Evolution of the New PP Approach

Tammy Compton

(Presented by Ed Morris)

September 10, 2014

Gossamer Laboratories

Feedback

- Should be directed to Tammy Compton: TammyCompton@GossamerSec.com +1 (240) 994-9770
- Questions
- Comments
- Complaints
- Historical inaccuracies
- Factual errors
- Outright lies
- Cease and desist letters
- Formal accusations of slander
- Subpoenas and summons

Other Feedback

- Should be directed to Ed Morris: EdMorris@GossamerSec.com +1 (703) 582-4448
- Compliments
- Praise
- Requests for speaking engagements
- Gifts
- Honorary degrees
- Bestowal of formal titles

Topics

- Background
- Initial Assurance Activities
- Evolving Assurance Activities
- Recommendations

Background 1, Medium Robustness

- **EAL4+ Assurance required**
- **Relied upon standard Common Evaluation Methodology and Common Criteria Security Assurance Requirements**
- **Technology specific**
- **Additional testing done beyond evaluator testing**

Background 2, Medium Robustness Criticisms

- Lengthy evaluation process
  - Potentially spanning more than one year
  - Evaluated products might be already obsolete
- Too costly
  - Evaluation expenses
  - Cost of vendor resources
  - Opportunity costs
- Inconsistent evaluation results between labs and between schemes
- Perceived lack of effort-commensurate improvement in evaluated products' security

Background 3, Achievable, Repeatable, and Testable

- **"Achievable, Repeatable, and Testable" (and Efficient)**
- **Embodied by the Protection Profile for Network Devices (NDPP) - Dec 2010**
  - **Departure from the Common Evaluation Methodology as well as many of the Common Criteria Security Assurance Requirements**
  - **"EAL0" – no defined associated EAL level**
  - **Exact Compliance (no Refinement or Augmentation)**
  - **First of the new style Protection Profiles with Assurance Activities**
    - Assurance Activities (defined in the Protection Profile) are designed to be specific to the applicable technology and security functions
    - Goal was repeatability among products/Schemes as well as more cost effective and meaningful evaluation results

Initial Assurance Activities

- **Can be thought of as a "Black-box" testing approach**
  - No access to source code needed
  - No documentation of internal architecture or interfaces
- **Required very little tool/test development effort**
  - Testing possible through readily available tools and client software
- **Heavily weighted to TOE Summary Specification descriptions**
  - Many Security Functional Requirements have no Test Assurance Activities
  - The existing Test Assurance Activities were focused on verifying the crypto algorithms (used in higher protocols), audit capabilities, and authentication mechanisms
- **Entropy analysis could not be done with a black-box approach—a source of problem for vendors.**

Newer Assurance Activities

- **First appear in drafts of the NDPP Errata 2 but MDFPP v1.0 released first.**
- **Testing requires (vendor or laboratory) development of specific testing tools**
  - Testing no longer possible through "black-box" testing, but instead requires specialized tools (e.g. debugging environments or special builds)
- **Much greater depth of testing for trusted channel protocols**
  - Protocol-layer testing (EAP-TLS and TLS protocol) and additional focus on X.509 certificate validation (validity, cert-chain, revocation).

Testing Example

- **NDPP Errata 2 testing example**
- **Original NDPP FCS_TLS_EXT.1 Test Assurance Activity**
  - The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement.
- **NDPP Errata 2 added Test Assurance Activity**
  - The evaluator shall setup a man-in-the-middle tool between the TOE and the TLS Peer and shall perform the following modifications to the traffic:
    - [Conditional: TOE is a server] Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the server denies the client's Finished handshake message.
    - [Conditional: TOE is a client] Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.
    - [Conditional: TOE is a client] If a DHE or ECDHE ciphersuite is supported, modify the signature block in the Server's KeyExchange handshake message, and verify that the client rejects the connection after receiving the Server KeyExchange.
    - [Conditional: TOE is a client] Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data

Testing Example (continued)

- No tools have been identified or provided for the man in the middle tests
- Evaluation labs have to find or develop their own tools
- The result is the testing can be more subjective given that labs are left to their own devices to develop test tools and procedures to perform technical tests that may be non-trivial
- No indication whether product vendors can create tools (and if so, what evaluators vetting is required)

Evolving Assurance Activities

- **After the NDPP, mobility became a primary focus of NIAP in the U.S.**
- **The mobility (and other evolving) PPs increase the focus on detailed Test Assurance Activities**
  - There are many test cases designed to test a range of protocol characteristics
- **In general, the evolving PPs indicate a growing level of required developer support for evaluations**
  - There are Test Assurance Activities that require access to interfaces or functions that would not normally be accessible, such as being able to dump memory or flash contents for analysis
  - There are requirements for design information that might be too sensitive to publish (e.g., in a Security Target), such as a complete cryptographic key hierarchy description

Evolving PP Testing

- **The following Test Assurance Activity (from the Protection Profile for Mobile Device Fundamentals) Requires both that secret key values can become known during testing and that storage locations can be accessed**
  - *Test 1:* The evaluator shall utilize appropriate combinations of specialized operational environment and development tools (debuggers, simulators, etc.) for the TOE and instrumented TOE builds to test that keys are cleared correctly, including *all* intermediate copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.

Evolving PP Testing (continued)

- **Based on the Test Assurance Activities**
  - **In many case the evaluators are not testing a commodity product, but rather some debug or specially instrumented version of the product**
  - **The evaluation doesn't address the relationship or correspondence between the 'special' product available for testing and the actual product that will be used by consumers**
  - **Like the NDPP Errata 2, there are plenty of requirements for tools and procedures that must be devised by evaluators to perform the required activities and require expert knowledge in certain technologies**

Evolving PP Testing (continued)

- **The following examples both require some level of technical expertise in order to develop suitable tools and procedures**
  - **Example from Protection Profile for Mobile Device Fundamentals**
    - **FCS_TLS_EXT.1**
      - Test 4: The evaluator shall configure the authentication server to send a certificate in the TLS connection that the does not match the server-selected ciphersuite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite or send a RSA certificate while using one of the ECDSA ciphersuites.) The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.
  - **Example from Web Browser PP**
    - **FDP_SDX_EXT.1**
      - Test 1: The evaluator shall use debugging or test facilities to introduce code into a rendering process that attempts to directly access the platform's file system, and then direct execution to it. The evaluator shall ensure that execution of this code fails to access the TOE file system

Future PP Testing Evolution

- **Not just a NIAP/US problem**
- **NDPP evaluations have been done in several other schemes**
- **NDcPP is (nearly) here**
- **More schemes and labs will only exacerbate issues**

Recommendations

- Some retrospective attention to requirements should be paid:
  - Does their relative depth reflect the original goals? i.e., are more intrusive/demanding requirements still quick and practical?
  - Does the assurance obtained remain valid for the production Product?
- The communities developing protection profiles should also develop or identify tools or at a minimum, define basic test procedures
- The oversight bodies need to ensure that evaluator tools and procedures are acceptable to perform the required Test Assurance Activities
- The Test Assurance Activities should acknowledge that many test cases might be supported or even implemented by product developers and should be clear about evaluator requirements (reporting, level and demonstration of understanding, etc.) in those cases

Questions?

Contacts:

- Ed Morris
- **(easy questions only, please)**
  - EdMorris@gossamersec.com
- Tammy Compton
- **(for all hard questions)**
  - TammyCompton@gossamersec.com

www.gossamersec.com
www.facebook.com/gossamersec
@gossamersec