REPORT OF THE WORKSHOP ON KEY MANAGEMENT USING PUBLIC KEY CRYPTOGRAPHY

February 10-11, 2000

A workshop was held at the National Institute of Standards and Technology (NIST) on February 10-11, 2000 to examine public key-based key establishment techniques that are currently available and to discuss the approach to the development of a Key Management Standard for Federal Government use. A list of registered attendees may be found on the KMS web site (http://www.nist.gov/kms).

Goals

NIST's goal for the development of the KMS is to complete their cryptographic tool kit, which includes algorithms for encryption, digital signatures, hashing, random number generation, entity authentication, and password generation. As with the other elements of the toolkit, the schemes defined in the KMS must be testable using the FIPS 140-1 process.

The stated goals of the workshop were to:

- Discuss the development of a FIPS that (1) contains secure key establishment schemes that are compatible with both Federal Government and private sector applications and (2) discusses key management issues (generation, protection, destruction, recovery, storage).
- Concentrate on key establishment schemes; these schemes should be considered as separate from communication protocols, but should be compatible with communication protocols as much as possible.
- Determine schemes that are useful for numerous unclassified applications and environments.
- Use existing or emerging standards/schemes.
- Minimize patent concerns.
- Maximize interoperability potential.

User Perspectives/Requirements

User perspectives and requirements for a Key Management Standard were provided for the Federal Government (Richard Guida), the financial institutions (Cindy Fuller and Marty Ferris) and the wireless community (Doug Rahikka). Mr. Guida's and Mr. Rahikka's presentations are provided on the KMS web site.

- Mr. Guida, Chair of the Federal Public Key Infrastructure (PKI) Steering Committee, stated that the government supports standards that are open in nature, promote interoperability, fully implement X.509 certificate path discovery and processing, support separate key pairs for digital signatures and encryption, and contain appropriate specificity so as to be unambiguous and clear to implementers. In addition, systems must support encryption key recovery for data in storage; no requirement for the recovery of encryption keys for data in motion has been identified. However, a need has been

identified for storing information as received as a proof of receipt for legal purposes. The government needs encryption for inter- and intra-agency, agency to trading partner, and agency to public interactions. The government has committed to the use of commercial-off-the-shelf (COTS) equipment, but this equipment must satisfy the security needs of the agencies.

- Cindy Fuller from the American Bankers Association (ABA) and Marty Ferris from the Financial Institution Protection Association reported that the American National Standards Committee X9F subcommittee on security in the financial industry is in the process of developing three public key-based standards for key establishment: ANSI X9.42, ANSI X9.44 and ANSI X9.63 (see the summaries and presentations for these three standards on the KMS web site). The financial community needs security tools that will facilitate trade, remove technical barriers, and are convenient and cost effective to use. More information on ABA and X9F may be obtained from the X9 web site at http://www.x9.org.

- Doug Rahikka, NSA, represented the wireless community and indicated that most government users need robust, efficient and scalable COTS products. These products should have high data rates and low bandwidth that will handle sensitive but unclassified (SBU) information and will rely on the commercial wireless (cellular) infrastructure. The smaller population of government wireless voice and data users requiring high level security were originally foreseen as needing to be backwards interoperable with the government's STU-III secure telephone unit (and its nonstandard modems). This would have required unique cellular STU-III bearer services, recently standardized within the Telecommunications Industry Association (TIA) standards bodies. Upon realization that the STU-III modem inter-working functions cannot be easily woven into the cellular switching infrastructure fabric, it has been decided that newly emerging government high level security wireless equipments will not require STU interoperability, but will ride transparently over standard commercial transport infrastructures and protocols by way of an end-to-end secure signaling protocol called FNBDT (Future Narrow Band Digital Terminal). Due to a heavy reliance on commercial wireless for providing native security to unclassified and SBU government users, and for providing a transport mechanism for end-to-end FNBDT-enabled security users (with enhanced specialized terminals), the government has been closely following the development of enhanced authentication and voice privacy algorithms as currently being designed within the TIA. These requirements are shown in the slide presentation, including publicly scrutinized protocols and algorithms, 128-bit privacy keys, a negotiation capability in the protocols, and backwards compatibility with older systems. Algorithms to be used in future cellular devices will likely include SHA-1 and the Advanced Encryption Standard (AES), which is currently under development (see http://www.nist.gov/aes).

Vendor Perspectives

The vendors and protocol developers in the audience were asked what direction they saw the marketplace going? What were the concerns? The response given was to remind the audience that the products currently in the field are not covered by a FIPS, and NIST needs to consider the current communication protocols when considering the key establishment scheme(s) to be standardized. [NOTE: I NEED HELP WITH THIS SECTION.]

Key Establishment Scheme Presentations

Several key establishment schemes currently under development were presented. A slide presentation and either a summary of the standard or link to the appropriate document is provided for each standard on the KMS web site.

- Sharon Keller from NIST presented ANSI X9.42, *Agreement of Symmetric Keys using Discrete Logarithm Cryptography*. ANSI X9.42 will soon be balloted out of committee, after which it will be sent out for public comment. ANSI X9.42 specifies six methods using the Diffie-Hellman (D-H) technique and two methods using MQV technique. Both D-H and MQV use Mod P math in ANSI X9.42. The standard also includes specifications for domain parameter generation and validation, key pair generation, public key validation, and key derivation from shared secret numbers.

- Burt Kaliski from RSA Labs presented ANSI X9.44, *Key Establishment using Factoring-Based Public Key Cryptography for the Financial Services Industry*. ANSI X9.44 is currently under development and may change significantly over the next few months. In its current form, ANSI X9.44 includes specifications for the generation of RSA and Rabin-Williams key pairs, cryptographic primitives for encryption and decryption, and schemes for both key agreement and key transport. Dr. Kaliski also identified a number of other standards to be considered during the development of the Key Management FIPS (see slide11), including S/MIME/CMS[1] key transport, SSL/TLS[2] key agreement, ISO/IEC 11770-3[3] and ANSI X9.70[4].

- Simon Blake-Wilson from Certicom presented ANSI X9.63, *Key Agreement and Key Transport using Elliptic Curve Cryptography*. ANSI X9.63 will soon be completed and balloted out of committee, after which it will be sent out for public comment. ANSI X9.63 specifies eleven schemes for key agreement: six

---

[1] Secure Multipurpose Internet Mail Extension/Cryptographic Message Syntax; available as RFC 2630 at ftp://ftp.isi.edu/in-notes/rfc2630.txt.

[2] Secure Sockets Layer/Transport Layer Security, available as RFC 2246 at http://sunsite.auc.dk/RFC/rfc/rfc2246.html.

[3] International Standards Organization/International Electrotechnical Commission 11770-3, *Information Technology, Security Techniques - Key Management - Part 3: Mechanisms using Asymmetric Techniques* (draft); see http://www.cancert.ca/Pages/27nSD7.htm for a catalog of ISO standards.

[4] ANSI X9.70, *Management of Symmetric Keys using Public Key Algorithms* (draft); refer to the American Banker's Association, http://www.x9.org.

distinct schemes using the Diffie-Hellman technique, two distinct schemes using MQV, and three schemes that add a key confirmation capability to one of the basic schemes. ANSI X9.63 also specifies two schemes for key transport. All schemes use elliptic curve math. In addition, the standard includes specifications for domain parameter generation and validation, key pair generation, public key validation, key derivation from shared secret numbers, an asymmetric encryption scheme, and a signature scheme.

- Sheila Frankel from NIST presented the Internet Key Exchange (IKE) protocol that was developed by the IPsec working group of the Internet Engineering Task Force (IETF). IKE includes specifications for the generation, exchange and establishment of keys for security associations using Diffie-Hellman, using both Mod P and elliptic curve mathematics.

- Chris Hawk from Certicom presented the Transport Layer Security (TLS) protocol developed by the Network Working Group of the Internet Society and published as RFC2246. TLS is a client-server protocol, where the client is defined to be the entity that sends the first message. The TLS protocol includes the establishment of symmetric keys using RSA key transport and Diffie-Hellman key agreement techniques.

The attendees suggested a number of other documents that could be considered when developing the Key Management FIPS.

- Robert Moskowicz from ICSA, an attendee at the workshop, announced that he is in the process of developing an internet draft for a Host Identity Payload (HIP). HIP is a new Key Management protocol. Details may be found at http://www.ietf.org/internet-drafts/draft-moskowitz-hip-arch-01.txt, http://www.ietf.org/internet-drafts/draft-moskowitz-hip-01.txt, and http://www.ietf.org/internet-drafts/draft-moskowitz-hip-impl-00.txt.

- Robert Zuccharato from Entrust suggested that RFC 2025, *The Simple Public-Key GSS-API Mechanism (SPKM)* should be included for consideration. This document may be found at http://sunsite.auc.dk/RFC/rfc/rfc2025.html.

- Richard Gray suggested that the ATM Security Specification (af-sec-0100.001), available from http://www.atmforum.com/atmforum/specs/approved.html, might be considered.

- Russ Housley from Spyrus suggested that NIST consider IEEE 802.10C, the *Interoperable LAN/MAN (Local and Metropolitan Area Networks) Security (SILS): Key Management (Clause 3)*. This standard is available from the IEEE Standards Association catalog at http://standards.ieee.org/catalog/IEEE802.10.html.

Patent Issues

Many of the key establishment schemes have patents on them. The attendees advised that at least one scheme in the Key Management FIPS should be non-patented or royalty free. Known patents from Certicom and IBM on ANSI X9.42 and X9.63 are provided on the KMS web site.

- RSA's patent (relevant to ANSI X9.44) expires in September 2000. However, other patents may be infringed.

- Licenses that apply to patents for techniques that appear in ANSI standards state that the terms are reasonable and non-discriminatory.

- Licenses for patents that apply to IEEE standards have been declared to be reasonable and non-discriminatory.

- Techniques developed using Federal government money are royalty free to the government.

- UMAC (specified at http://www.cs.ucdavis.edu/~rogaway/umac/) and HMAC (specified in ANSI X9.71 and RFC 2104) may not be covered by any patents. For ANSI X9.71, contact the American Banker's Association at http://www.x9.org. RFC 2104 is available at http://www.ietf.org/rfc2104.txt.

Performance and Cost Issues

The attendees expressed concern over the implementation of a key establishment scheme in restricted environments, such as smart cards and cellular phones. NIST should consider the processing capability in these environments, as well as power consumption, bandwidth, error rates and memory size.

Other Issues

A number of other issues were brought up for consideration during the workshop:

- Concern about a hostile party interrupting or subverting the process. The schemes should be resilient when attacked by hostile entities.

- The key establishment schemes should be scalable.

- Consider how a responder might dictate the terms of a key agreement.

- Consider allocating the work of the key agreement scheme to the initiator, if appropriate. Consider allowing an imbalance in processing capability, as in the case of a client/server model.

- Consider resistance to denial of service attacks.

- Consider including an ability to determine the assurance afforded to an implemented scheme/process, i.e., how well built is it?

- Consider incorporating an indicator in a certificate that identifies the assurance level of the implementation.

- Consider issues associated with life cycle management of the keys.

- Consider selecting a scheme with the best security attributes for a given environment.

Key Management Standard Approach and Contents

The attendees were requested to provide their views on the approach and content of a Key management FIPS.

Approach:

- The development effort should be divided into multiple parts. The initial effort should be the identification of key establishment schemes, hereafter called the scheme standard. Other parts could address protocols and other key management considerations. Additional guidance could be provided concerning:
  - the quality of an implementation,
  - a tutorial for use of the schemes in assorted environments,
  - advice on Computer Security for the new/naïve user.
- Consider creating profiles for industry standard communication protocols such as TLS.
- Consider using the proposed NIST Recommendation, when appropriate. The concept of the NIST Recommendation is currently under discussion. The intention of the Recommendation is to provide guidance in a timely fashion either until a FIPS is fully developed and approved, or instead of pursuing the FIPS process. A Recommendation would be intended to have more "clout" than a guideline.
- Future workshops could be held to discuss the selected schemes or to address interoperability issues in order to provide NIST with further guidance.
- Ongoing interaction with the public sector should be continued.
- Prepare a "framework" document, initially, that discusses the documents to be developed, their proposed content and includes a timeline of the development process.
- Consider adopting the ANSI key establishment standards until a FIPS is available. Consider making this statement in FIPS 140-2.

Contents:

- The scheme standard should include Diffie-Hellman, RSA/Rabin-Williams and Elliptic Curve techniques as specified in ANSI X9.42, X9.44 and X9.63.
- The scheme standard should include "flow" of information for illustrative purposes. These flows should not be considered as communication protocols, but would be incorporated in such protocols.

- The standards should be written to be testable. The scheme standard should be written to be testable using the NIST Cryptomodule Validation Program (CMVP) and the FIPS 140-1 process, e.g., the scheme should be able to tested as if it were a "black box", with the output being a symmetric key and appropriate descriptive data, e.g., control vectors.
- The standards should be written for the vendors to implement and the labs to test.
- Refer to IEEE P1363-2000 for ideas for presentation within the scheme standard and for a discussion of security attributes.
- A protocol standard should include an abstract definition of the protocol (e.g., ASN.1) and may also include concrete definitions, whereby the order of the bits and bytes are unambiguously defined.
- A standard that addresses key management should address "security association" management and the negotiation of cipher suites (e.g., what algorithm will be used for key establishment, what algorithm will be used for data encryption, what keys sizes will be used, etc.).
- Include specifications for the representation of keys, e.g., using an ASN.1 OID (Object Identifier). Use the most efficient bit specification method.
- Allow for 1-Pass, 2-Pass and 3-Pass protocols.
- Include a table of security properties; this may not be possible for the schemes without placing that scheme in a communication protocol. Note that when key recovery techniques are included, perfect forward secrecy may not be possible.
- Include a fully defined key derivation function.
- Consider pointing to a recommended set of domain parameters. Note that, in the case of elliptic curve cryptography, NIST has published a set of recommended curves for Federal Government use.
- Supply key sizes and modulus sizes that are consistent with the key sizes used for the AES.
- Consider including other recommended parameters, encoding restrictions, exponent sizes and elliptic curves, when appropriate.

Future Schedule

Due to limited resources at NIST and an intense effort to develop the AES before the end of FY2000, intensive efforts to develop a Key Management Standard cannot be initiated until the beginning of FY2001. However, in the meantime, the recommended documentation for consideration can be acquired and comments solicited about the development effort. A "framework" document that discusses the documents to be developed, their proposed content and includes a timeline of the development process will be prepared first. It is anticipated that a draft of this document will be available for review during the first quarter of FY2001.