Booz | Allen | Hamilton

CYBER

FIPS!... I Did It Again

Justin Fisher, CST Technical Director

May 19th, 2017

CYBER SOLUTIONS

Background

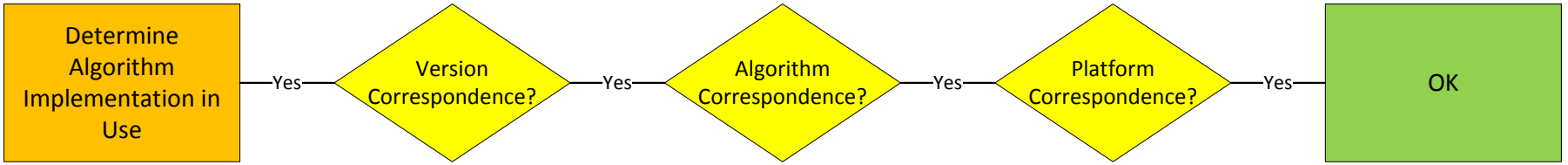
+ ***NIST provides a framework to evaluate large amounts of security and functionality of interest to the Common Criteria community***
+ ***Common Criteria evaluations in the US are designed to take advantage of this, but there are limitations***
+ ***Understanding what does and doesn't overlap helps vendors manage certification test planning***

CAVP + CC Overlap

+ ***NIAP and collaborative PPs define a lot of security functionality that is directly testable under CAVP***
  - ***Asymmetric key generation and establishment***
  - ***Symmetric encryption/decryption***
  - ***Deterministic random bit generation***
  - ***Just to name a few…***
+ ***Collaborative PPs typically use ISO language for cryptographic requirements but the algorithms and their operating parameters (key sizes, modes, etc.) are usually consistent with FIPS 140-2 Approved algorithms***
+ ***Assurance Activities are generally derived from NIST Validation System documents***
+ ***According to NIAP Policy Letter #5, CAVP certificates must be used to satisfy the relevant cryptographic algorithm testing***

CAVP + CC Overlap Decision Process

+ ***To determine if an algorithm implementation can be used for an evaluation, the vendor/ST author must perform several suitability checks***



+ ***If any of these checks fail, corrective action is required!***

Determine Algorithm Implementation in Use

+ ***The first step in figuring out if a TOE can satisfy the CAVP requirements is to understand what algorithm implementation is being used***
+ ***This may be a full standalone FIPS module or it can be a CAVP-only algorithm implementation (for now)***
+ ***For vendors that do a large volume of evaluations, use of a single shared library across multiple products is typical***
+ ***Expectation is to identify the initial set of CAVP certificates that you expect to apply so that they can be examined in detail***

Version Correspondence

+ ***Every algorithm implementation has a version associated with it (hardware/software/firmware/ hybrid)***
+ ***If an ST author wishes to claim CAVP certificates for an algorithm implementation, the version of the implementation used must be the same as what appears on the corresponding validation list(s).***

OpenSSL FIPS Object Module

Version 2.0.14

Algorithm Correspondence

+ ***Algorithm correspondence is determined by multiple checks:***
  - *For each of the cryptographic algorithm SFRs, is the remainder of the ST consistent with the SFR?*
  - *For each of the cryptographic algorithm SFRs, is there a corresponding CAVP certificate?*
  - *For each CAVP certificate, are the claims made in that certificate consistent with the ST?*
  - *For each CAVP certificate, are the claims made in that certificate suitable to meet NIAP Policy Letter #5*

FCS_RBG_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

Hash_Based DRBG: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (SHS Val#3411)] **HMAC_Based DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512) (HMAC Val#2714)]

CTR_DRBG: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_Use_df: (AES-128 , AES-192 , AES-256) (AES Val#4141)]

BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES Val#4141)]

CTR_DRBG(AES)	DRBG Validation List CTR_DRBG[(AES-128 v AES-192 v AES-256) **NOTE**: DRBG Val# must correspond to AES-128 v AES-192 v AES-256 Val#(s)]

Algorithm Correspondence (Continued)

+ ***Emphasis here is also on ST consistency, not just consistency with the Policy Letter***
  - *A security algorithm claim must include the sum total usage of the algorithm in all other security functions.*
  - *Example: a claim of AES-CBC is not sufficient if the TOE claims both CBC and GCM in its SSH implementation.*
  - *Check this first so that CAVP correspondence (and eventual testing, if needed) only needs to happen once.*
+ ***The algorithm certificate can (and often will) claim more than what the ST does***
  - *Subsequent CC evaluation activities will show that the TOE's cryptographic functionality can be limited to what is claimed in the ST.*
+ ***If the policy doesn't require a specific option to be chosen, any value for it is permissible***
  - *Example: CTR_DRBG(AES) is satisfied via DRBG Validation List, CTR_DRBG[(AES-128 v AES-192 v AES-256)].*
  - *Presence/absence of derivation function, use/non-use of prediction resistance, reseed is/is not implemented, and number of output blocks can all be specified when generating the test vectors for this function. Some of this may show up on the algorithm certificate but none of it is used to determine whether Policy Letter #5 is satisfied.*

Algorithm Correspondence (Continued)

+ ***Most algorithm correspondence is relatively straightforward to show***
+ ***The major question most people have is on FCS_CKM.1 and FCS_CKM.2***
  - *[NDcPP case study] These are used for trusted communications protocols (TLS, SSH, IPsec).*
  - *RSA is always necessary when TLS is claimed because of the mandatory ciphersuite.*
  - *Either FFC or ECC is necessary when SSH is claimed for either Diffie-Hellman Group 14 or ECDH-SHA2.*
  - *FFC is necessary when IPsec is claimed for Diffie-Hellman Group 14 and ECC is necessary if DH Groups 19 and/ or 20 are selected.*
+ ***FCS_CKM.1 requires conformance to FIPS 186-4***
  - *Many older algorithm validations do not conform to this - differs from FIPS 186-2 and so an older implementation may not be able to meet this without a code change.*
+ ***FCS_CKM.2 requires conformance to either KAS or CVL for FFC***
  - *CVL testing is used when the implementation conforms to all of 800-56A but key establishment.*
  - *KAS FFC/ECC is used when the implementation is fully conformant to 800-56A.*
  - *There is currently a conflict between 800-56A and Diffie-Hellman that the CC Network iTC is working to resolve.*
  - *There is also vendor affirmation of SP 800-56A-rev2 under FIPS 140-2 IG D.1-rev2, which is an entire topic on its own!*
+ ***FCS_CKM.2 requires vendor assertion for RSA***
  - *NDcPP defines a specific assurance activity for this but there is no NIST counterpart and so vendor affirmation under FIPS 140-2 IG D.4.*

Platform Correspondence

+ ***Every algorithm implementation is tested on one or more platforms based on the implementation type:***
  - *Hardware – part number*
  - *Firmware – processor*
  - *Software – OS and processor*
+ ***Ideally, the TOE will use the exact same environment as what was tested, but this is not always realistic.***
+ ***NIAP allows for equivalency FOR SOFTWARE ONLY, within limits:***
  - *OS: minor version differences are acceptable*
  - *Processor: must be same manufacturer in same family*
  - *All use or non-use of hardware acceleration (e.g. AES-NI) must be the same in both the CAVP certificate and the ST.*
+ ***NIAP guidance on this supersedes any comparable NIST guidance, e.g. IG G.5***
+ ***If there is any question as to equivalence, contacting NIAP/test laboratory is recommended***

Cavium Octeon II (MIPS) w/
ExtremeXOS-Linux 3.1

Corrective Actions

+ ***Several options for a vendor to pursue, but each has its own challenges***
+ ***If the issue is version correspondence:***
  - *It is generally recommended that the vendor use the latest version of what has been certified.*
  - *If the vendor is using a new version that hasn't been tested yet the possibility of being forced to downgrade is a point of frustration.*
+ ***If the issue is algorithm correspondence:***
  - *In many cases the algorithm implementation meets requirements above and beyond what the vendor decided to test – in these cases additional testing may be done and approved without code changes.*
  - *For some cases, the vendor may have no choice but to implement a code change.*
+ ***If the issue is platform correspondence:***
  - *The vendor may attempt to provide a justification to NIAP as to why the TOE platform is sufficiently similar to existing validations to be equivalent.*
  - *If no equivalency argument is feasible, re-testing may be needed.*
+ ***If the vendor does not control the source code, corrective action through a third party may be logistically difficult.***

Module Overlap (NDcPP Case)

+ ***CMVP module validation isn't required for CC but there are areas where it may help***
+ ***The entropy assessment required by many PPs is similar to what is required by FIPS 140-2 IG 7.14***
+ ***A validated module will perform self-tests and this evidence can be used to satisfy FPT_TST_EXT.1 requirements***
+ ***A validated module may perform some audit functions of cryptographic operations, which can be used to satisfy part of FAU_GEN.1 requirements***
+ ***A validated module will perform secure key storage which addresses FPT_SKP_EXT.1 requirements***
+ ***Note the caveat that many software modules place significant responsibilities on the calling application – in these cases it is the responsibility of the TOE developer to ensure that the module is being implemented in the manner specified in its Security Policy in order to be able to assert that the requirements are being met***
  - *A software library may rely on an OS for key storage*
  - *A software library may rely on an underlying hardware platform to supply entropy*

Summary

+ ***CAVP certificates may demonstrate that a TOE satisfies cryptographic requirements***
+ ***This may eliminate the need for duplicate testing but only if the TOE's configuration is consistent with what has already been tested***
  - *Using the right version of the implementation.*
  - *Ensuring the tested algorithms are consistent with NIAP guidance.*
  - *Verifying that the operational environment is consistent with what was used for CAVP.*
+ ***Ensuring that the ST is internally consistent before verifying the extent to which existing CAVP certificates can be relied upon is key to eliminating unnecessary effort***
+ ***When relying on a third-party cryptographic provider, corrective action is often difficult to arrange***
+ ***Module validation is not required for CC but if a module has been validated, vendors and evaluators should always be looking out for areas where the module can show that a CC requirement has been satisfied***

Questions?

Contact Booz Allen Hamilton to learn more

Justin Fisher

Booz Allen Hamilton Cryptographic Security Test Laboratory

(410) 694-3664

fisher_justin@bah.com

Involved in NIAP Technical Communities for:

+ *Full Drive Encryption*
+ *Software File Encryption*
+ *Enterprise Application Software*
+ *Dedicated Security Component*
+ *And More!*