Cryptographic Key Management Workshop

March 4-5, 2014

Session 5: Measures and Security Controls

Elaine Barker and Ron Ross

Security Strength

- **Definition:** The amount of cryptographic protection that can be provided by a combination of a cryptographic algorithm and a key.

- **Five strengths, measured in bits**: 80, 112, 128, 192, 256. 80 bits of strength no longer approved by the Federal govt.

Security Strength (contd.)

- **Key strength**: a function of the entropy in the key and the algorithm used.
- **Algorithm strength:** Depends on the attacks on the algorithm, given a key length.
- SP 800-57, Part 1 lists the maximum security strength that can be supported by an approved algorithm with a given key length.

FIPS 140 Security Levels

- FIPS 140 addresses the security of cryptographic modules.
    - Cryptographic modules perform the basic cryptographic functions (e.g., encrypt, sign, generate random values).
    - Four increasing levels of security defined: Levels 1, 2, 3 and 4; level 1 provides the least amount of protection.
    - Eleven requirement areas.

- An FCKMS **shall** use FIPS 140-validated cryptographic modules (PR: 2.9).

FIPS 140 Security Levels (Contd.)

- Level 1:
  - Logical separation of roles and services.
  - Production-grade equipment.
  - Entry and output of CSPs (e.g., keys) can be in plaintext.
  - Example: Software and firmware components on a general-purpose computer using an unevaluated operating system.

FIPS 140 Security Levels (Contd.)

- Level 2:
  - Role-based authentication.
  - Locks or tamper evidence.
  - Entry and output of CSPs (e.g., keys) can be in plaintext.
  - Example:
    - ✓ A general-purpose computer using an operating system meeting Common Criteria Protection Profiles and evaluated at EAL2 (or higher).
    - ✓ EAL2 intended for low to moderate levels of security requirements.

FIPS 140 Security Levels (Contd.)

- Level 3:
  - o Identity-based authentication.
  - o Tamper detection and response.
  - o Entry or output of CSP (e.g., keys) in encrypted or as key splits.
  - o Example:
    - ✓ A general-purpose computer using an operating system meeting Common Criteria Protection Profiles and having a trusted path; evaluated at EAL3 (or higher).
    - ✓ EAL3 intended for moderate levels of security requirements.

FIPS 140 Security Levels (Contd.)

- Level 4:
  - Identity-based authentication.
  - Tamper detection and response envelope.
  - Entry or output of CSP (e.g., keys) in encrypted form or as key splits.
  - Environmental protection features or rigorous testing.
  - Example:
    - ✓ A general-purpose computer using an operating system meeting Common Criteria Protection Profiles and a trusted path, and evaluated at EAL4 (or higher).
    - ✓ EAL4 intended for moderate to high levels of security requirements.

Questions and Comments?

Impact/Sensitivity Levels

Ron Ross

Impact/Sensitivity Levels

- See Ron Ross's slides, which are posted separately

Impact/Sensitivity Levels

Impact/Sensitivity Level	Minimum FIPS 140 Security Level	Minimum Algorithm/Key Security Strength
Low	Level 2, or Level 1 w/compensating physical protections	112
Moderate	Level 3	128
High	Level 4	192*

* Should this be 256?

Questions and Comments?

Security Controls

Elaine Barker

Security Controls
(Section 8)

- **Definition:** Security mechanisms and management that protect the FCKMS components, along with the keys and metadata (Section 8).

Physical Security Controls
(Section 8.1)

- An FCKMS **shall** support the physical protection of FCKMS modules, cryptographic modules, components, devices, unencrypted keys and sensitive metadata (PR: 8.1).

Operating System Security
(Section 8.2.1)

- An FCKMS **shall:**
  - Support hardening principles (PR: 8.2),
  - Maintain software integrity (PR: 8.3), and
  - Protect access to sensitive keys and metadata by non-validated software (PR: 8.4).
- An FCKMS **should:**
  - Verify software integrity during system startup (PA: 8.1),
  - Use trusted operating systems (PA: 8.2), and
  - Provide multi-person control of critical functions (PA: 8.3).

Individual FCKMS Device Security
(Section 8.2.2)

- An FCKMS **shall** verify that devices are operating correctly (PR: 8.5).

Malware Protection

(Section 8.2.3)

- An FCKMS **shall:**
  - Support malware protection capabilities (PR: 8.6), and
  - Verify the source and authenticity of software and check for malware (PR: 8.7).
- An FCKMS **should:**
  - Support configurable, dynamic network malware monitoring (PA: 8.4),
  - Perform checks for malware (PA: 8.5, 8.6 and 8.7), and
  - Verify software integrity at installation, etc. (PA: 8.8).

Auditing and Remote Monitoring
(Section 8.2.4)

- An FCKMS **shall:**
  - Protect the audit capability and audit logs from unauthorized disclosure and modification (PR: 8.8),
  - Support the detection of unauthorized attempts to access, modify or destroy keys (PR: 8.9), and
  - Support the audit of security-relevant events and record appropriate data (PR: 8.10).

Auditing and Remote Monitoring (Contd.)

(Section 8.2.4)

- An FCKMS **should:**
  - Support the monitoring of internal components, modules, etc. (PA: 8.9),
  - Support the ability to select the security-relevant events to be audited (PA: 8.10),
  - Support the use of SCAP (PA: 8.11), and
  - Support individual accountability (PA: 8.12).

Network Security Control Mechanisms
(Section 8.3)

- An FCKMS **shall:**
  - Support one or more security-control mechanisms (PR: 8.11),
  - Install network security-control mechanisms in physically secure facilities (PR: 8.12), and
  - Allow only authorized entities to configure, initiate, activate, and disable network security-control mechanisms (PR: 8.13).

Network Security Control Mechanisms (Contd.)
(Section 8.3)

- An FCKMS **should:**
  - Support the identification and authentication of each FCKMS module and device (PA: 8.13), and
  - Support all of the network security-control mechanisms listed unless exempted (PA: 8.14).

Cryptographic Module Controls
(Section 8.4)

- An FCKMS **shall** use a cryptographic module in accordance with its security policy (PR: 8.14).

Security-Controls Selection Process (Section 8.5)

- An FCKMS **shall**:
  - Be tailored in accordance with SP 800-53 (PR: 8.19),
  - Assess the effectiveness of the FCKMS security controls on an ongoing basis (PR: 8.22), and
  - Comply with FIPS 199, FIPS 200, and SP 800-53 (PR: 8.23).

(Continued on next slide)

Security-Controls Selection Process (Contd.) (Section 8.5)

- An FCKMS **shall** specify:
  - The types of information to be protected (PR: 8.13),
  - The FIPS 199 security categories (PR: 8.16),
  - The FIPS 200 impact level (PR: 8.17),
  - The SP 800-53 security-control baseline (PR: 8.18),
  - That then security controls were assessed and are adequate (PR: 8.20),
  - The assurance requirements necessary for the impact level (PR: 8.21), and
  - The events that require the immediate need to assess the security of the information system, to reassess the current security controls, and to take corrective action (PR: 8.23).

Questions and Comments?