Security Policy & Remote Testing
Working Group Updates

ICMC 2017
About Me

Ryan Thomas
Laboratory Manager, Acumen Security
rthomas@acumensecurity.net
Update Security Policy WG

Is it time to get the band back together?
Security Policy Working Group

- Group focused on some of the important information that needs to be captured in the FIPS 140-2 Non-Proprietary Security Policy document
- SPs were inconsistent when it come to how things like TLS, IKE, DRBG were being listed
- Included: Approved, Allowed and Non-Approved Algorithms Tables, Keys and CSPs Table, Approved and Non-Approved Services Table
- Develop a workable mapping between the Tables.
The Security Policy document as we know it today may be evolving as a part of the CMVP automation that is underway.

Group is on pause until we have a better understanding of what the documentation requirements will be post-automation.

Latest work is on the CMUF portal.

Is there interest in restarting this effort?

Or .. should we spend our time elsewhere?
Remote Testing Working Group
Remote Testing Working Group

First, let's recognize the contributors!

- Yi Mao, Atsec
- Jonathan Smith, Cygnacom
- Ryan Horan, NIST (CMVP)
- Others at CMVP
Remote Testing Working Group

• CMVP Manager’s Manual states hw must be tested in-person at vendor or lab premises.

• It doesn’t specify define how sw must be test (it does with hw)

• CMVP have stated remote testing of sw is currently not permitted …. Don’t shoot the messenger

• We are a forward looking certification program 😊
Many times there is no technical difference to testing while physically present or testing over a Remote Testing Environment (RTE).
Remote Testing Working Group

- How must we obtain equivalent assurances for a RTE?
  - Module’s boundary and must be version consistent with SP
  - OS, module version, processor family and hw platform model must be consistent with CAVP certificates (as required by IG G.13)
Remote Testing Working Group

Some other conditions that must be satisfied:

- RTE must be authorized and controlled by the vendor (more on this in a bit)
- Testing must be conducted over secure network protocols
- Tester must have the ability to control operational environment module is tested on
- Tester must be able to install, initialize and/or start the module while connected to the RTE
Remote Testing Working Group

- Testing over a TRE must cover the same set of FIPS 140-2 requirements:
  - All module services need to be invoked
  - Role-based (for L2) or identity-based (L3) authentication performed
  - Induction of self-test failures and module error handling
  - Single-user requirements

Lab’s test report will document how the above conditions are met.
Remote Testing Working Group

“A cloud system shall not be used”

• Hardware is hosted at a 3rd party site
• Vendor/lab likely do not have the type of control required by the proposed IG
• Very difficult to obtain the same level of assurance
Remote Testing Working Group

• Many times in my experience labs/vendors have to find creative solutions to demonstrate conformance to the requirements - this is no different.
• Many vendors have limitations on distribution of module source code.
• So, a combination approach could be taken. Some requirements tested remotely and some done in person.

Lab has discretion – but can check with CMVP
Remote Testing Working Group

• Careful what you ask for. This could potentially be more work ...
  – Lab has to defend their approach and that the testing is equivalent to in-person testing
  – Vendor has to provide a signed letter (to lab) describing the remote access connection and integrity of test results
Remote Testing Working Group

- Draft sent out to CST laboratories April 28th, 2017
- Comments due June 9th, 2017
- Talk to your lab to get a copy or send me an email 😊
rthomas@acumensecurity.net

www.acumensecurity.net