Adding to the Approved List of Algorithms (C16)

Kelvin Desplanque (Cisco Systems), Tony Busicglio (Acumen Security), and Dr. Lily Chen (NIST)

5 November, 2015

Kelvin Desplanque (Cisco Systems), and

Tony Busicglio (Acumen Security)

5 November, 2015

Introductions

- Kelvin Desplanque – TME, Cisco Systems, Inc. (AKA the Vendor)
- Tony Busciglio – Co-founder, Acumen Security (AKA the Lab)

Identifying the need for either a new algorithm or an enhancement to an existing algorithm.

- A vendor sees an opportunity where either an entirely new cryptographic algorithm/protocol, or an enhancement to an existing algorithm/protocol would improve either the capabilities or the efficiency of some cryptographic service.
- In the ideal world, the person(s) responsible for coming up with this enhancement gives the certification team sufficient advance notice of what they are planning.
- … unfortunately this is not an "*Ideal world*".

cisco Acumen Security NIST

Identifying the need for either a new algorithm or an enhancement to an existing algorithm (cont.)

- Inject yourself into the product design lifecycle, even if you are not particularly welcome there. Observer status is just fine.
- Don’t trust anyone … and remember that it’s not personal.
- Read as much of the new product design documentation as you can get your hands on.
- Perform a thorough FIPS gap analysis. If something appears to be cryptographic in nature, and was not previously validated, assume that it is indeed “new”, and ask lots of questions.
- Resolve any doubts with both the Program Managers and Sales.

Identifying the need for either a new algorithm or an enhancement to an existing algorithm (cont.):

- Remind the designers that you are the FIPS subject matter expert, not the chip vendor who appears to have read the FIPS document for the first time during a lunch break sometime last week.
- Be honest with the product team with respect to your assumptions and clearly communicate to them the potential negative implications of their enhancement.
- Let them know that non-FIPS approved cryptography might take considerable time to be accepted by the CMVP (NIST) … or it may never happen.

Informal Approach: Seeing how this new algorithm/protocol could fit into the FIPS 140-2 validation scheme (Vendor)

- The vendor's certification team initiates dialogues with an NVLAP accredited FIPS test lab, and the proper groups at NIST (CMVP, CAVP, CTG, etc.) to see how such a new or enhanced cryptographic algorithm/protocol could fit into the FIPS 140-2 framework.
- Determine if there is wider industry acceptance of the new or enhanced method which is supported currently (or in the foreseeable future) by one or more of the domestic or international standards bodies (e.g. IEEE, IETF, ANSI, ITU, etc.)

Informal Approach: Seeing how this new algorithm/protocol could fit into the FIPS 140-2 validation scheme (NIST)

- What is NIST's perspective on your proposal?
- You will just have to wait for Lily Chen's slides on this …

Formal Approach (Vendor):

- Follow the proper steps in order to communicate to NIST that you, as a cryptographic product vendor, wish to propose either a new or enhanced algorithm/protocol for inclusion within the FIPS 140-2 framework.
- Determine precisely what the Vendor, Test Lab and NIST must do in the respective roles they must play in the formal approach to adding new or enhanced algorithms or protocols to the FIPS 140-2 framework.

Formal Approach (Lab):

- Any question/clarification of requirements can be clarified by submitting a Request for Guidance (RFG)
- Two types:
  - Informal: Considered as ad hoc. Not appropriate for algorithm consideration.
  - Formal: Official request must be submitted to the CMVP. This is the applicable option.
- After request is submitted the CMVP, the request is handed off to the CTG group which considers the proposed algorithm.
- After an amount of time, a yes/no decision is returned.

cisco Acumen Security NIST

Formal Approach (Lab) (cont.):

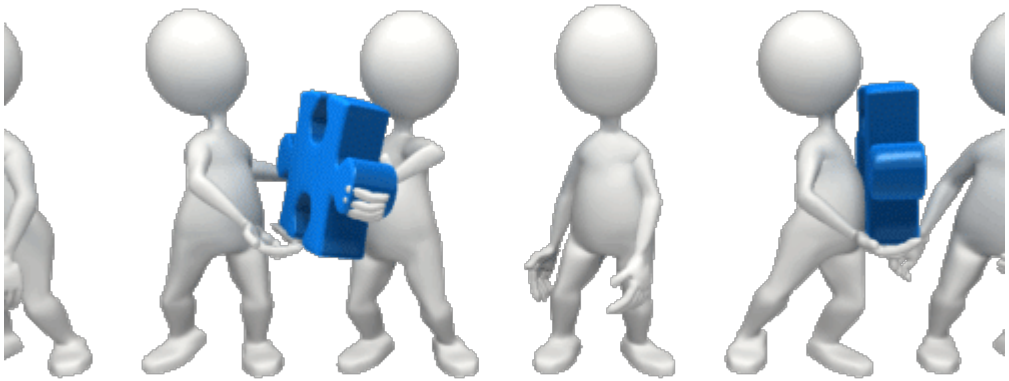
- RFG Content:
  - Indication of PROPRIETARY/NON-PROPRIETARY,
  - Descriptive title,
  - Applicable statement(s) from FIPS 140-2,
  - Applicable assertion(s) from the FIPS 140-2 DTR
  - Applicable required test procedure(s) from the FIPS 140-2 DTR,
  - Applicable statements from FIPS 140-2 Implementation Guidance,
  - Applicable statements from cryptographic algorithmic standards,
  - Background information if applicable,
  - A concise statement of the problem, followed by a clear and unambiguous question regarding the problem, and a suggested statement of the resolution that is being sought.

Supporting the Submission (Vendor & Lab)

- Complete RFG with details for each of the identified sections.
- Pointers to international/recognized community acceptance.
- Heuristic analysis of the strength of the new algorithm.

Supporting the Submission (Vendor-Lab-NIST)

- During the study phase by NIST, the vendor (with the support of the lab) may be required to provide supplementary information or test data in support of their proposal as required.



The Decision (Vendor)

- The program (NIST) comes to a decision – either **YES** or **NO**.

The Decision (NIST/CMVP)

- If YES, what happens next with respect to formalizing the decision and embedding the new or enhanced algorithm/protocol within the FIPS 140-2 framework?

The Decision (NIST/CMVP)

- If NO, what steps can a vendor and their selected test lab take to either appeal the decision, correct the proposal, or reach some mutually agreeable compromise in order to have the proposal reconsidered for approval?

Follow-on steps (NIST/CMVP)

- After accepting the submission, how does the CMVP deal with either accepting vendor attestation of the new or enhanced algorithm/ protocol?
- How does the CMVP include provisions for POSTs/KATS/Conditional Tests (if necessary), standards' documents revisions, etc ?
- … and how does the CAVP proceed with providing a proper test mechanism for this so that that it may validated and subsequently be listed on the CAVP algorithms pages?

Part II … and now for the NIST take on this


CISCO


Acumen Security


NIST