Internationalization Activities & ISO/IEC JTC1 SC27 Projects

Eric A. Hibbard, CISSP,CISA

June 17, 2009

ISO/IEC JTC1 SC27 Security Techniques

- SC27 Organizational Structure:
  - WG 1 – Information security management systems
  - WG 2 – Cryptography and security mechanisms
  - WG 3 – Security evaluation criteria
  - WG 4 – Security controls and services
  - WG 5 – Identity management and privacy technologies
- ISO/IEC SC 27 Meetings:
  - Last WGs & Plenary: May 4-8, 2009; Beijing, China
  - WGs: Nov 2-6, 2009; Seattle, WA (U.S. hosting)
  - WGs & Plenary: Apr 19-27, 2010; Melaka, Malaysia
  - WGs: Oct/Nov, 2010; Europe
  - WGs & Plenary: Apr/May, 2011; Singapore
- Documents:
  - http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306

Status

- ISO/IEC JTC1 SC27 identified as the appropriate standards body
- Prerequisite - NIST acceptance of XTS-AES (as defined in IEEE Std 1619-2007) as an Approved Mode of Operation for FIPS 140-2; accomplished, with some specific constraints.
- IEEE-SA is still working through its issues for submitting text to ISO/IEC JTC1 SC27, for consideration in the next revision of ISO/IEC 10116:2006 (modes of operation)
- SC27 just voted to simply re-affirm ISO/IEC 10116 (i.e., no updated planned)

Crypto Projects

- ISO/IEC CD 10118-2 Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher
- ISO/IEC FCD 11770-1 Information technology -- Security techniques -- Key management -- Part 1: Framework
- ISO/IEC FCD 15946-5 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 5: Elliptic curve generation
- ISO/IEC NP 18033-1 Information technology -- Security techniques -- Encryption algorithms -- Part 1: General
- SO/IEC NP 18033-3 Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
- ISO/IEC NP 18033-4 Information technology -- Security techniques -- Encryption algorithms -- Part 4: Stream ciphers
- SO/IEC NP 19790 Information technology -- Security techniques -- Security requirements for cryptographic modules
- ISO/IEC CD 29150: Signcryption
- ISO/IEC WD 29192 Proposal on lightweight cryptography

ISO/IEC SC27 Important Projects

- ISO/IEC 27000:2009 Information security management systems - Overview and vocabulary
- ISO/IEC 27001 Specification for an ISMS (WD)
- ISO/IEC 27002 Code of practice for Information Security Management (WD)
- ISO/IEC 27003 Information security management system implementation guidance (register and circulate as FDIS)
- ISO/IEC 27004 Information security management measurements (register and circulate as FDIS)
- ISO/IEC 27007 Guidelines for ISMS auditing (register and circulate as CD)
- ISO/IEC TR 27008 Guidance for Auditors on ISMS Controls (circulate as 3rd WD)
- ISO/IEC 27031 Specification for ICT Readiness for Business Continuity (register and circulate as CD)

ISO/IEC SC27 Important Projects (cont.)

- ISO/IEC 27032 Guidelines for Cybersecurity
- ISO/IEC 27033 IT network security (multi-part)
  - Part 1 – Overview and concepts (FCD)
  - Part 2 – Application security management process (CD)
- ISO/IEC 27034 Application security (CD)
- ISO/IEC 27035 Security incident management (circulate as FCD)
- ISO/IEC 29000 Privacy Framework (register and circulate as CD)
- ISO/IEC 29001 Privacy Reference Architecture (circulate as 3rd WD)

ISO/IEC SC27 Other Projects of Possible Interest

- ISO/IEC 27009: Guidance for auditors on ISMS controls.
- ISO/IEC 27010: Information security management for inter-sector communications (WD)
- ISO/IEC 27035: Information security incident management (CD).
- ISO/IEC 29128: Verification of cryptographic protocols (CD)
- ISO/IEC 29146: A framework for access management (WD)
- ISO/IEC 29147: Responsible vulnerability disclosure (3rdWD)
- ISO/IEC 29149: Best practice on the provision of time-stamping services (4thWD)

ISO/IEC SC27 Study Period Topics

- Access control
- Secret sharing mechanisms
- Mechanisms supporting anonymity
- Tamper protection requirements and evaluation
- Redaction