



## Assurance Activities Test Model

Quang Trinh  
28 September 2011

# Introduction



- Overview
- Testing Approach
- Level of Detail
- Method of Testing
- Test Results and Reporting
- Conclusions

# Overview



In recent years, the notion of “Tailored Assurance” has emerged and seems to be gaining momentum in the Common Criteria (CC) community, mostly led by efforts from the U.S. Scheme.

The U.S. has published the Security Requirements for Network Devices Protection Profile (NDPP) and intends to publish more Protection Profiles which will “represent an evolution of traditional Protection Profiles.”

The cited goals are to:

- improve consistency,
- produce comparable and meaningful results,
- reduce cost and efforts, and
- others stated in the ‘Common Criteria Reforms’ paper

[[http://www.niap-ccevs.org/cc\\_docs/CC\\_Community\\_Paper\\_10\\_Jan\\_2011.pdf](http://www.niap-ccevs.org/cc_docs/CC_Community_Paper_10_Jan_2011.pdf)].

# Overview



## Achieving the Goals

- The Security Requirements for Network Devices Protection Profile (NDPP) ‘Tailored Assurance’ activities strive to meet the cited goals by:
  - Providing detailed guidance about what information needs to be made to evaluators (and other product users) in the Security Target.
  - Providing detailed guidance about what information needs to be made to product users (and evaluators) in the available product installation and operation guides.
  - Providing detailed guidance on the tests that evaluators need to perform in order to ensure the other information is accurate.

*This presentation addresses the testing aspect of the assurance activities.*

# Overview



## Perceived Problem

- Of the assurance activities, it is believed that testing is critically important.
  - Assertions in the Security Target and guidance documents are just that unless they are substantiated by some sort of testing.
- Unlike most current Common Criteria evaluations, the principal burden lies on independent evaluator testing since vendors are not required (or even allowed) to share their testing efforts.
- To fulfill the cited goals each Protection Profile (PP) needs to define testing activities according to a well-defined testing model that serves to guide PP authors appropriately.

# Overview



## Proposed Solution

- A test model need to be developed that directs testing activities in all new Protection profiles).
- The test model needs to address the following topics so that new PPs will not only promote consistent evaluation results for conforming product, but also PPs will have some measure of consistency from PP to PP.
  - Testing Approach – The model needs to address the approach for defining test activities in PPs.
  - Level of detail – The model needs to indicate the required level of detail for defined test activities.
  - Method of testing – The model needs to indicate how preferences or requirements for specific types or methods of tests should be addressed in PPs.
  - Meaningful and well-documented test results – The model needs to indicate how test results should be produced by evaluators.

# Testing Approach



## Testing Approach

- The testing approach defines essentially where testing assurance activities should be defined in a PP and also to what those activities apply (e.g., interfaces, functions, requirements).

### **SFR-based Test Approach:**

- Each Security Functional Requirement (SFR) has at least one “test” assurance activity that describes how the lab must verify/confirm the SFR. For complex SFRs (multiple elements) such as FDP\_ACF, multiple tests may be required.

### **SF-based Test Approach:**

- Similar to SFR but for security function. Each Security Function (SF) has at least one “test” assurance activity that describes how the lab must verify/confirm it.

### **TSFI-based Test Approach:**

- The claimed security functionalities are tested through the TOE Security Function Interfaces (TSFIs).

### **Hybrid Test Approach:**

- Any combination of the test models above.

# Level of Detail



## Level of Detail

- Once the test approach has been established, the Protection Profile (PP) should define the level of details for testing.
- This not only includes the number of Target of Evaluation (TOE) Security Functions (TSF) attributes to be tested but TSF Interfaces (TSFIs) to be tested and the sampling of the TOE models and type of tests (e.g., blackbox).



## All Security Attributes

- All security attributes identified in the Security Functional Requirement (SFR) should be tested.
  - Username, Password, Roles, Privileges, Permissions
  - Cryptographic Keys , Algorithms
  - Access Control Lists, Rules,
  - Management Security Attributes such as Session Timeout Values, Password Complexity Attributes, etc.



## All TOE Security Functional Interfaces (TSFIs)

- All identified external TSFIs should be covered.
  - Graphical user interfaces including all security-relevant tabs and fields
  - Command-line interfaces including all security-relevant commands.
  - Application program interfaces including all security-relevant calls
  - Security protocols including security-relevant fields
  - Configuration files

# Level of Detail



## Black Box

- The evaluators should perform some vulnerability testing.
- Protection Profiles (PPs) should document or reference common weaknesses vulnerabilities for that technology type.
- Ensure products have good user input validation, prevention against Denial of Service, etc.

## Code Review

- The new PPs should allow for code review if there is any functionality that requires too much time and effort to test.
  - This should be documented as such.

## Test Configuration

- The labs should put the Target of Evaluation (TOE) in configuration consistent with Security Target (ST).
  - For example, TOE must be in FIPS mode
- Sample of the TOE models based on available design understanding.



## Automated vs. Manual Testing

- There are the advantages and disadvantages in each case.
- Protection Profiles (PPs) should identify any preferences or requirements.
  - In particular, PPs should identify any relevant security tools that should or must be used.
- PPs should also indicate whether and how vendor tests and test activities might come into consideration.

# Method of Testing



## Automated Testing

- Simplify complex manual tasks
- Reduce time and effort during testing
- Provide more systematic approach
- Result in less mundane human errors
- Require time and effort during the development phase
- Require expertise in coding
- Require assistance from vendor

# Method of Testing



## Manual Testing

- Easier to implement if technology type is simple
- For graphical user interfaces, may be the only choice
- Require no knowledge of code
- Hard to be reproduced perfectly
- Prone to human errors during execution

# Method of Testing



- The new Protection Profiles (PPs) should not require one over the other without good reasons.
  - Should rely on evaluator experience.
  - This does not mean PPs can't recommend one over the other.
- Based on the technology type, the new PPs should require automated security tools.
  - For example, for network appliance, port scanning tools should be required or Web-based admin console should require web vulnerability scanning tools.
  - However, the selection of security tools should be left to the labs.
- Vendor testing can complement independent evaluator testing if sufficiently well understood.

# Test Results and Reporting



- The evaluators should produce test results that are useful for customers and end-users
  - ‘Pass’ verdict is not a good example.
  - The test results should specify how the claimed security functionalities were tested based on test approaches (SFRs, SFs, TSFIs, Hybrids).
  - If security tools were used, the test report should specify how they were used and what was verified.
  - If vendor testing was performed, the test report should specify what was performed to provide additional assurance.
  - The test results should be made public.

# Test Results and Reporting



- The test reporting template should provide a way to produce comparable results.
  - The Protection Profiles (PPs) should guide evaluators to produce consistent and meaningful test results.
  - Example such as Derived Test Requirements (DTR) or automated reporting tool such as one used for FIPS 140-2 should be considered and reused where possible.

# Conclusions



- The new Protection Profiles (PPs) have an opportunity to achieve all the goals in the Common Criteria (CC) reforms.
- To improve consistency, produce comparable and meaningful results, reduce cost and efforts, the new PPs should use a well-defined testing model with effort to avoid the following issues:
  - Security claims not tested or verified independently
  - Different evaluators producing different test results
  - Evaluation time and efforts reduced at the cost of assurance
- The new PPs seem to be off to a good start, but all the new PPs need to develop appropriate testing activities that are focused on meeting the cited goals.

# Conclusions



- This presentation recommends several ideas and recommendations that will support the stated goals in the CC reform.
- The notion of a test model should be considered and developed to improve Protection Profile (PP) consistency and perhaps also to reduce the effort to develop new PPs.

# Contact



**Quang Trinh**

**SAIC Accredited Testing & Evaluation Labs,  
Common Criteria Evaluator and FIPS Tester**

**[Quang.M.Trinh@saic.com](mailto:Quang.M.Trinh@saic.com)**

**<http://www.saic.com/infosec/testing-accreditation/common-criteria.html>**