Cygnacom Solutions

Cryptography and the Common Criteria (ISO/IEC 15408)

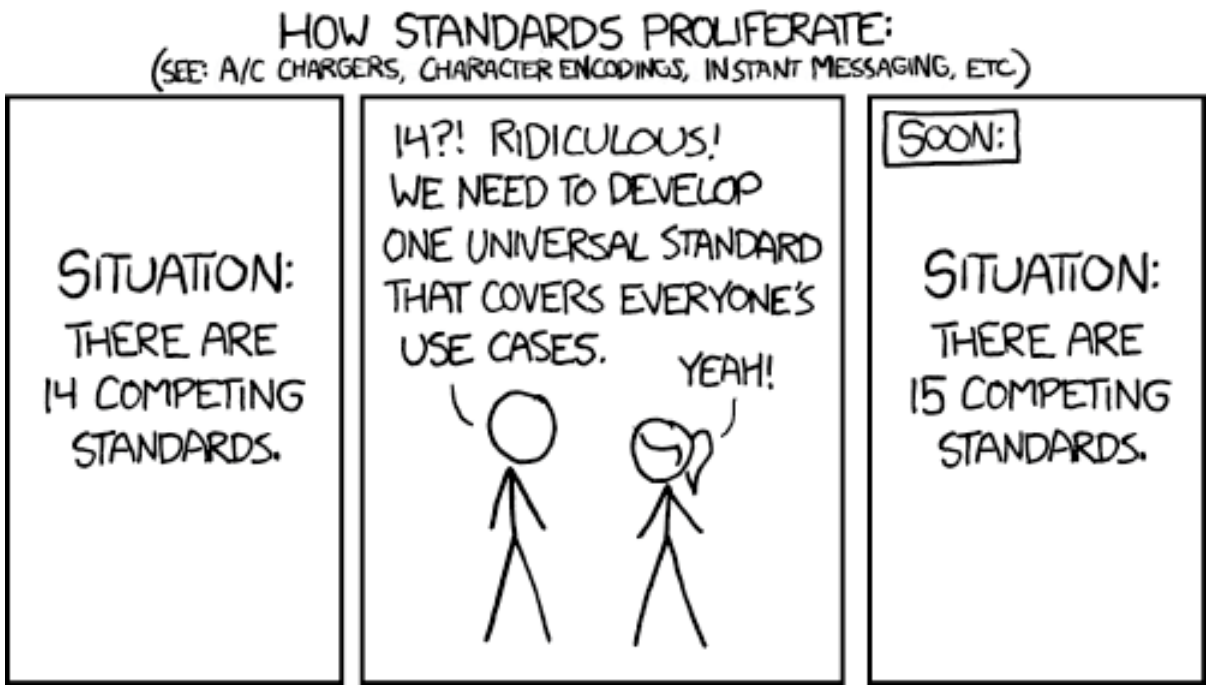
by Kirill Sinitski

ICMC15

About CygnaCom

- FIPS and Common Criteria Services
  - Accredited testing laboratories
  - NIAP, NIST, CSEC
- Professional Services
  - PKI infrastructure and deployments
  - Gov't security policies

Standards



About Common Criteria

- What is Common Criteria (ISO/IEC 15408)
  - Internationally Recognized Standard
- Common Criteria Recognition Arrangement (CCRA)
- Schemes
  - Represent Individual Countries
  - Certificate Authorizing and Consuming
- Common Criteria Portal and Scheme Lists

Why Common Criteria?

- National IA acquisition policies
  - US NSTISSP #11
  - Canadian PWGSC tenders
- Evolution and EALs
  - Understanding EALs
  - Standard Protection Profiles
- Categories of products
  - Portal vs. NIAP

CC Evaluation Process Overview

- Key Common Criteria Documents
  - Security Target
  - Protection Profile
- Evaluation Process
  - Eligibility
  - Kick-off and in-evaluation list
  - Milestones
  - Final Reports
  - Posted

Scheme Policy on Cryptography

- US: NIAP Policy Letter #5
  - CAVP and/or CMVP
- Canada: CCS Instruction #4
  - CMVP for core functionality, CAVP for everything else
- Germany
  - List of approved algorithms

Standard and Collaborative PPs

- Protection Profile (PP) is a framework
  - Security Target "template"
  - Standard within standard
    - Defines evaluation boundary
    - Defines security problem definition
    - Specifies security functionality
    - Establishes documentation and testing activities
  - EAL vs. Standard-PP
  - International vs. NIAP
  - Extended Packages
  - Exact Conformance

Standard Protection Profiles

- NIAP PPs
  - Network Devices (NDPP)
  - Wireless LAN (WLAN)
  - Enterprise (ESM)
  - Mobility (MD)
  - Application (App on OS)
  - Operating System (OS)
  - Encrypted Storage
- International Collaborative PPs
  - Network Devices (NDcPP)
  - Drive Encryption

"Baseline" Cryptographic Requirements

- SFR - Cryptographic Support (FCS)
  - Cryptographic Key Generation
  - Cryptographic Signatures
  - Encryption/Decryption
  - Hashing
  - Keyed-Hash Message Authentication
  - Random Bit Generation
- Assurance Activities
  - Zeroization
  - Seeding and Entropy

Cryptographic Keys

- Cryptographic Key Generation
  - Generation is optional, keys can be imported
  - RSA
    - 2048-bit or greater
    - Meet FIPS PUB 186-4 Appendix B.3
  - ECC
    - NIST P-256, P-384, P-512 curves
    - Meet FIPS PUB 186-4 Appendix B.4
  - FCC
    - 2048-bit or greater
    - Meet FIPS PUB 186-4 Appendix B.3

Cryptographic Keys

- Cryptographic Key Destruction
  - Zeroization is mandatory
  - Volatile memory
    - Direct overwrite with random or zeroes, read-verify
  - EEPROM
    - Direct overwrite with random followed by a read-verify
  - Flash
    - Direct overwrite with zeroes, block erase, and read verify
  - Disk drive
    - Three times random pattern

Cryptographic Signatures

- RSA
  - FIPS PUB 186-4 Section 5.5
    - RSASSA-PKCS1-v1.5 or RSASSA-PSS
  - 2048 bits or greater generation

- ECDSA
  - FIPS PUB 186-4 Section 6
  - 256 bits of greater
  - NIST curves P-256, P-384, and optionally P-521

Encryption and Decryption

- AES
  - Typically: CBC, GCM
  - Rarely: XTS, CCM
  - Key sizes: 128, 192, 256
  - NIST SP 800-38 A-E or ISO 10116, ISO 19772

Hashing

- SHA-1
  - Allowed to comply with SP 800-131A
  - Usually PP has a note on overall crypto strength
- SHA-2
  - Typically: SHA-256, SHA-384, SHA-512
  - Rarely: SHA-224
- FIPS Pub 180-4, ISO/IEC 10118-3:2004

Keyed-hash message authentication

- HMAC-SHA-1
  - Usually PP includes a note on key size range
- HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512
- FIPS Pub 198-1, ISO/IEC 9797-2:2011, Section 7

Random Bit Generation

- RNGs
  - Hash_DRBG
  - HMAC_DRBG
  - CTR_DRBG (AES)
- Seeding
  - 128, 256 bits of entropy
  - NIST SP 800-57, ISO/IEC 18031:2011 Table C1
  - Chain from platform's certified DRBG
- Entropy Assessment Report (EAR)
  - IAD review process
  - Loosely following NIST SP 800-90B

"Exotic" Cryptographic Requirements

- EP File Encryption
  - Key Wrap, Key Wrap with Padding, RSA using KTS-OAEP
  - Key Storage, Key Management
- WLAN
  - Key Distribution from 802.1X Authorization Server
  - AES Key Wrap in an EAPOL-Key frame
- NIAP Policy Letter #23
  - IEEE 802.11-2012
  - AES-CCM for wireless chipset

Documentation Requirements

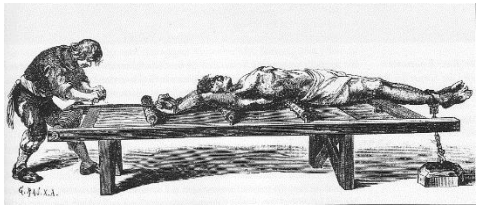
- Certificate Coverage Table

FCS_COP.1(1) Cryptographic Operation (encryption/decryption)	AES-CBC-128 and AES-CBC-256 for data encryption/decryption implemented to meet FIPS PUB 197, "Advanced Encryption Standard (AES)" in compliance with NIST SP 800-38A. Encryption/decryption performed by the cryptographic module operating in the FIPS mode.	AES #2971
FCS_COP.1(2) Cryptographic Operation (cryptographic signature)	RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater in compliance with FIPS PUB 186-3, "Digital Signature Standard". Cryptographic signature functionality is performed by the cryptographic module.	RSA #1560
FCS_COP.1(3) Cryptographic Operation (cryptographic hashing)	SHA-1 and SHA-256 cryptographic hashing implemented to meet FIPS PUB 180-3, "Secure Hash Standard" is performed by the cryptographic module operating in the FIPS mode.	SHA #2497

- CSP Zeroization Table
- Entropy Assessment Report

Entropy Assessment Report

- Part of all Standard PPs
  - Random Bit Generation (FCS_RBG_EXT.1)
  - NIST special publication 800-90B
- Entropy Assessment Report (EAR)
  - Unconditioned source data analysis
  - Operating Conditions
  - Health Testing
  - Entropy production and consumption rates
  - Sources - hardware and software



Entropy Assessment Report (continued)

- Detailed PRNG seed creation description
  - Saved state description
  - Seed and Nonce Composition
- Per Source Analysis
  - 1 mil samples for each entropy source
  - "Raw" data from each source
- Operating Scenarios
  - Initial startup entropy rate
  - Idle system entropy rate

Cygnacom Solutions

Third-party Cryptographic Modules

- Open Source Software
  - OpenSSL, LibreSSL, NaCL, cryptlib
- Closed Source Software
  - NanoSSL, SafeNet
- Hardware Implementations
  - HSMs
  - CPU and cryptographic acceleration
  - Hardware noise sources
- Opportunity
  - Test harness
  - Platform CMVP certificates

System Integration Blues

- Applicability
  - Platforms and equivalence arguments
  - Old compliance claims (e.g. FIPS PUB 186-2)
  - Missing certificate coverage (e.g. ECDSA P-384)
- Documentation
  - Entropy and seeding
  - Zeroization of CSP
  - NIST SP 800-56B compliance tables
- Vulnerability analysis
  - CVE history

Cygnacom Solutions

Equivalency Arguments

- Only applicable to CMVP
- Acceptable Deviations in Operational Environment
  - OS version and compiler version
  - Processor model
- Unacceptable Deviations
  - Processor Architecture (ARMv7 vs x86)
  - OS kernel (Windows 7 vs. BSD)
- Problematic Claims
  - Operational Environment Mismatches
    - ARMv7 vs PowerPC, NetBSD vs. RHEL
  - Wrong modes and key sizes
    - AES128-CBC vs AES256-CTR

Cygnacom Solutions

Common Problematic Claims

- Claiming OpenSSL certs with just library
  - Baseline OpenSSL library inadequate
- Modifying certified module in any way
  - Mix and match claims
  - Multiple modules with questionable interoperability
- Operational Environment Mismatches
  - ARMv7 vs PowerPC
  - NetBSD vs. RHEL
- Wrong modes and key sizes
  - AES128-CBC vs AES256-CTR

Questions?