

# IEEE Key Management Summit 2008

## Cryptography Everywhere

### *A Security Administrator's Nightmare*

Tim Hahn

Chief Architect Secure Systems and Networks  
IBM Distinguished Engineer

# Topics for Discussion

- Where, when, and why cryptography is used
- Who is maintaining the keys
- There must be a better way
- Requirements for Key Management Systems
- Recommendations

# Motivations for Using Cryptography

- Increasing pressure on organizations to protect access to information
  - intended access paths
  - un-intended access paths
- Government and industry regulations require special handling of information
  - PCI-DSS
  - State regulations for handling personal information
- Protect information from disclosure even if that information is lost or stolen

# Where Cryptography is Used

- Operating Systems
  - Protected keyrings (key stores)
  - Encrypting file systems
- Applications/Application Infrastructures
  - Application Servers
  - Databases
  - Messaging Infrastructure
- Encryption-enabled Devices
  - Disk and tape drives
  - Flash memory: USB and SSD
- Endpoint systems
  - handheld devices
  - personal computers
- Network Equipment

# How Cryptography is Used

- Data in flight
  - Virtual Private Networks (VPNs)
  - SSL/TLS connections (using public/private keys and certificates)
  - Messaging infrastructures (using SSL/TLS or shared secrets)
  - WS-Security
- Data at rest
  - File and folder encryption – including the use of intermediate devices
  - Removable media (tape) encryption
- For sharing user credentials between organizations
  - Federated Identity Management
  - Credential formats such as SAML

# Who Maintains the Keys

- Key Management is driven by the tools and applications where it is used
  - System Administrators manage keys used for operating systems
  - Network Administrators manage keys used in networking equipment
  - Storage Administrators manage keys used for Storage Device-level encryption
  - End users manage keys used for Endpoint devices and mail (!)
  - Database Administrators manage keys used for database field-level encryption

# Stop the Insanity!

- There must be a better way!
- Ensuring proper and controlled handling of key material requires discipline and skill
- Ensuring business continuity and also secure handling of keys implies
  - centralized administration
  - across widely dispersed computing systems, devices, and applications
  - running both connected and disconnected

# Existing Publications as Guides

- NIST SP 800-57
  - Define a State Model for Key material
  - Define basic functions
    - Creation, Distribution, Backup, Archive, Recovery
  - Guidelines for Access Control and Audit
  - Suggestions for Centralized Key Management Procedures
- ANSI X9.24
  - Management of symmetric keys
  - Keys used for financial services:
    - Point of Sale (POS)
    - Automated Teller Machines (ATM)

# Some Useful Definitions

- Key Store
  - where key material is held
- Key Serving
  - providing a key to a key-using entity (device or software) at or near the time of use
- Key Administration
  - backup/recovery, archive/restore, rotation, refresh, renewal, synchronization, life cycle, ownership, audit, and long term retention of key material

# Requirements

- Centralized Administration of keys
  - Across systems, applications, devices
  - Across key types – public/private, symmetric, derived
- Maintain key material lifecycle according to NIST 800-57 state model
- Support distributed stewardship of key material
- Distribute key material to required locations prior to use
- Serve key material to applications at the time of use
- Interact with signing authorities to support automated renewal and subsequent distribution

# Recommendations

- Create a Key Management standard which
  - supports all key types
  - applies to applications, systems, and devices
  - allows for converged administration
- Define a converged Key Management protocol
  - supporting all key types
  - applicable to a wide range of use cases
  - supporting:
    - key storage
    - key serving
    - key administration

# Summary

- Cryptography is employed in many places and in many ways across a computing environment
- Key management responsibility is dispersed amongst many IT roles
- Compliance and attention to security demand better governance over key material
- Requirements for Key Management systems arise from existing standards
- Converged Key Management is necessary across
  - applications
  - systems
  - technologies
  - vendors