Improving cPP Development with Users Participation

Quang Trinh
Global Certification Team (GCT)
May 18, 2017
Overview

• History
• Statistics
• Benefits
• Cryptography
• Conclusion
History

Remember the old BRPP and MRPP?

- Created in a vacuum (Really no inputs or feedbacks from industry)
- No public invitation for collaboration (My way or the highway?)
- Hard to maintain and keep up with the changing technology
- Conflicting requirements between PPs
  - For example, MRPP Router vs MRPP Firewall vs VPN MRPP

Disclaimer: Based on personal experience. Show progress.
PP Development Progression

Closed → Limited → TC → iTC
International Technical Community

• International Technical Communities (iTCs) → collaborative protection profiles (cPPs)

“Membership of an iTC brings together many skills and backgrounds needed for the creation of an effective cPP and its Supporting Documents.”

Network iTC Statistics

iTC ND/FW Membership

- Government (40%)
- Lab (29%)
- Vendor (28%)
- Other (3%)
More WORK!
What are the benefits?
What do individuals get from iTCs?

• Regular discussions with colleagues outside their own organisation
• Sharing of knowledge
• Learning about technical and procedural aspects of cPPs and evaluation/certification
• Satisfaction from contributing to something bigger than the ‘home team’
What do organizations get from iTCs?

- Direct contact and discussion with requirement authors and risk owners
- Greater understanding of cPP requirements and how they are to be evaluated
- Understanding of emerging requirement areas
- Opportunities to challenge and review requirements before they are adopted
Cryptography Requirements (from NDcPP)

Cryptographic Key Management
- FCS_CKM.1 – Generation
- FCS_CKM.2 – Establishment
- FCS_CKM.4 – Destruction

Cryptographic Operations
- FCS_COP.1 – Encryption/Decryption, Signature Generation/Verification, Hashing, HMAC.

Random Bit Generation
- FCS_RBG_EXT.1 – Approved DRBG and entropy source

Cryptographic Protocols
- FCS_HTTPS
- FCS_TLS
- FCS_SSH
- FCS_IPSEC
Improvement Examples (part 1)

• Reference international standards to make cPP more internationally accepted
  For example
  • FIPS PUB 197 → ISO 18033-3
  • NIST SP 800-90 → ISO/IEC 18031:2011

• Adding AES CTR mode and not making CBC mandatory
Improvement Examples (part 2)

- Addition of FCS_CKM.2 which was not in NDPP
  - Specify the Approved key establishment algorithms
- Clarify zeroization requirements
  - No read-verify
  - Allow for other bits (non-zero) to be used
- Approved DRBG
  - Remove ANSI X9.31 Appendix 2.4 using AES
  - Remove Dual_EC_DRBG (any)
Future Improvement or Challenge?

- FFC domain parameters and RFC precomputed
- FCS_CKM.4 – beyond documentation, testing, when destroy
- Inclusion of non-NIST ECC Curves
- Additional algorithms for cryptographic key generation
- TLS tests clarification
- Addition of TLSv1.3
- NTP requirement
Conclusion

We believe with more users providing feedbacks in the cPP development processes, they can improve and influence the security requirements and assurance activities greatly.