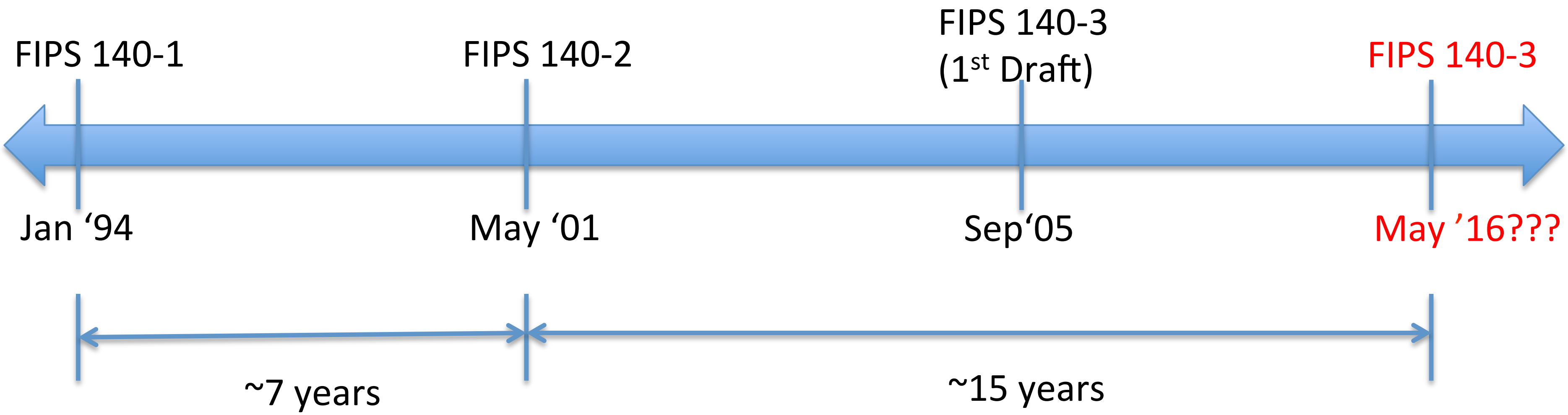
FIPS is FIPS, Real World is Real World and never the twain shall meet?

Ashit Vora, ICMC 2015

Acumen Security

FIPS Standard: A History



FIPS 140-1

Jan '94

FIPS 140-2

May '01

FIPS 140-3
(1st Draft)

Sep'05

FIPS 140-3

May '16???

~7 years

~15 years

FIPS 140-2 By The Numbers

Pages

Std	DTR	IG
69	127	63

# Of Requirements

287

50% are documentation

>50%

Requirements orthogonal to Crypto (Sections 3, 5 and 9)

Frequency of the word "key"

Std: 349 / 25235
DTR: 551 / 47230

OSSL Vulnerabilities

2013	2014	2015
5	22	26

# of time OSSL FIPS module updated since 2013

0

The Problem: Perception of FIPS

What CMVP thinks?

What Product Vendors think?

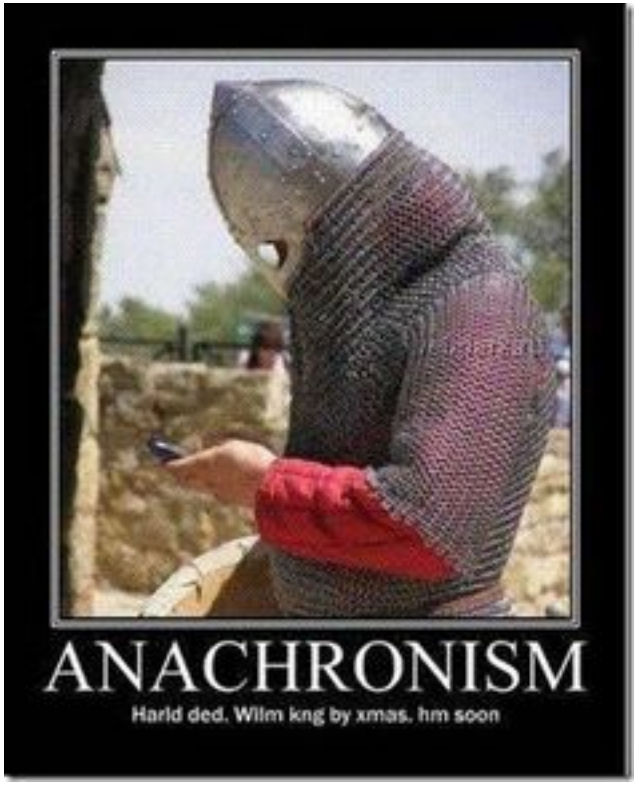
What Federal Agencies Think?

What it actually is?

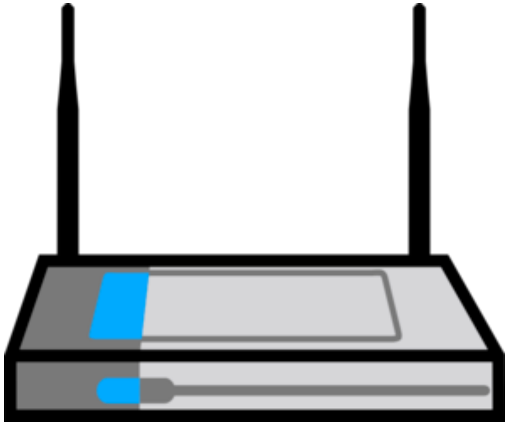
- A bit of everything above and a bit of nothing
- Ensures what is <u>claimed</u> has been implemented correctly
- At levels 1 and 2 little more assurance than the product implements crypto as per spec
- FIPS validation does not mean the overall “cryptographic posture” of the system is secure

How did we get here?

… With best of intentions. However FIPS is a...

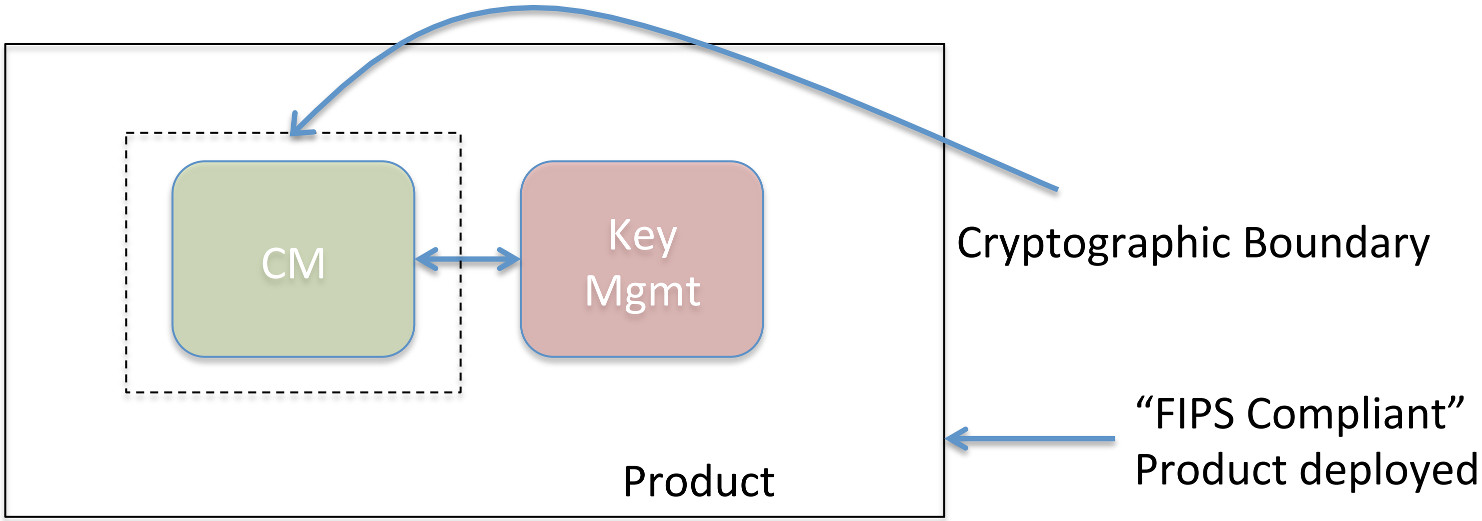


Real World v/s FIPS: Opacity



- COTS product -> easy to buy a product and open at your own leisure
- Causes vendors to downgrade to level 1 or design purpose built “opacity shields”
- Tamper labels in a similar vein add nothing to security posture of the product
- Products are rarely deployed with opacity shields and tamper labels
  - See access points at NIST, none of them have tamper labels

Real World v/s FIPS: Key Mgmt



- Possible to have a module FIPS validated without including key management at all
  - In fact most software libraries do not include key management
- This is a direct result of crypto boundaries shrinking
- At level 1 most software module validation give little assurance beyond proper implementation of algorithms

Real World v/s FIPS: Passwords

- Authentication requirements are rudimentary at best
- No consideration for password complexity, frequency of change, multi factor authentication etc
- PKI is not covered at all
- Gives a false sense of security

Real World v/s FIPS: OpenSSL

- OpenSSL is the most widely used cryptographic library in the world
- Most prevalent in networking products. But also commonly seen in software applications, IoT products etc
- Extremely common to claim FIPS compliance by the virtue of using FIPS validated version of OpenSSL FOM

HOWEVER…

- OpenSSL's FIPS validation does not cover any of the higher order protocols/ algorithms. E.g. TLS is outside of the crypto boundary
- Key Management is completely out of scope

The security assurance provided by OpenSSL's FIPS validation is little more than ensuring that the cryptographic algorithms are implemented as per specifications

Other Examples

- FCC, FSM and Configuration Management requirements -> Do not add security
- Software/firmware load test -> no requirement for root of trust

So How Do We Get Better?

- Stop considering the standard as the constitution or religious text
  - It is okay to change with time and technology progression
  - Follow the CC example: Use the standard as a base/toolkit and provide technology specific requirements (that map back to the standard)
- Do not tie validations to specific versions. Allow for minor changes/bug fixes
- Encourage and reward vendors to draw larger cryptographic boundaries
  - At least do not penalize them!
- Spend time, effort and energy on requirements that matter:
  - Section 1: Cryptographic Module Specification
  - Section 5: Physical Security (for levels 3 and 4)
  - Section 7: Cryptographic Key Management
- Focus on key lifecycle. Make those requirements more all-encompassing
  - Implementing cryptographic algorithms is easy
  - Managing and protecting keys is tough and that is where attacks will come from

Ashit Vora
avora@acumensecurity.net
www.facebook.com/acumensec
@acumensec

Thank You!

Apologies to Rudyard Kipling for borrowing from his poetry!