Security Policies as the Foundation for Cryptographic Key Management

Elaine Barker, CKMS Project Leader

Dennis Branstad, CKMS Presenter

Miles Smid, CKMS Project

Presentation Summary

- Introduction to Layered Security Policies
  - From Information Management to Key Mngt.
  - From Dept. of Com. To NIST Employees
- Security Domains – Simple to Complex
- Key Management – Static to Configurable to Dynamic Security Domain Negotiation
- Policy Negotiation – Local to Global
- Policy Specification – Ad Hoc to Formal

Security Policy Specifications

- A Security Policy should be written so that people can understand and follow it;
- A Security Policy should be encoded so that an automated system can enforce it;
- A formal specification of a security policy can be understandable to humans and automatically enforced by a CKMS.

Security-Domain Based Cryptographic Key Management

- Goal: Automated negotiation of key management based on the domain security policies of two or more mutually suspicious participants in a sensitive transaction.
- Assumption: Security is proportional to cost, the services used, and the protection provided.
- Approach: Develop an automated Policy Negotiation method using formal syntax specifications of compatible Security Policies.

Information Management Policy

- Highest-Level Organizational Policy for Managing and Protecting Information in all forms (paper, computer data, electronic storage);
- Established by the Organization’s CEO or CIO;
- Policy is provided to all the Organization’s employees so they can follow the policy.

Information Management Policy (Con’t)

- Based primarily on organization’s goals and objectives;
- Based often on industry standards of good practice (e.g., health patient privacy rules);
- Assigns Information Management Roles and Responsibilities to individuals;
- Foundation for Information Security Policy.

Information Security Policy

- Establishes high-level rules for protecting organization’s information independent of the storage media (e.g., paper, electronic);
- Establishes information sensitivity levels;
- Establishes security labels for information;
- Protection services are based on threats;
- Level of protection is based on risks to information that could result in its loss, or its unauthorized disclosure or modification.

Data Security Policy

- Based on the Information Security Policy;
- Rules for protecting electronic information;
- Governs use of Computers & Applications;
- Covers use of communication networks;
- Specifies data security levels, labels, etc.;
- Basis of Cryptographic Data Protection;
- Basis of Cryptographic Key Management.

CKMS Security Policy

- Based on an organization’s Data Security Policy, specifically on data cryptographic protection;
- Protecting a cryptographic key and its associated metadata is required to protect the information protected by the key;
- Often based on CKMS Profiles (e.g., Federal) of organizations using the services of the CKMS;
- CKMS Technical Capabilities must support and be used to enforce the CKMS Security Policy.

CKMS Security Policy (Con’t)

- Specifies detailed CKMS requirements for protecting cryptographic keys and their associated metadata within the CKMS;
- Based on, and supports, the sensitive data and applications’ protection requirements;
- Governs key and metadata protection and management throughout the entire lifecycle of a cryptographic key.

Relationships among Policies

- Policy statements should be layered from high to low ranging from high level goals to details on how to implement and enforce the policy; e.g.
  - Simple high-level policy: Protect sensitive data;
  - Simple mid-level policy: Encrypt sensitive data during communication and in long-term storage;
  - Simple low-level policy: Encrypt and Label data with AES-128 whenever it is stored outside a physically secure facility;
  - Simple CKMS policy: Use a validated FIPS140-2 Cryptographic Module whenever encrypting the application data and the Key used to encrypt it.

DOC/NIST Policies Principles of Information Security

- DOC/NIST’s Information and Data Security Policies include all aspects of protecting information and data. These include:
  - *Confidentiality – Protecting Data from unauthorized disclosure;*
  - *Integrity –Protecting Electronic Data from unauthorized, unanticipated, or unintentional modification;*
  - *Availability – Electronic Data must be available on a timely basis.*
- The potential impact on DOC, NIST, Federal employees, and private individuals is categorized as:
  - *low (limited),*
  - *moderate (serious), or*
  - *high (catastrophic or severe)*

DOC/NIST Computer Use Policy

- To be authorized access to NIST Computers and Networks, users must:
  - Read the DOC/NIST Policies on IT Usage and Data Access & sign acceptance form;
  - Take the DOC/NIST IT Security Course;
  - Retake the Information Security Training course annually;
  - Review and accept all the DOC/NIST Data Security Policies.

DOC/NIST Information Policy on Personally Identifiable Information (PII)

- NIST computer users should delete unnecessary PII;
- NIST PII should be stored only on NIST-owned computers, never on personally owned computers or data storage media;
- Removable data storage media must not be used to store plaintext PII;
- Laptops , tablets, and removable data storage media must use FIPS 140-2 encryption if they contain PII and are intended to be removed from NIST.

CKMS Security-Policy Related Questions

- How does the CKMS Security Policy help enforce an organization’s Computer & Data Security Policies?
- What security mechanisms must be in the CKMS to provide the protection required by the security policy?
- What administrators must be notified when the CKMS Security Policy is modified? How are they notified?
- Under what conditions may a key and its associated metadata be shared and used?
- Should technical-related portions of the CKMS security policy be expressed in tabular form or in a formal language so that the CKMS can automatically enforce them?

CKMS Policy Implementation

- The designer must select CKMS services, functions, algorithms, protocols, key types, etc. to be included in an implementation/product based on future markets;
- The designer can selectively implement functions and features statically by “hard coding” all parameters or dynamically by “soft coding” support of parameters specified in a static or dynamic security domain policy;
- Design and implementation of a static CKMS is simpler; operation is efficient, cost is less, BUT
- A CKMS capable of enforcing several security policies may support more domains and have a larger market.

Structured Policy Specifications

- Flow charts and tables can be manually “encoded” such that they can be enforced by a CKMS; BUT
- Security Administrators can be aided in using an automated, template-based, question-answer program to create a flexible security domain policy;
- A structured security domain policy specification can be translated into a formal Policy Specification Language with Formal Syntax Rules defining all acceptable “sentences” of the Policy Language;
- Semantics (the “meaning” of the “sentences” of a language) can be structured to be understandable to humans and enforced directly by a CKMS.

Example: Simple Security Policy

- <Level> ::= “High” | “Moderate” | “Low”;
- <Label> ::= “Financial” | “Health”;
- <Protect> ::= “Encrypt” | “Sign”;
- < Data> ::= “Payment” | “Cancer”;
- <Sentence> ::= <Level> <Label>
  <Protect> <Data> “.”;

Sentence 1: High Financial Sign Payment.

Sentence 2: Low Health Encrypt Cancer.

Test: How many legal sentences exist in this Policy?

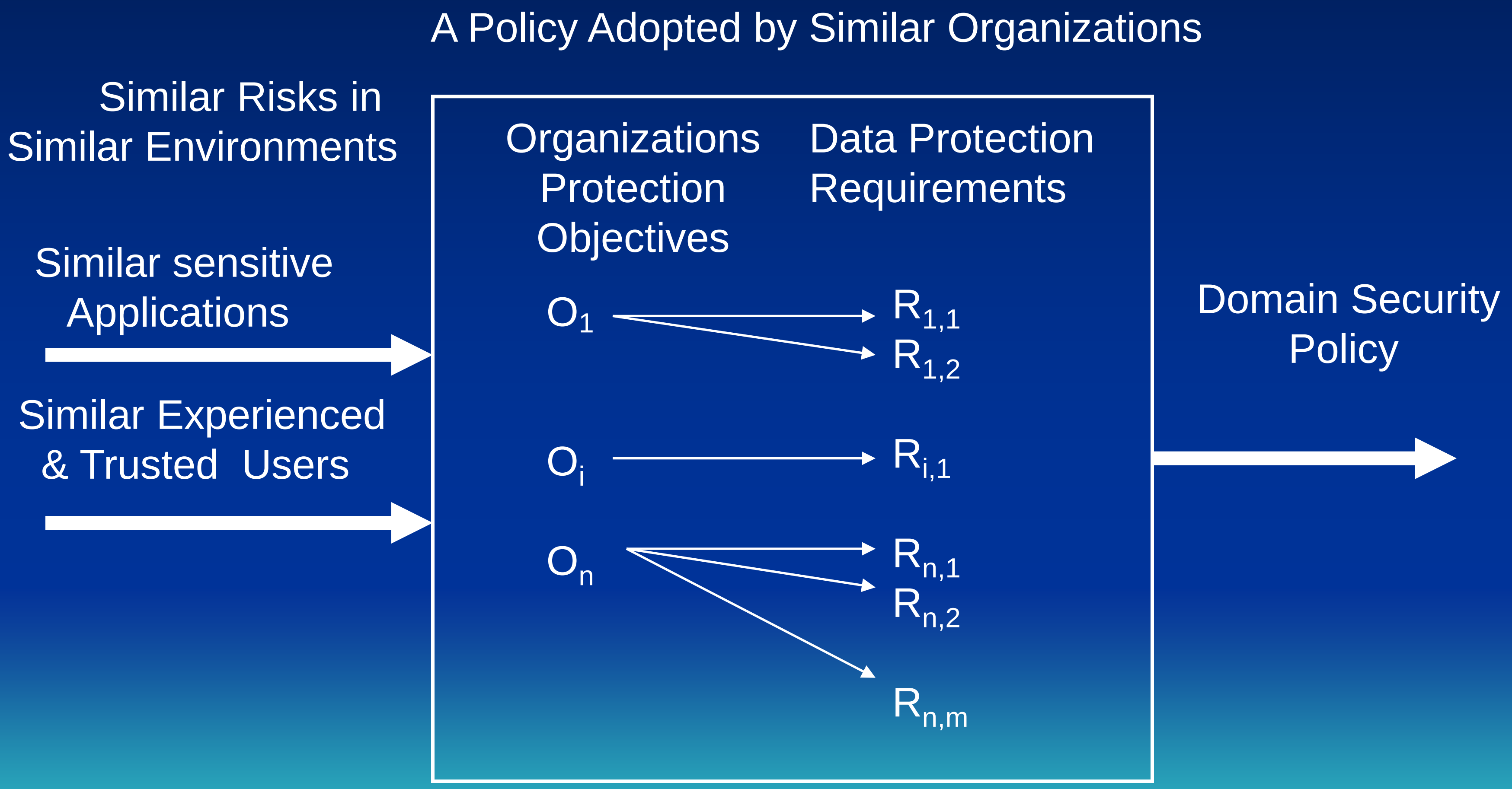
Policy Language Semantics

- Formal semantics specify an unambiguous meaning for each sentence of a language.
- Each sentence of a Formal Security Policy Language would have semantics that a CKMS Policy Program would enforce.
- Ex: HIGH HEALTH SIGN PAYMENT. would be implemented as a process that signs highly valuable health payment data.

Security Domain

- Collection of Computers, Communications, Applications, and Users processing data in accordance with a single data security policy called the Domain Security Policy;
- The mutually trusting entities (e.g., users) in a Security Domain can easily exchange data, keys, and metadata in accordance with the Domain Security Policy currently being enforced by a CKMS.

Domain Security Policy Creation



A Policy Adopted by Similar Organizations

Similar Risks in Similar Environments

Similar sensitive Applications

Similar Experienced & Trusted Users

Organizations Protection Objectives

Data Protection Requirements

O_1 → $R_{1,1}$, $R_{1,2}$

O_i → $R_{i,1}$

O_n → $R_{n,1}$, $R_{n,2}$, $R_{n,m}$

Domain Security Policy

Sharing Sensitive Data from Different Security Domains

- Users in two different Security Domains can share sensitive information if the Domain Security Policies are equivalent or compatible;
- Equivalent policies provide protections that are mutually acceptable to users in both Domains;
- Compatible policies or not equivalent but have equivalent subsets of protections that satisfy both security policies if the provided data processing services are restricted. (Note: Details and mechanisms are still under study.)

Obtaining Assurances of Security

- Exchanging data from different security domains may initially require an authority from each domain to examine the policy from the other domain and verify that they are equivalent;
- If not equivalent, both authorities have to concur if and where they are compatible;
- Research question: Can an automated Domain Security Policy Language Processor be created to determine if two policies are equivalent, compatible, or neither?

Multi-Level Security Domains

- A Security Domain can have a multi-level policy for one or more security services;
- Example: A Domain Security Policy may allow supporting low & moderate confidentiality services and moderate & high integrity services;
- Two entities from a multi-level domain must be assured that an appropriate level protection is provided for the keys and metadata by the CKMS in accordance with the multi-level policy.
- Question: Can this assurance be automated?

Three(+) Cooperating Entities

- Trust among entities in the same simple Security Domain is associative and commutative.
- Trust among entities in equivalent Security Domains may be associative and commutative.
- Research Question: Can (How can) Trust among multiple entities in different Security Domains be made distributive?

  i.e., Does A ~ B and B ~ C imply that A ~ C?

CKMS Federal Profile: Future Features that may be “Nice to Have”

- Multi-Level Security: Selectable based on requirements and costs (e.g., processing time) ;
- Scalable Security: Selects acceptable level of protection while minimizing costs;
- Selectable Security: CKMS Multi-Domain Policy Enforcement supports selectable security;
- Negotiated Security for Transaction: Based on the policies of two or more entities participating in a sensitive transaction;
  - Requires creation of a new temporary or permanent Security Policy for the transaction.

Federal, National, Global CKMS

- Current Draft Profile created for U.S. Federal Sector including Agencies and Contractors.
- A Private Sector (e.g., Financial, Health, Industrial) can create its own CKMS Profile.
- A Foreign organization can create its own Profile based on local standards, laws, requirements.
- A Global CKMS could provide security for multiple domains in multiple countries if given a formal and robust policy specification language.

Future CKMS Design Alternatives

- Enforces CKMS Policy + one Domain Policy;
- Enforces CKMS Policy + several Domain Policies;
- Enforces CKMS Security Policy + assists Domain Administrators in creating a new Domain from two compatible Domains;
- Enforces CKMS Security Policy + automatically creates new Domain from two or more compatible Domains;
- Automatically creates a new Domain for two or more mutually suspicious but cooperating entities from compatible Domains.

Final Thoughts

- Organizational policies must identify goals, threats, risks;
- Information policies must establish data categories, labels, sensitivity levels, handling restrictions, roles, responsibilities;
- Data Security policies must specify human, physical, communications, and computer protections for data;
- CKMS Policies should be configurable and automated to manage keys that protect sensitive applications and data.
- Global secure applications must support various policies.
- Goal: Automated security policy specification, negotiation, and enforcement is desirable for sensitive applications among mutually suspicious but cooperating organizations.
  - Key Management based on automated dynamic Domain Security Policy support will help meet this goal.