Workshop Summary

Elaine Barker

National Institute of Standards and Technology (NIST)

For those viewing via webcast, please submit questions to kmwquestions@nist.gov

Key Management: Why and How

- Need to undertake key management as part of national cyber security initiative
  - Workshop is a first step
- Joint Government Industry Partnership is the best
- Key Organizations to be involved:
  - NIST and Other Government Agencies
  - Standards Groups
    - IETF
    - IEEE
    - OASIS
    - Others
  - Industry and Academia

Key Management: For Whom

- E Commerce
- Banking
- Air Traffic
- Aerospace
- Defense
- First Responders
- Health care
- Internet (Routing, DNSSEC, etc.)
- Citizens and Consumers

3

Considerations for Future Key Management Systems

- Design systems for high availability
  - Survivable KM Systems
  - Emergency access to keys
- Worry about unintended consequences
  - Good and bad
- In light of quantum computing
  - Look at means other than public key
  - Look at quantum resistant algorithms and schemes

4

Requirements

- User-Friendly
  - Easy to use – Plug and Play
  - User Driven capability
- Secure
- Cost-Effective
- Fault-tolerant, highly available
- Protection against destructive attacks
- Interoperable
  - Enterprise-Wide
  - Multi-Partner
  - Multi-Vendor
  - Multi-Application

5

Requirements

- Scalable
- Enhanced Interoperability in time of emergency
- Metadata
- Metadata security

6

Requirements

- Key Inventory Control
- Accountability/Auditing
- Policies for managing keys and metadata
- Safety requirements for certain applications

7

Challenges: What Makes KM Hard

- Cost
- Enrollment
- Complexity
- Future Computing Paradigms are unclear (e.g., Cloud Computing)
- User-Friendly
- Security Analysis
- Competing Solution; Do not Interoperate

8

Applicable Models

- Life Cycle
  - Birth to death
- Security Analysis
  - Model all actors and actions
- Information Management Models

9

Users of KM System

- Who are the users of key management?
  - Human users
  - Devices
  - Applications
  - Programmers
  - Administrators
  - Others ?
  - All of the Above?

10

Design Considerations

- Mix of long-term symmetric and asymmetric keys for some applications
- Algorithm Agility
- Security Parameters Agility
- Keep it simple
- Keep it cheap

11

Technologies and Standards

- Identity Based Encryption
- Enterprise Key Management
- OASIS KMIP
- CMC
- Use factory-generated device keys for Enterprise enrollment and registration
- Identity based symmetric keys may reduce the scale of symmetric key distribution problem
- Cloud computing
- Subset Difference Revocation
- Group Key Management: Contributory

12

Next Steps

- Send Comments (including comments on the webcasting process) to:
  - keymanagementworkshop@nist.gov
- Conference Blog
  - http://keymanagement.wordpress.com/
- Workshop Page (will include slides, workshop recording links, future reports, etc.)
  - http://csrc.nist.gov/groups/ST/key_mgmt/

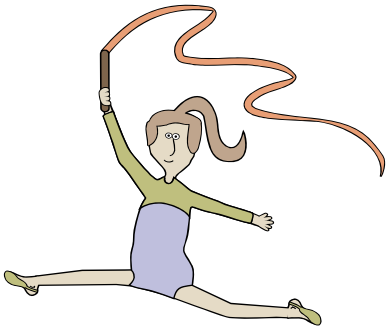
13

Next Steps

- Workshop Summary Report in July 2009
- Key Management Framework Annotated Outline circa Fall 2009
- IEEE Key Management Workshop in Spring 2010
- NIST Recommendations for further Research and Studies

14

What Did I Miss?



For those viewing via webcast, please submit questions to kmwquestions@nist.gov

15