First Hand Experience from a Network Devices Protection Profile Evaluation

Tammy Compton, James Arnold, Tony Apted

September 19, 2012

Topics

- Project Background
- NDPP Specific Observations
- Related EAL2 Project Observations
- Recommendations

Project Background

- 3 Families of Products – 2 groupings
  - Switches
  - 2 sets of Firewall appliances
- Network Devices Protection Profile (NDPP)
  - Switches
- Traffic Filter Firewall Protection Profile (TFPP) – EAL2
  - Firewall appliances

Evaluation Startup

- Switch Products
  - EAL 1 Security Target work units performed
  - No oversight meeting required
  - In evaluation June 2011
- Firewall Products
  - EAL 2 Security Target work units performed
  - Held initial Validation Oversight Review (iVOR) meeting
  - Addressed identified iVOR issues
  - In evaluation June 2011

Evaluation Timeline

- NDPP evaluation started in earnest in late October 2011
  - Delayed for product release
- All analysis work done in November
  - EAL 1 Common Evaluation Methodology (CEM) work units
  - Design- and guidance-related assurance activities
- Testing completed in December
  - Test-related assurance activities
- Completed package submitted for Validation in early January 2012

Design Observations

- Target of Evaluation (TOE) Summary Specification (TSS) as functional specification
  - Minimal information for network interfaces
  - Guidance documents complete for administrative interfaces
- TSS for assurance activities
  - Specific information required to be present
  - Not all information tested or even validated (e.g. RFC claims)

Guidance Observations

- EAL1 Guidance requirements the same as EAL2
- Assurance activities
  - Identify specific guidance details that must be checked
  - For the most part the required guidance is an interpretation of the guidance assurance requirements
  - List of processes is an odd guidance requirement, particularly if there is no interface to list them

Testing Observations

- No vendor testing required
- All evaluation team tests derived from the NDPP
  - Test Plan reusable for other NDPP evaluations
  - Testing effort 1 week – multiple models
  - Equivalency argument for multiple, related models accepted
  - Involved many network packet captures
  - Many non-TOE components
  - Relatively uncomplicated test concepts

Stumbling Blocks

- Reporting Expectations
  - Unclear what information the Scheme wanted
  - Scheme wanted to release information the lab and developer felt was proprietary
  - Substantial delays in rounds of review
- Entropy
  - NDPP version 1.0 required a TSF-independent hardware source
  - Waited for NDPP version 1.1
  - Delays with NSA review

EAL2 Comparison - Timing

- Schedule
  - Started in earnest in late October 2011 as well
  - Test Validation Oversight Review in May 2012
  - Final Validation Oversight Review in July 2012
  - Done and waiting Federal Information Processing Standard (FIPS) certification
- Bug Fixes
  - All products changed to meet Protection Profile audit requirements

EAL2 Comparison - Analysis

- Design Analysis
  - Longer than NDPP
- Testing
  - About the same level of effort but less focus on team tests
  - All SFRs tested with exception of FDP_RIP.1
  - Used same model equivalency argument
  - More vulnerability testing

Benefits

- Process now more defined for Standard Protection Profile-based evaluations
  - Relatively brief evaluation check-in
  - Synchronization meetings held after the TSS and guidance have been evaluated according to the assurance activities
- Some NDPP SFRs have changed
  - Audit of cryptographic failures removed
  - Entropy can now be based on hardware and/or software

Recommendations

- There should be a standard report template to be used for Stand Protection Profile-based evaluations
- There should be no nation- or Scheme-specific requirements or evaluation activities – in particular the required NSA review of entropy information is not internationally correct
- The terms and process for any pioneering evaluation efforts should be well-established and agreed prior to commencing any such projects.

Questions?

Contacts:

- Tammy Compton
  - TammyCompton@gossamersec.com
- James Arnold
  - JamesArnold@gossamersec.com
- Tony Apted
  - Anthony.J.Apted@saic.com