Check Point
SOFTWARE TECHNOLOGIES LTD

FIPS 140-2 VENDOR EXPERIENCE

Fitting a square peg in a round hole

Malcolm Levy | Certification Manager

WELCOME TO THE FUTURE OF
CYBER SECURITY

CLOUD • MOBILE • THREAT PREVENTION

Agenda

- Vision
- Challenges
- Processes
- Recommendations

Certification vision

- Provide Check Point certified solutions that meet customer needs
  - According to regulatory requirements
  - For all customer certification requirements (not just FIPS 140-2)
  - Useful certified solutions in the evaluated configuration
    - To reduce their risk
    - To meet their business needs
  - Provide the certification within a short time of the product release
  - Allow customers to always use certified systems – and remain certified during updates!!

US Government required certifications

- FIPS 140-2
- Common Criteria (PP based)
- NSA CSFC
- DISA (UCCO)
- USGv6

Non-product:

- FISMA
- FedRAMP

Challenges in certifying

- Certifications are not aligned
- Times to certify vary greatly
- Products are constantly evolving

FIPS 140-2 challenges

Check Point
SOFTWARE TECHNOLOGIES LTD

- Standard leads to prescriptive evaluations
  - Neither CMVP or labs are willing to look beyond their current outlook
- Evaluations get bogged down in the detail
- Time to evaluate is many times too long
- Certifications always lag behind product releases
- Process is like a blind tunnel
- Much of the certification process is of little relevance to actual deployments

Problem with modelling the module

Check Point
SOFTWARE TECHNOLOGIES LTD

- A module must be must be presented as software/firmware/hardware/ hybrid
  - According to the presentation the requirements change!!
- Customers buy products and not modules
- Lack of pragmatism
  - Contradictory requirements result in definition of a FIPS 140-2 mode that is lab tested and rarely used
- FIPS 140-2 terminology does not equate to R&D usage eg software/firmware, single user, GPC

What works and what doesn't

Check Point
SOFTWARE TECHNOLOGIES LTD

- CAVP is deterministic and works well
- Code review is typically well understood

But

- There is great difficulty accepting a single code source as the module
- Too much time is spent on legalistic arguments on how the module is presented
- Labs are very cautions as they don't want to be fined
- Any communication is between the lab and CMVP with no space for the vendor
- Seems to be a differing "oral law" according to each labs experience

FIPS rewards Compliance and not Security

Check Point
SOFTWARE TECHNOLOGIES LTD

- In FIPS 140-2 you are rewarded for defining a minimal boundary through easier certification and maintenance – this gives less security
- Levels do not equate to security
  - They only consider the module, not the system
  - There is no requirement that **entropy**, **key generation** and **algorithms** are included in the boundary
  - There are no requirement that **external** entropy or keys used by the module are validated ?
  - **Self-protection** of the module needs to be considered irrespective of how the module is classified (beyond its own boundary)

Time to certify > time for software updates

Check Point
SOFTWARE TECHNOLOGIES LTD

- A single build is certified
- Today, software is constantly updated – monthly and often sooner
- Once a module is certified it should remain certified:
  - The correctness of the implementation is already proven with KAT and run-time checks.
  - FIPS 140-2 should allow a vendor assertion for module updates – provided self-tests still pass and algorithms still proven.
  - If more self-tests are required – these should be added to the standard

FIPS 140-2 in the world of certification

Check Point
SOFTWARE TECHNOLOGIES LTD

- What added value does FIPS 140-2 give to that provided in a cPP compliant CC certification? These also require CAVP certificates and perform their own entropy analysis and validate the cryptographic implementation at a protocol level within the claimed functionality being certified.
- Where the FIPS 140-2 boundary excludes entropy and key generation, does FISMA fill the assurance void for Federal customers?
- Customer perception is that higher FIPS 140-2 Levels are more secure…
- Wouldn't it be better to have separate labels for assessment of **Entropy**, **Keys**, **Algorithms**, **Protection** of the module ?

Summary

- Simplify process to essentials
- Replace Levels with stated validation for Entropy, Key generation and Algorithms, Self-protection
- Find a way to allow continuous certification/vendor assertions
- Security is important

Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU

Fitting a square peg in round hole

Malcolm Levy | Certification Manager

WELCOME TO THE FUTURE OF
CYBER SECURITY

CLOUD • MOBILE • THREAT PREVENTION