



A Comparison of Security Standards

Marcus Streets
Security officer
Thales nCipher

ICCC 10 September 2009

The problem - a plethora of Standards



- ISO 27001
- FIPS 140-x
- CAVP
- PCI DSS
- Baseline / Enhanced / NATO
- Claims Tested Mark
- Common Criteria

ICCC 10 September 2009



- **What**
 - ISO/IEC 27001:2005 – Information technology -- Security techniques -- Information security management systems
 - Previously known as BS7799:1995
- **Why**
 - Compliance with data security laws
 - “Viral” spread
- **Who**
 - Any business
- **How**
 - Evaluation
 - Identify threats – establish countermeasures
- **Effort**
 - Man months to man years



- Designed for all businesses – not just security businesses
 - Most businesses are not threatened by Blofeld style master criminals stroking their cats
 - Therefore evaluation generally looks at low level threats
- Evaluators will look for proof counter-measures adequately meet threats
 - This may drive need for CC as proof a security program is “adequate”
 - Would be useful if CC 4.0 terminology was consistent with ISO 27001



- **What**
 - Federal Information Processing Standard for Hardware Security Modules
- **Why**
 - US and Canadian Federal Government mandate
 - Adopted in other industries due to lack of other standards
- **Who**
 - Federal agencies and their contractors
 - Other businesses requiring cryptography
- **How**
 - Validation
- **Effort**
 - Man months (Level 1-3)
 - Man years (Level 4)



- Started as Federal Standard 1027
 - Hardware DES Encryption only
 - FIPS 140 was a name change only
- FIPS 140-1 January 1994
 - All HSMs
 - Introduces four levels
 - Start of the Validation Program
- FIPS 140-2 25th May 2001
 - Minor Updates only
- FIPS 140-3 (tba)
 - In “Development Hell”



- Four levels (may change in FIPS 140-3)
 - 1: No physical security
 - 2: Tamper Evident
 - 3: Tamper Resistant
 - 4: Tamper Responsive
- NIST approved algorithms only
- Specific tests listed in DTR
 - No tests for non-invasive attacks
 - FCC Class B testing as proxy



- ISO/IEC 19790:2006
 - ISO standard based on FIPS 140-2
 - Work on testing requirements still on progress
- Japanese scheme JCMVP
 - Run by IPA
 - Based on NIST/CSE's CMVP scheme
 - 3 approved labs
 - 10 certificates issued
 - Allows more algorithms than NIST/CSE



- What
 - Algorithm Testing

- Why
 - Required as part of FIPS 140-2

- Who
 - Vendors of FIPS 140-x modules

- How
 - Off line testing



- What
 - Requirements for US Personal Identity Verification scheme
- Why
 - US Federal requirement HSPD-12
- Who
 - Vendors' selling to US government
- How
 - Complete FIPS 140-2 or CC Evaluation
 - Apply to be listed
- Effort
 - Man days



- What
 - Standard for Hardware Security Modules used in payments industry
- Why
 - Required by VISA, Mastercard and AMEX
 - EMV protocols not approved by NIST/CSE
- Who
 - Merchants dealing with credit cards
- How
 - Validation
 - Similar level of rigour to FIPS 140-2 level 3
- Effort
 - Man months



- **What**
 - Separate Government programmes in each NATO state
- **Why**
 - Military and Classified data
- **Who**
 - Specialist Security Vendors
- **How**
 - Detailed evaluation of design and implementation
 - Secret government eyes only algorithms
- **Effort**
 - Multiple Man Years



- What
 - UK standard
- Why
 - Low cost alternative to CC
 - British alternative to FIPS 140-x
- Who
 - British security vendors
- How
 - Light weight evaluation
- Effort
 - Man Weeks



- **What**
 - ISO/IEC 15408
 - Successor to ITSEC
- **Why**
 - Government non-secret
 - European Digital Signature Law
- **Who**
 - Specialist Vendors
- **How**
 - Evaluation
- **Effort**
 - Man months (EAL2)
 - Man years (EAL4)
 - Multiple man years (EAL7)