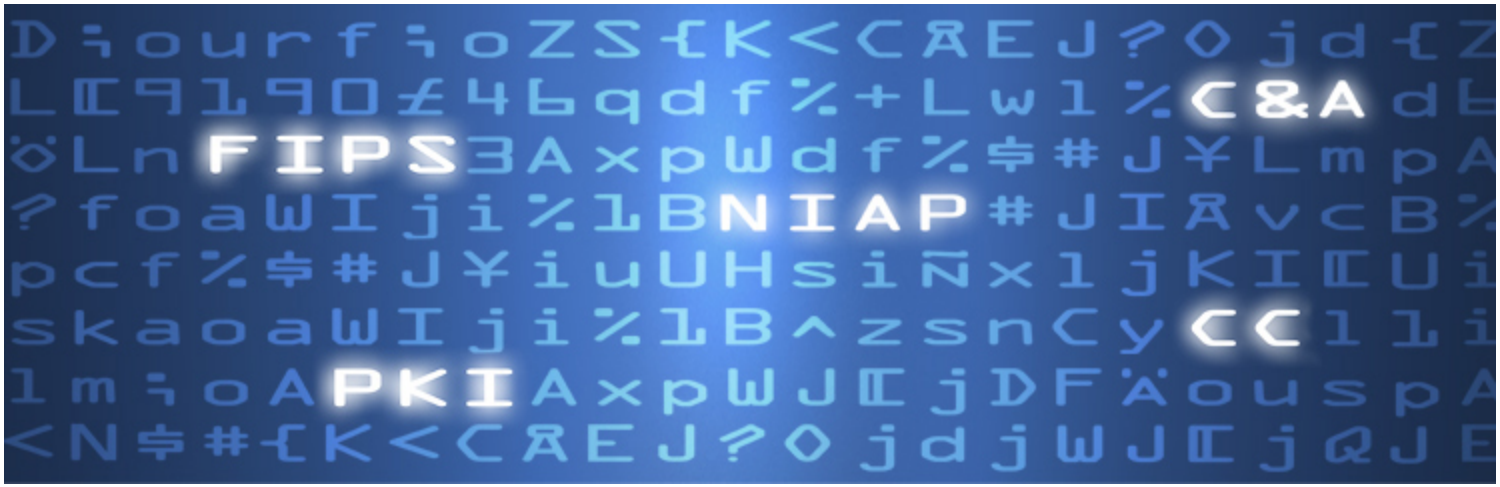
Cygnacom Solutions



The Common Criteria (CC) Threads within ISO 19790

(aka FIPS 140-3)

by Iain Holness and Dayanandini Pathmanathan

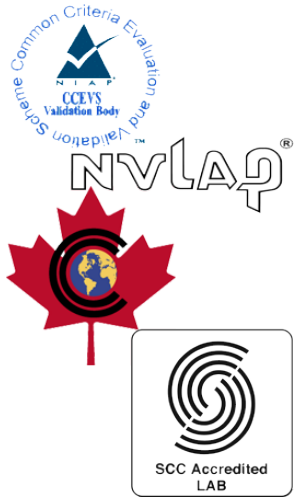
ICMC16

In this Presentation

- Introduce ourselves as Cygnacom
- Look at differences and common ground for FIPS and CC
- Give an Overview of ISO 19790
- Look at areas of ISO 19790 that draw upon CC
- Briefly look at other National and Industry schemes that use ISO 19790 or FIPS

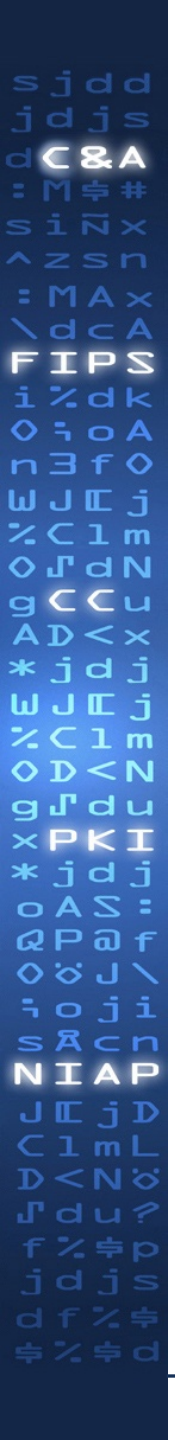
CygnaCom Solutions Laboratories

- Accredited FIPS and Common Criteria laboratories
- Consultation Services
- Professional Services



Cygnacom Solutions

CC within ISO19790: You may think it's hiding in plain sight, but really, it isn't. You just need to look carefully.



Cygnacom Solutions

FIPS and CC: differences and common ground

- The FIPS 140-2 standard is currently required by the U.S. & Canadian governments
- Common Criteria is a separate international standard
- FIPS focuses on the cryptographic module itself
- CC examines the security functionality of the module
- However: there is an evidence and assessment overlap

So what is ISO 19790?

- It is an ISO standard, created in 2005, that was created for other nations to use FIPS without an implied American bias
- It has 4 levels, the same as FIPS 140-2
- The majority of it is taken directly or reworded from FIPS 140-2 and its associated Implementation Guidance (IG)
- A small amount of it is derived from multiple elements of CC's Common Evaluation Methodology (CEM)
- The FIPS Detailed Test Requirements (DTR) dictates how labs are to carry out FIPS validations, and was used as the core for ISO 24759, which dictates testing for ISO 19790

What Areas of ISO 19790 Draw on CC?

- Life-cycle assurance
  - Configuration Management
  - Delivery and Operation
  - Development
  - Vendor testing

Looking at Life-cycle assurance

- General evidence required for all levels of this area:
  - Security Policy (same as FIPS 140-2)
  - CM documentation
  - User and administrative documentation
  - A Finite State Model (FSM)
  - Hardware schematics
  - Source code for the module, with explanatory text
  - Change log

How Life-cycle assurance ties in CC

- Configuration Management
  - Levels 1 and 2
    - Proof that a CM system is being used
    - Each version of each configuration item (CI) has a unique identifier (module, hardware components, software components, documentation, etc.)
    - The CM systems tracks and maintains changes to the identification and version / revision of each CI through the module's lifecycle
  - Levels 3 and 4
    - An automated CM system must be used

- Development
  - Level 1
    - The CM system must track all of the source code and everything associated with building the module from the source code
    - Review of annotated source code, FSM, and any hardware schematics
  - Levels 2 and 3
    - If Assembly or microcode were used, a rationale is required as to why this was done
    - Were simple and efficient source code development practices followed?
  - Levels 3 and 4
    - Evidence: Functional Specification
    - Evidence: Subsystem design and data flows

- Delivery and Operation
  - Level 1
    - Documentation for secure installation, initialization, and startup of the module
  - Levels 2 to 4
    - Secure delivery procedures for shipping the module to customers, including detection of any tampering with the module
- Vendor Testing
  - Levels 1 and 2
    - Evidence required for functional testing performed on the module (test plans and testing results)
    - The vendor shall use automated security diagnostic tools
  - Levels 3 and 4
    - The vendor shall provide test plans and results for low-level testing of the module

So what are we looking for again?

Results of ISO 19790 incorporating CC

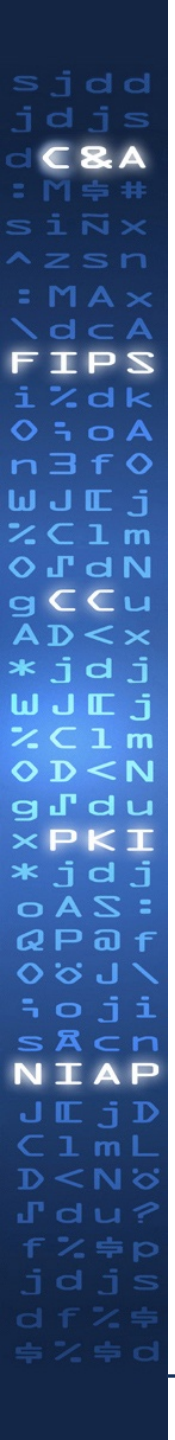
- Greater emphasis on the module's life cycle and the vendor's secure development practices
- More evidence is required from vendor
- Lab personnel will be performing more analysis
- More time spent in the IUT phase
- Net result: increased assurance that the module being validated is more robust, with greater security applied across its entire lifecycle

Other schemes using ISO 19790 / FIPS 140-2

- National government schemes
  - Japan's CMVP
  - Korean CMVP
  - Brazil's Cryptographic Approval Process (run by National Institute of Information Technology)
- Industry schemes
  - French Cartes Bancaires scheme (Méthod d'Évaluation des Produits de Sécurité –method of evaluating security products or MEPS)
  - PCI-HSM standard (PCI Security Standards Council)

In this Presentation we explored

- Differences and commonalities between FIPS and CC
- An overview of ISO 19790
- Areas of ISO 19790 that draw upon CC
- Other National and Industry schemes that use ISO 19790 or FIPS 140-2



Questions?