Revised on November 12, 2015
after presentation at ICMC 2015 on November 5, 2015

Proposed Changes for a Long Overdue Revision of FIPS 140-2

Francisco Corella
fcorella@pomcor.com
Karen Lewison
kplewison@pomcor.com

***Acknowledgement**: these slides have been revised based on feedback received during the presentation*

pomcor
pomcor.com

FIPS 140 is Out-Of-Date

- Federal Information Processing Standards (FIPS) are typically revised every 5 years
- FIPS 140-1: January 1994
- FIPS 140-2: May 2001
- FIPS 140-3: abandoned after drafts in 2007 and 2009
- Annexes and Implementation Guidance updates have provided revisions, but of limited scope

Technology Evolution Has Rendered FIPS 140-2 Obsolete

- Mobile devices have changed the computing landscape
  - by replacing PCs for some applications
  - by replacing smart cards for other applications
  - by enabling new kinds of applications
- FIPS 140-2 has become obsolete because it is incompatible with mobile technology
  - ISO 19790 has been suggested as a replacement of FIPS 140-2 but only makes incremental changes to FIPS 140-2 and has also become obsolete

FIPS 140 Must Be Rethought

- Three things that must change
  - Allow data encryption as alternative to tamper resistance
  - Eliminate most self-tests
  - Rethink certification
- Caveat: one thing that should not change
  - Mitigation of side channel attacks (contemplated in Section 4.11 of FIPS 140-2 as possible in future versions) should stay out of scope

Encryption vs. Physical Security

- FIPS 140-2 relies on physical security to define security levels
  - Tamper evidence required for level 2
  - Tamper resistance and/or response for levels 3 and 4
- Mobile devices rely on encryption for key/data protection
  - iOS: File and key encryption with a hierarchy of data encryption keys
  - Android: “Full disk” encryption
  - BYOD device management: enterprise data and keys segregated in encrypted containers

Encryption in FIPS 140-2

- Encryption does play a role in FIPS 140-2, but a very limited one
  - FIPS 140-2 requires key zeroization in some scenarios, but encrypted keys are exempted from the requirement
- No concept of hardware/cloud roots of trust for the derivation of key-encryption keys
  - Key-encryption keys must be derived from a user-supplied password (IG 7.16 refers to SP 800-132)
  - But that would require a very high entropy password capable of withstanding an offline guessing attack
  - And high or even medium entropy passwords are not practical on mobile devices
- Encryption cannot be used to claim a higher security level

Suggested Changes re Encryption

- Allow encryption as an alternative to physical security at levels 2 and 3
- Allow encryption in addition to physical security to achieve level 4
- Allow encryption keys to be derived from a physically protected key and/or a key stored in the cloud

Online Authentication Methods for Retrieving a Key-Encryption Key from a Key Storage Service to a device hosting a cryptographic module

1. Password
   - Immune against offline guessing attack after device capture
2. One-time password (OTP) generated by or delivered to separate device
3. Two-factor authentication (2FA) with PIN or password plus OTP
4. 2FA with key pair stored in the clear plus PIN or password
5. 2FA with key pair stored in the clear plus OTP
6. 2FA with key pair + PIN, with PIN hashed with public key in service database
   - PIN immune against offline guessing attack after breach of service database
7. Key pair regenerated from protocredential and PIN
   - PIN immune against offline guessing attack after device capture

Disclosure: *Pomcor has intellectual property related to methods 6 and 7, including patents pending, and US patent 9,185,11 specifically related to method 7*

Rethinking Self-Tests

- Self-tests drain the battery and increase latency in mobile devices
- Power-on self tests do not make sense in mobile devices
  - A mobile device only loses power if the battery is removed
- Self-testing an algorithm against a test vector stored with the algorithm serves no purpose
  - Attacker who is able to change the algorithm is also able to change the test vector and/or the testing procedure

Rethinking Self-Tests (Continued)

- Continuous testing of a random bit generator (RBG) makes sense, but…
  - FIPS 140-2 calls for testing the output of the RBG
  - What should be tested instead is the output of the NOISE SOURCE, as specified in SP 800-90B
- Suggestions
  - Require continuous testing of noise sources of RBGs, if noise sources are used
  - Eliminate the algorithm self-tests

Rethinking Certification

- Certification is impossible for a cryptographic module implemented by software running on a commercial mobile device under a commercial mobile OS:
  - Hardware, OS, and software must be certified together, but are supplied by different entities
  - Hardware, OS, and software change too frequently, and on different schedules

Suggested Changes re Certification

- Allow separate role-specific certification of module components (e.g. hardware, OS, software)
- System integrator builds module using the components and requests certification based on the prior certifications of the components
- Allow independent revalidation of different components at different times without requiring revalidation of the module

Caveat: Avoid Requirements to Mitigate Side-Channel Attacks

- Section 4.11 of FIPS 140-2 suggests that requirements to mitigate side-channel attacks may be added to the standard in the future
- Preventing side-channel attacks is essential, but not necessarily the responsibility of a cryptogaphic module
  - Side-channel attacks can be prevented effectively by *protocol-level* countermeasures
    - E.g. blinding can prevent timing and electromagnetic attacks
  - But efforts to prevent *algorithmic-level* leakage are onerous and of limited effectiveness

Conclusion

- Mobile devices have made FIPS 140-2 obsolete
- FIPS 140-2 must be rethought
  - Major changes are needed, incremental changes are not enough
  - ISO 19790 is obsolete as well
- The proposed changes would help make a future version of FIPS 140 relevant to mobile devices

Thank You for Your Attention

- Contact us for additional information and discussion:

  Francisco Corella:
  fcorella@pomcor.com
  +1.619.770.6765
  Karen Lewison:
  kplewison@pomcor.com
  +1.669.300.4510

- Or check our site and blog

  pomcor.com
  pomcor.com/blog