Is Common Criteria the new FIPS 140?

What are we going to talk about?

- Introductions
- Background (FIPS 140/Common Criteria)
- Functional Comparison
- Testing Comparison
- Conclusions (Is CC the new FIPS 140)
- Looking Forward
- Questions

Who am I? I'm Tony B!

- How long have you been doing this stuff: 16 years*
- Where have you done it: Cert. Labs (x2), Vendor (x1)
- What have you done: Lot's stuff!
- What do you do in your spare time: Kids, lots of Kids!

* This means I'm old!

Who am I? I'm Clint W!

- How long have you been doing this stuff: 15 years*
- Where have you done it: Cert. Labs**, Vendor (x1)
- What have you done: A little bit of everything
- What do you do in your spare time: Hunt, Eat bacon!

* This in no way indicates that I am old

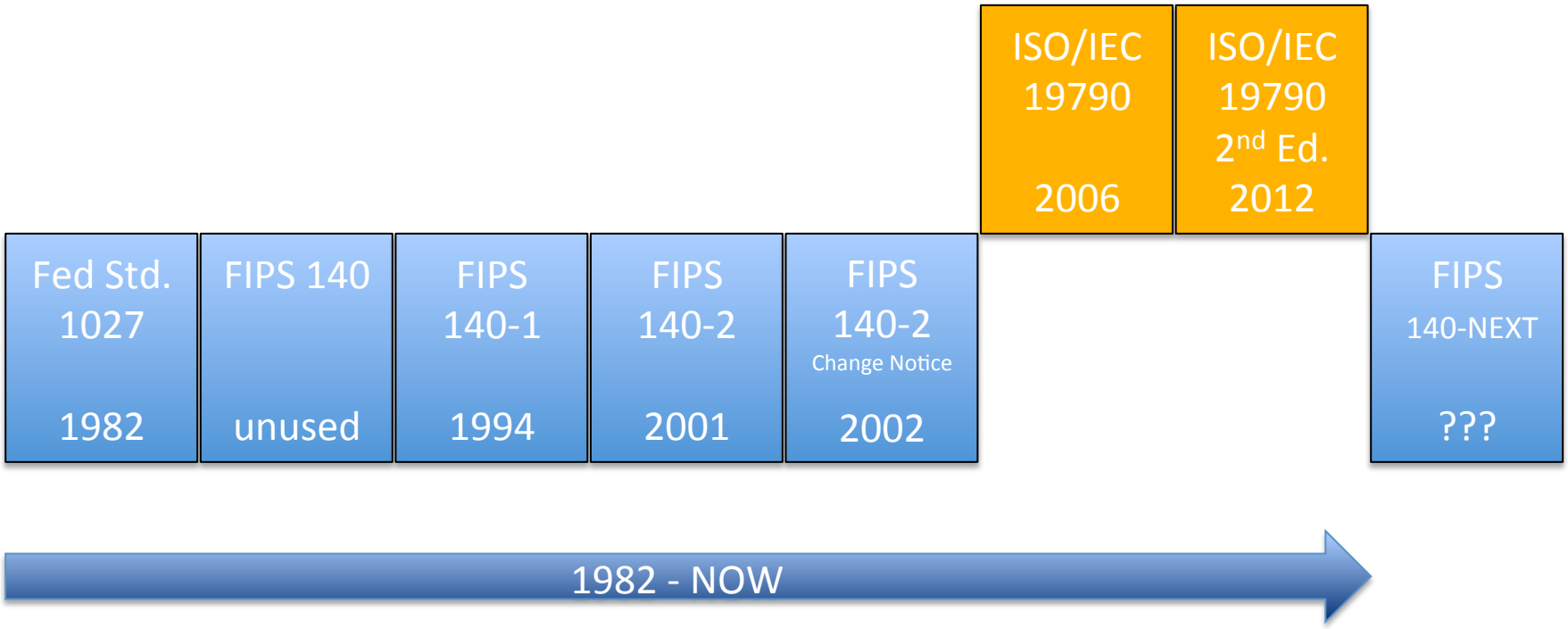
** I put the "s" in Cert. Labs

Is CC the new FIPS 140?

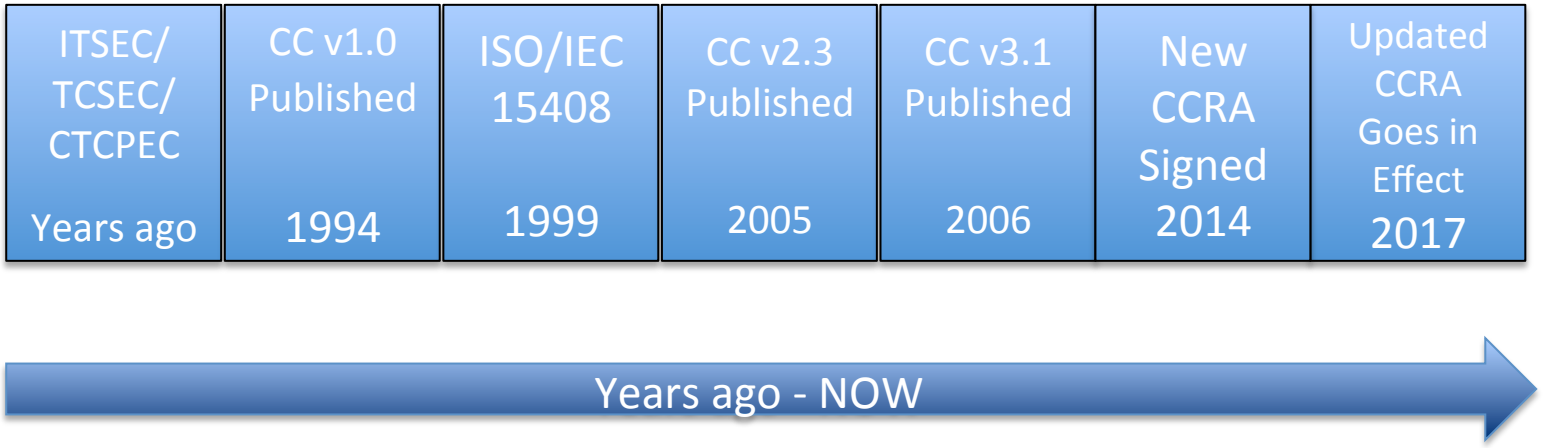
Acumen Security

Why is this a Question?

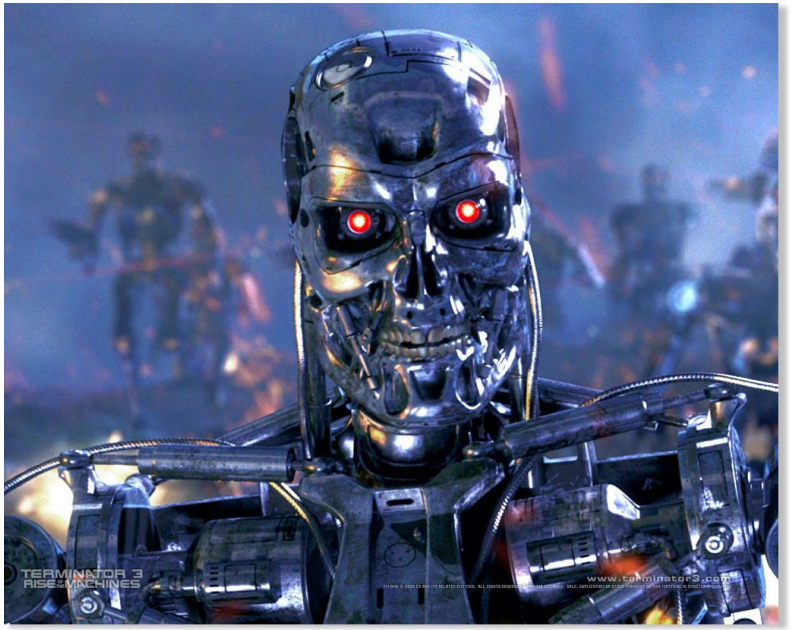
Tell us about FIPS 140 (History Lesson)

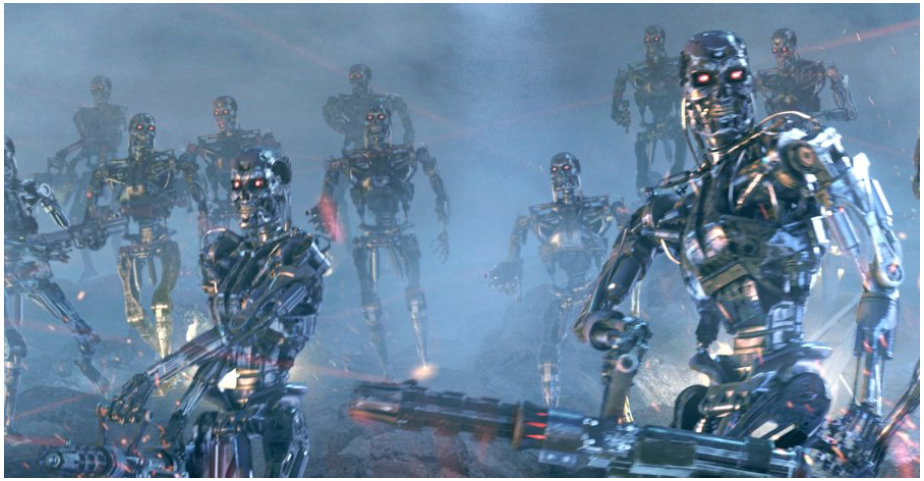


Tell us about Common Criteria (History Lesson x2)



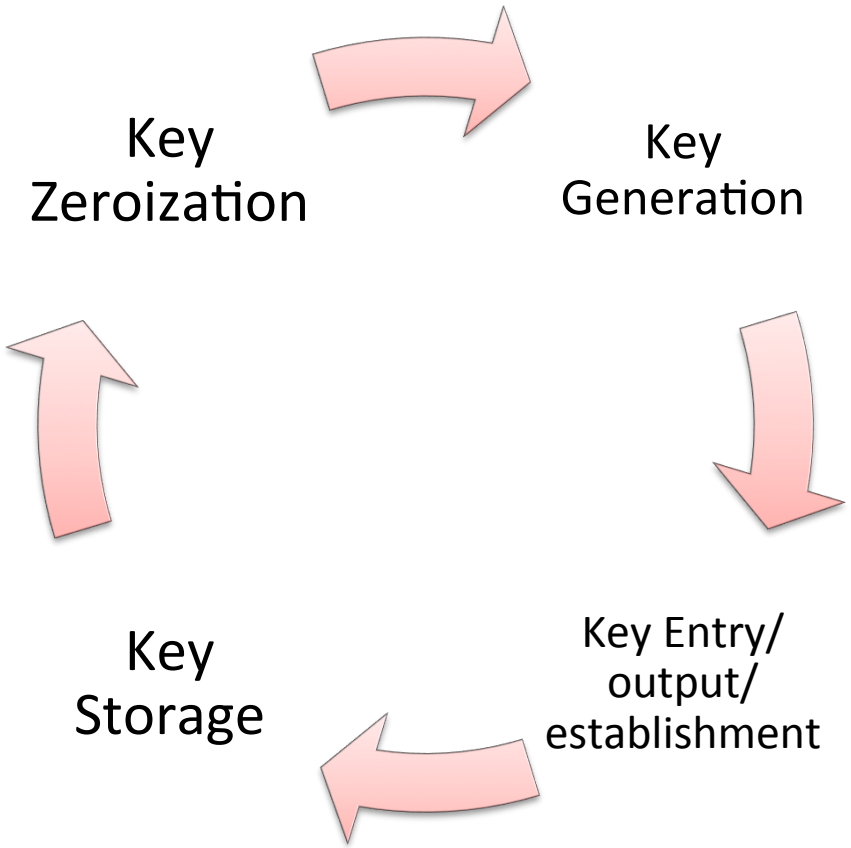
Rise of the Collaborative Protection Profile





You Show Me Yours, I'll Show You Mine!

Whatcha lookin' at FIPS 140?



Whatcha lookin’ at CC?

SHHH!!! Algorithms: What's Allowed?

FIPS 140

- Symmetric:
  - AES
  - TDES
- Hashing:
  - SHA-1
  - SHA-2
  - SHA-3
- MACing:
  - HMAC
  - CMAC
  - GMAC
- Signatures
  - RSA
  - ECDSA

Common Criteria

- Symmetric:
  - AES
- Hashing:
  - SHA-1
  - SHA-2
- MACing:
  - HMAC
  - CMAC
  - GMAC
- Signatures
  - RSA
  - ECDSA

Let’s make sure everything’s OK! What’s Allowed?

FIPS 140

- Algorithm KAT POSTs
- Integrity Test
- CRNGT
- Software Load Test
- Bypass tests
- Pairwise Consistency Test
- Key Entry Tests

Common Criteria

- Software Load Test
- Other tests as determined by the vendor

Let's make some keys! What's Allowed?

FIPS 140

- SP 800-90A DRBG
- SP 800-56A
- SP 800-108
- SP 800-132
- SP 800-135 KDF
  - TLS 1.0, 1.1, 1.2
  - SSH 2.0
  - IKEv1/IKEv2
  - SNMPv3

Common Criteria

- SP 800-90A DRBG
- SP 800-56A
- SP 800-135
- SP 800-108
- SP 800-132
- SP 800-135 KDF
  - TLS 1.1, 1.2
  - SSH 2.0
  - IKEv1/IKEv2

Let's put those keys somewhere! What's Required?

FIPS 140

- AS07.37: Cryptographic keys stored within the cryptographic module shall be stored either in plaintext form or encrypted form.
- AS07.38: Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorized operators.
- AS07.39: The cryptographic module shall associate the cryptographic key stored within the module with the correct entity to which the key is assigned.
- AS07.40: Documentation shall specify the key storage methods employed by the cryptographic module.

Common Criteria

- FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Clean up time! Key Destruction: What's Required?

FIPS 140

- AS07.41: The cryptographic module shall provide methods to zeroize all plaintext secret and private cryptographic keys and CSPs within the module.

Common Criteria

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [selection:

For volatile memory, the destruction shall be executed by a single direct overwrite [selection: consisting of a pseudo-random pattern using the TSF's RBG, consisting of zeroes] followed by a read-verify.

If the read-verification of the overwritten data fails, the process shall be repeated again.

For non-volatile EEPROM, the destruction shall be executed by a single, direct overwrite consisting of a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), followed by a read-verify.

If the read-verification of the overwritten data fails, the process shall be repeated again.

For non-volatile flash memory, the destruction shall be executed by [selection: a single, direct overwrite consisting of zeroes, a block erase] followed by a read-verify.

If the read-verification of the overwritten data fails, the process shall be repeated again.

For non-volatile memory other than EEPROM and flash, the destruction shall be executed by overwriting three or more times with a random pattern that is changed before each write.

Time to get our hands dirty: Testing Algorithms!

FIPS 140

- Symmetric Algorithms:
  - CAVP Testing
- Hashing:
  - CAVP Testing
- MACing:
  - CAVP Testing
- Signatures
  - CAVP Testing

Common Criteria

- Symmetric Algorithms:
  - CAVP Testing
- Hashing:
  - CAVP Testing
- MACing:
  - CAVP Testing
- Signatures
  - CAVP Testing

Time to get our hands dirty: Testing Key Storage!

FIPS 140

- TE07.39.01: The tester shall review the documentation on key storage and shall verify that the procedures address how a stored key is associated with the correct entity.
- TE07.39.02: The tester shall alter the association of key and entity. The tester shall then attempt to perform cryptographic functions as one of the entities and shall verify that these functions fail.
- TE07.40.01: The tester shall review the vendor documentation to verify that the information specified in VE07.40.01 is included

Common Criteria

The evaluator shall examine the TSS to determine that it details how any preshared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

Time to get our hands dirty: Testing Key Zeroization!

FIPS 140

- TE07.41.03: The tester shall initiate zeroization and verify the key destruction method is performed in a time that an attacker cannot access plaintext secret and private cryptographic keys and other unprotected CSPs while under the direct control of the operator of the module (i.e. present to observe the method has completed successfully or controlled via a remote management session). If the method is not under the direct control of the operator, then rationale shall be provided on how the zeroization method(s) are employed such that the secret and private cryptographic keys and other CSPs within the module cannot be obtained by an attacker.
- TE07.41.04: The tester shall verify that all plaintext secret and private cryptographic keys and CSPs that are not zeroized by the zeroize command are either 1) encrypted using an Approved algorithm, or 2)
- physically or logically protected within an embedded validated cryptographic module (validated as conforming to this standard).

Common Criteria

- The evaluator shall check to ensure the TSS lists each type of plaintext key material and its origin and storage location. Evaluation Activities for SFRs The evaluator shall verify that the TSS describes when each type of key material is cleared (for example, on system power off, on wipe function, on disconnection of trusted channels, when no longer needed by the trusted channel per the protocol, etc.).
- The evaluator shall also verify that, for each type of key, the type of clearing procedure that is performed (cryptographic erase, overwrite with zeros, overwrite with random pattern, or block erase) is listed. If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the clearing procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are cleared by overwriting once with zeros, while secret keys stored on the internal persistent storage device are cleared by overwriting three times with a random pattern that is changed before each write")

What all can we test?

FIPS 140

- Algorithm Correctness
- Key Creation
- Key Storage
- Key Zeroization

Common Criteria

Is CC the new FIPS 140?

Let's see, Yes or No!

Acumen Security

FIPS 140-What? Yup, CC is the New FIPS 140!

- Technology specific cryptographic requirements
- More specific/holistic testing
- Recognized in multiple countries
- Collaboratively developed functional and testing reqs

Nope, CC will never ever ever be the new FIPS 140!

- More flexible
  - Algorithms
  - Use cases
  - Product Types
- Less expensive
- More focused
- Deeper testing
  - Source review
- Procurements want it!

Ok, Ok, What's next?

Acumen Security

Coming Soon to a FIPS module near you!

- FIPS 140-3
  - Someday before I retire!
- More algorithms
- Automation
- More IGs!

Let's look into our crystal ball and *CC* whats in store!

- Updated functional requirements
- Updated testing requirements
- New use cases
  - More Protection Profiles
  - Modular Protection Profiles

Is CC the new FIPS 140?

You decide!

Acumen Security

Questions!

Acumen Security

Thank you!

Acumen Security