EQUIVALENCE WORKING GROUP

Cryptographic Module Users Forum

Product factors

- Many vendors have several options for products that are not security relevant:
  - Power
  - Airflow
- Often these can be excluded per AS01.09
- **However components can't always be excluded from the boundary of the module.**
  - E.g. Memory and processors

Current challenges

- Certifications are expen$ive
  - Capital expense
  - Manpower
  - Lab and NIST Fees

Current Solutions?

- Test Everything – in the absence of guidance, labs must test all combinations of hardware
- This is not practical or sustainable
- How do we balance efficiency and expediency with assurance?

Mission Statement

- The Equivalence Working Group will work towards a recommendation in the form of draft Implementation Guidance (IG) to the CMVP to reduce the overall amount of testing by considering some technologies/components “equivalent”.

Draft IG

- **Problem:** In the case where a vendor wishes to group multiple hardware modules in the same report, and therefore on the same certificate, under what conditions can the lab perform limited operational testing on the group of modules and still provide the assurance that all of the modules meet the FIPS 140-2 standard? What is the minimum set of "limited testing", if any, that must be performed by the lab?

Assumptions

- This IG only applies to Operational testing of Hardware modules
- There are multiple modules per IG 1.22 and these modules meet the CMVP requirements for grouping in a single report
- Physical testing (section 4.5) is not addressed for level 2 and above. In other words this IG will not exempt the lab from performing physical security testing for modules at Level 2 or above. This is because the lab needs to examine each module for, e.g., opacity and tamper evidence, if there are physical differences between the modules. **However, equivalency arguments can still be made for operational testing.**

Sample table of HW components

- Equivalency arguments/reports based on HW factors and their associated security relevancy
- Table of components
  - Storage/Memory
  - CPU
  - Power/Airflow
  - I/O
- Minimum test suite required

Towards a Resolution

- **Still need to determine:**
  - Component groups and their associated Minimum test suite (types of testing)
    - Full test
    - Partial test
    - No test?
  - What goes on the certificate?

Sample process

- Vendor Produces Equiv Report Based on Equiv table and IG

- Vendor Report sent Lab

Lab agrees/disagrees

- Report sent along with module submission to CMVP

- Equivalent models are shown on certificate

Next steps…

- Work on components list and minimum testing requirements for each…