Exact Conformance

James Arnold | Tammy Compton

September 11, 2013

Gossamer Laboratories

Topics

- Protection Profile Conformance Today
- Common Criteria Conformance Definitions
- Exact Conformance Rules
- Recommendations

Protection Profile Conformance Today

- **U.S. Scheme Conformance**
  - A-la-cart Security Target (ST) evaluations no longer accepted
    - Evaluations are limited to Protection Profile (PP) conformant products, so conformance is a must and no longer a choice
  - Protection Profile augmentations no longer freely accepted
    - Can't add claims for features beyond Protection Profile requirements
  - Emphasis on Protection Profile development
    - Goal of reducing choices and limiting scope
    - PPs must define allowed flexibility

…what are the rules?

Common Criteria Conformance Definitions

- **CC Currently Defines**
  - **Demonstrable Conformance**
    - The Security Target has to arguably solve at least the same security problem
  - **Strict Conformance**
    - The Security Target has to solve at least the same security problem using at least the same requirements found in each selected Protection Profile
- **Evolving Requirement for**
  - ***Exact Conformance***
    - The Security Target is limited to the requirements and scope defined in a selected Protection Profile

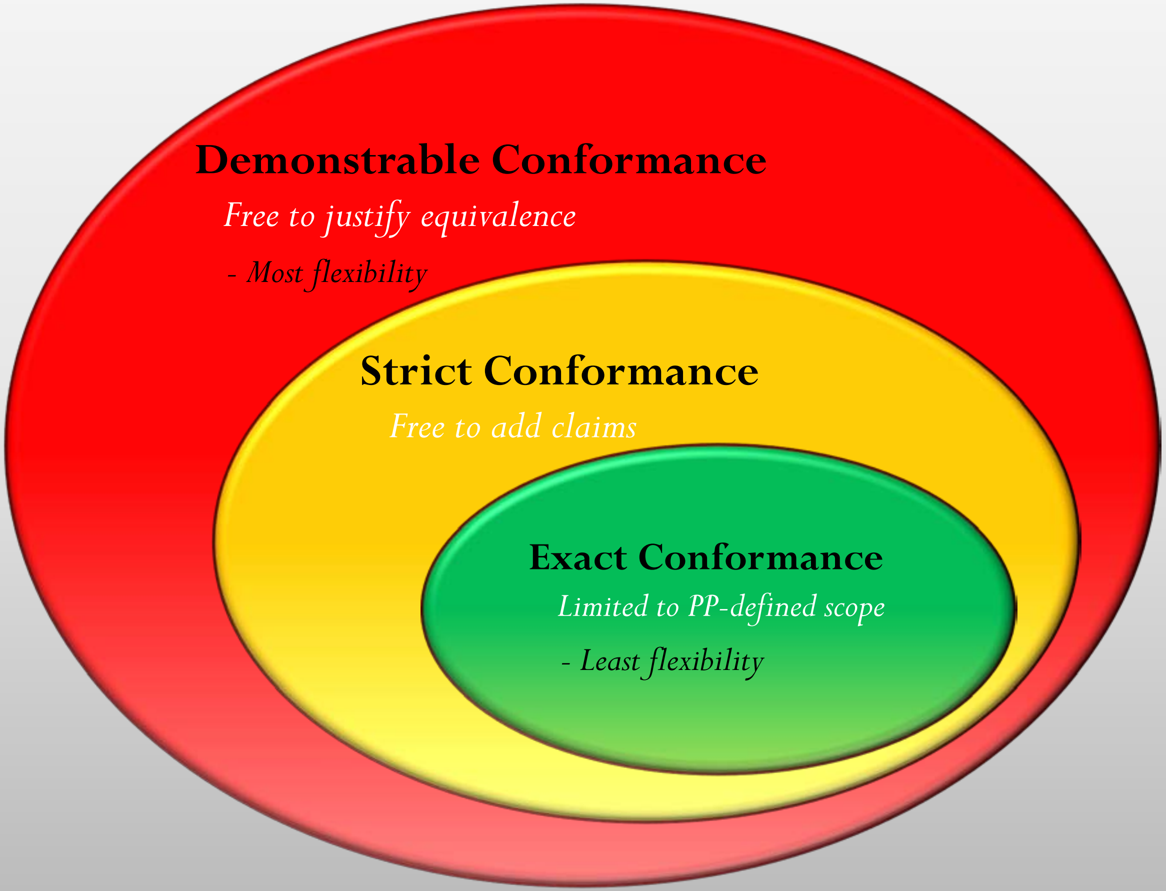
Common Criteria Conformance Definitions

- ***Demonstrable conformance*** ⇨ **Exact conformance**
  - Relation between an ST and a PP, where the ST provides a solution which solves the generic security problem in the PP
  - The PP and the ST may contain entirely different statements that discuss different entities, use different concepts etc. Demonstrable conformance is also suitable for a TOE type where several similar PPs already exist, thus allowing the ST author to claim conformance to these PPs simultaneously, thereby saving work.

Common Criteria Conformance Definitions

- *Strict conformance* ⇨Exact conformance
  - Hierarchical relationship between a PP and an ST where all the requirements in the PP**, and only those requirements,** also exist in the ST
  - This relation can be roughly defined as “the ST shall contain all statements that are in the PP, ~~but~~ **and** may **not** contain more”. Strict conformance is expected to be used for stringent requirements that are to be adhered to in a single manner.

Common Criteria Conformance Definitions



Demonstrable Conformance

Free to justify equivalence

- Most flexibility

Strict Conformance

Free to add claims

Exact Conformance

Limited to PP-defined scope

- Least flexibility

Exact Conformance Rules

- Protection Profile Augmentation
  - Optional Requirement Components
- Requirement Operations
  - Assignment
  - Selection
  - Iteration
  - Refinement
- Assurance Activity Operations

Exact Conformance Rules

- Protection Profile Augmentation
  - Optional Requirement Components
    - **Each PP can define optional requirements and only those may be used in an ST to augment that PP**
- Requirement Operations
  - Assignment
  - Selection
  - Iteration
  - Refinement
- Assurance Activity Operations

Exact Conformance Rules

- Protection Profile Augmentation
  - Optional Requirement Components
- Requirement Operations
    - **All requirement operations must be made on the requirement versions found in the PP (e.g., it is not allowable to revert to the Common Criteria versions)**
  - Assignment
  - Selection
  - Iteration
  - Refinement
- Assurance Activity Operations

Exact Conformance Rules

- Protection Profile Augmentation
  - Optional Requirement Components
- Requirement Operations
  - Assignment
    - **All requirement assignments left incomplete in the PP must be completed according to the assignment description in the PP (e.g., found in the assignment text and application notes)**
  - Selection
  - Iteration
  - Refinement
- Assurance Activity Operations

Exact Conformance Rules

- Protection Profile Augmentation
  - Optional Requirement Components
- Requirement Operations
  - Assignment
  - Selection
    - **All requirement selections left incomplete in the PP must be completed according to the selection choices in the PP**
  - Iteration
  - Refinement
- Assurance Activity Operations

Exact Conformance Rules

- Protection Profile Augmentation
  - Optional Requirement Components
- Requirement Operations
  - Assignment
  - Selection
  - Iteration
    - **Requirements can be iterated in accordance with explicit guidance in a given PP or when the scope of the original requirement is not exceeded**
  - Refinement
- Assurance Activity Operations

Exact Conformance Rules

- Protection Profile Augmentation
  - Optional Requirement Components
- Requirement Operations
  - Assignment
  - Selection
  - Iteration
  - Refinement
    - **Refinement is generally not allowed, except as might be necessary to support correct iteration of SFRs (e.g., to split a concept to be fully addressed in iterated parts)**
- Assurance Activity Operations

Exact Conformance Rules

- Protection Profile Augmentation
  - Optional Requirement Components
- Requirement Operations
  - Assignment
  - Selection
  - Iteration
  - Refinement
- Assurance Activity Operations
  - **Assurance Activities should not be changed**
  - **The exception is when evaluators refine or improve Assurance Activities based on findings during the course of evaluation**

Recommendations

- Create and adopt a CC addendum defining and expressing rules for *Exact Conformance*
- Develop Assurance Activities for *Exact Conformance* evaluation
- Eventually Revise CC Parts 1 and 3
  - *Exact Conformance* definition (Part 1, Section 4.1)
  - *Exact Conformance* concept (Part 1, Annex D)
  - Adjust all other CC references (e.g., APE_CCL.1.11C) related to PP conformance
- Develop guidance for PP developers to help ensure any necessary or desired level of flexibility is properly built into forthcoming PPs

Questions?

Contacts:

- James Arnold
  - JamesArnold@gossamersec.com
- Tammy Compton
  - TammyCompton@gossamersec.com

www.gossamersec.com

www.facebook.com/gossamersec

@gossamersec

Disney Walk around the World January 1996 – CCv1.0