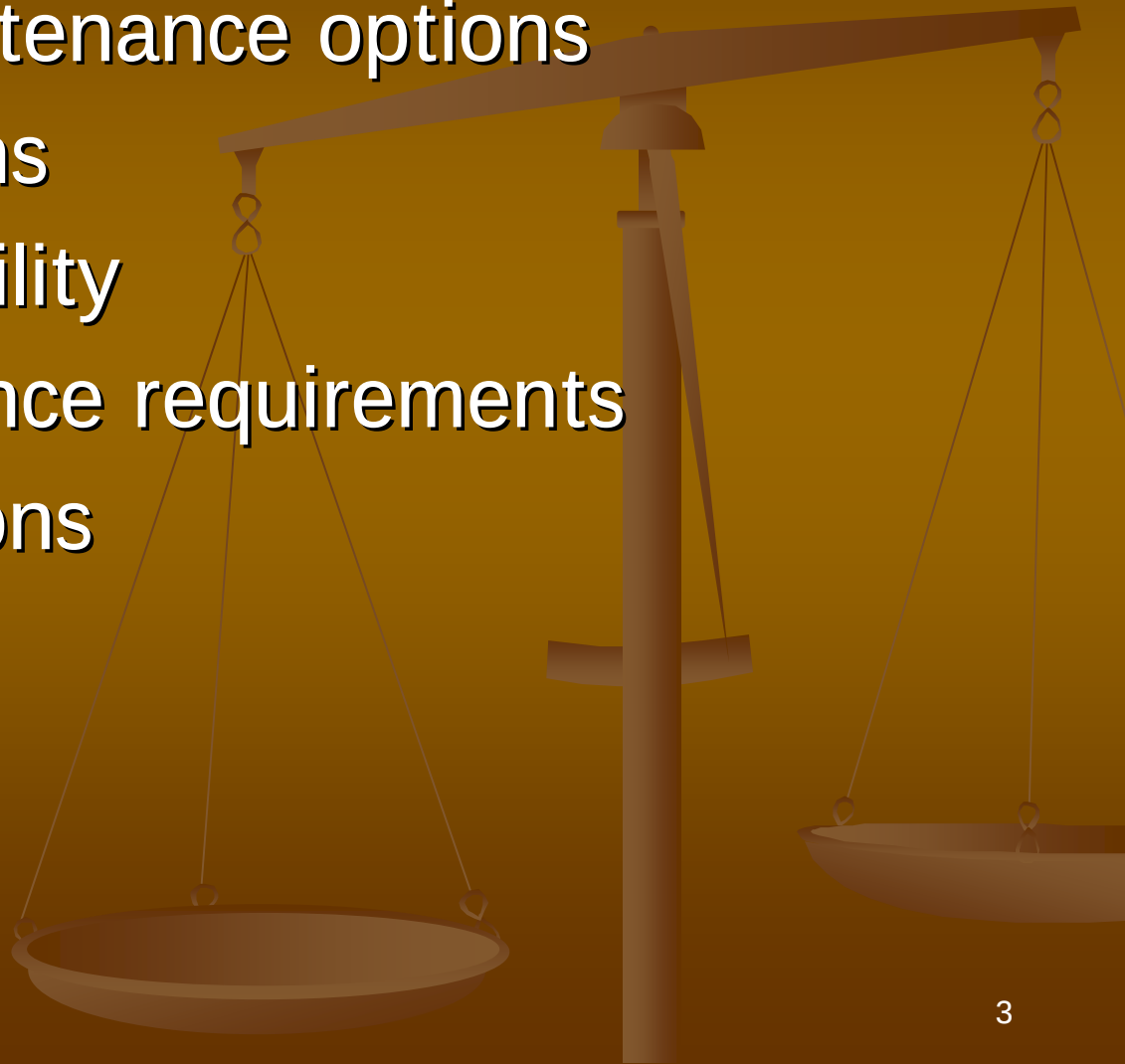
Common Criteria: Delta Evaluations

- Evaluations are expensive
  - Maximizing investment
- Evaluations take a long time
  - Keeping evaluation current

Just what options are or should be available?

Topics

- Assurance maintenance options
- Delta evaluations
- Material availability
- Security assurance requirements
- Recommendations

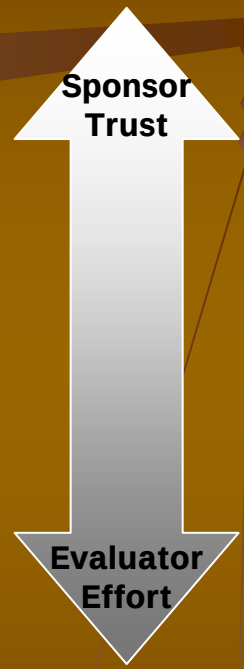


Assurance Maintenance Options

- Currently recognized approaches
  - Assurance Continuity
    - Developer driven
  - Re-evaluation (with maximum reuse)
    - Complete evaluation, reusing previous findings when possible
  - Component/Composed TOE
    - Evaluate component once, use many times
      - Component TOE evaluation yields composition artifacts
      - Composed TOE evaluation consumes composition artifacts

Delta Evaluations

- Delta evaluation reuse scenarios
  - Trivial reuse
    - Developer assurance of no changes
  - Simple reuse
    - Evaluator determines no changes
  - Common reuse
    - Evaluator focus on identified changes
  - Complex reuse
    - Combining or reusing results from different sources



Material Availability

- Evaluation related material
  - Evaluation result
    - Certificate, ST, certification/validation report
  - Evaluation evidence
    - Evaluation inputs
  - Detailed evaluation results
    - Evaluation technical report, work packages

Material for Reuse

	Evaluation Result	Evaluation Evidence	Detailed Results
Trivial Reuse	Yes	No	No
Simple Reuse	Yes	Yes	No
Common Reuse	Yes	Yes	Maybe
Complex Reuse	Yes	Yes	Maybe

Security Assurance Requirements

- Security Target

Trivial Reuse	No – ST should always change
Simple Reuse	Yes – PP conformance; 'borrowed' material
Common Reuse	Yes – ST changes; PP tailoring
Complex Reuse	Yes – Multiple conformance

Security Assurance Requirements

- Configuration management, Delivery, Life-cycle

Trivial Reuse	Yes – No change per developer
Simple Reuse	Yes – Evaluator determines no change
Common Reuse	Yes – Changes to applicable process
Complex Reuse	Yes – Combination of multiple processes

Security Assurance Requirements

- Design

Trivial Reuse	Maybe – Unlikely if TOE changed
Simple Reuse	Maybe – Unlikely if TOE changed
Common Reuse	Yes – Changes to design
Complex Reuse	Yes – Combination of multiple design elements (products)

Security Assurance Requirements

- Guidance (including operation)

Trivial Reuse	Yes – No change per developer; no other indicators of change
Simple Reuse	Yes – Evaluator determines no change; no other indicators
Common Reuse	Yes – Changes to applicable guidance or other inputs
Complex Reuse	Yes – Combination of multiple guidance documents

Security Assurance Requirements

- Tests

Trivial Reuse	Maybe – Unlikely if TOE changed; independent testing issues
Simple Reuse	Maybe – Unlikely if TOE changed
Common Reuse	Yes – Changes to tests or test inputs
Complex Reuse	Yes – Combination of multiple products

Security Assurance Requirements

- Vulnerability Analysis

Trivial Reuse	Maybe – Public domain (an input) is always changing
Simple Reuse	Yes – Relevant public domain information may be unchanged
Common Reuse	Yes – Changes to vulnerability analysis
Complex Reuse	Yes – Combination of multiple products

Recommendations

- Delta evaluation approach should be adopted
  - Reuse any evaluation findings where possible
  - Don’t force use of information if not required
  - Acknowledge trust in developers
  - Delta evaluation report
  - Validation process for delta evaluation
    - Delta certification/validation result
  - Mutually recognize delta evaluation results

Conclusion

- Existing assurance continuity approaches each have pros and cons
- Delta evaluation concepts can be employed today, but only when it fits in one of the existing approaches

Contact

James Arnold

SAIC CCTL Technical Director

James.L.Arnold.Jr@saic.com

Terrie Diaz

SAIC CCTL QA Director

Terrie.L.Diaz@saic.com

http://www.saic.com/infosec/cctl.html