Key Management Workshop Issues
November 1-2, 2001

Key Establishment Schemes Workshop Document

Schemes

1. Precomputation of ephemeral keys is sometimes desirable to prevent denial of service attacks.
2. A C(2,1) scheme such as the one in RFC 2945 should be considered.
3. A symmetric key-wrapping scheme should be provided.
4. Consider providing or allowing an Extensible Authentication Protocol, a zero knowledge protocol, and a multicast protocol (MSEC).
5. Allow for low entropy keys derived from passwords.
6. Consider schemes for wireless systems.
7. Consider IKE, TLS, S/MIME, and IPSEC schemes. Although these widely used protocols may have a scheme that is similar to one specified in the schemes document, these protocols would probably not meet all the requirements of the schemes document (e.g., domain parameter validation and key derivation). Will NIST make an exception list of protocols that use at least some schemes that are close to, but not fully compliant with, the schemes standard?
8. Allow for anonymous user systems.

Key Derivation Function (KDF)

1. Do not use the U AND V or U OR V technique.
2. Put U and V in sort order as in X9.42.
3. Consider whether IDs should be mandatory or only optional. Some attendees preferred optional IDs.
4. Add or use the X9.42 method with ASN.1 coding.
5. Unify X9 techniques.
6. Allow for multi-user systems
7. Use a KDF with provable properties. How random are the bits?
8. Allow for anonymous users.
9. Investigate how the proof for KDF was done in IKE.

Key Confirmation (KC)

1. Consider SRP KC (RFC 2945).
2. There seemed to be general agreement that KC should be optional.
3. Perhaps KC should be moved to the Guideline.
4. KC should be defined and the security properties discussed.

Desired Key Establishment Attributes

The following attributes were considered as desirable:

1. Identity confirmation
2. Forward secrecy
3. Anonymity?

4. Denial of service prevention
5. Proofs of security
6. Ease of upgrades to better security

Public Key and Domain Parameter Validation

1. Domain Parameter Validation and Public Key Validation should be specified in the schemes document rather than referenced by it.
2. NIST should consider whether validation of domain parameters and public keys should be optional. If domain parameter validation is required, many of the existing protocols will not comply (See Schemes #7). Also, the domain parameter validation method of X9.42 requires that a particular prime generation method be used. This level of standardization may not be desirable.
3. Consider whether Domain Parameter Validation may be used in a denial of service attacks.

Scheme Validation

1. Where does the scheme boundary end? Inside of the cryptographic module, inside of the product, or inside of the protocol? (Note: this question refers to the boundary of a FIPS 140-1/2 cryptomodule.)
2. At what level will testing be conducted?

Appendices

1. Give examples of complex functions that are not provided in the referenced ANSI documents (e.g., NIST approved elliptic curve examples).
2. Discuss denial of service attacks and explain how they may be mitigated.
3. Discuss how the schemes mitigate attacks.

Password Derived Keys and ANSI X9.44 Presentations

1. Password derived key establishment schemes such as those specified in P1363.2 should be allowed
2. RSA will propose RSA-KEM for inclusion in ANSI X9.44. RSA-KEM would provide for “tight security proofs”.

Process

1. Provide new drafts ASAP even though they are not complete. The industry and other standards groups will consider techniques specified in drafts. This is superior to waiting until a complete draft is ready because then it may be too late to influence other groups.

Key Management Guideline Workshop Document

1. Introduction

1. Explain why this document and key management are important. Poor key management may easily compromise strong algorithms. Possible examples include weak products, inappropriate algorithm pairing, poor physical security, weak protocols, etc.
2. Authentication of networking components as described in 802.1x should be mentioned.
3. This document has multiple audiences. The Content/Organization section should identify how each type of reader might use the document. What sections are applicable to each group? In other words, explain how to use the document.
4. Verify that "must" and "should" are used properly throughout the document.
5. Throughout document remove redundancy in "public/private key pairs".
6. Change "secure media" to "secure storage".
7. Provide a different definition for "split knowledge".
8. Provide guidance for setting up and managing a key management structure.

3. Cryptographic Algorithms

1. Explain why FIPS approved cryptographic algorithms are important (e.g., government analysis, common levels of security, interoperability, and five year review).
2. Consider not "hard coding" the approved algorithms.
3. Point out the security differences between unkeyed hashes, keyed hashes, and MACs
4. Change 3.2.2 title to "Symmetric Key Algorithms used for Encryption and Decryption".
5. Section 3.2.5 states that "If a public key algorithm is used to distribute the keying material, the key encrypting key is actually a key pair". Just say a key pair is employed.
6. Discuss why you need authentication with encryption.
7. Could add discussion of provable algorithms in the future.

Table 1

1. Clarify whether Master keys used for key derivation and keys derived from a master key are always symmetric.
2. The X in a box sometimes indicates a requirement and at other times indicates an option. This can be confusing. Also, the table key should be put adjacent to the table.
3. Jim Schaad had many suggestions for revising this table and he said he would submit his version of the table.
4. Add a short term key wrapping key. (Or indicate that a key wrapping key may be either long or short term.
5. Add a category of short term key.

6. Add a security services column.
7. Add a cryptoperiod column.
8. Consider adding the encrypted data, MAC, Signatures, and key IDs as other keying material portion of the table.
9. Do ephemeral key pairs require integrity protection?
10. Don't private keys (e.g., signing keys) need to be associated with their owner? If so, the table does not indicate this.
11. Secret authentication keys and public authentication keys need to be associated with other information only as long as validation is desired.
12. When the keys are grouped into categories as per the viewgraphs presented by Miles, it becomes apparent that **secret key agreement keys** are missing.
13. Clarify whether Master Keys and keys derived from Master keys are always symmetric keys.
14. Long and short term Master Keys may need to be considered separately.
15. Define "associated". See the IPSEC security association in RC 2401. In this document, the security association is defined for a whole set of data, not just encrypted information.
16. Most IV implementations do not protect either the confidentiality or the integrity of the IV.

4. Key Management Lifecycle

1. Map the subsections into the four major categories.
2. Should a diagram be added?
3. Clarify that not every state is required by all systems. Some stages may be combined or occur in a different order.
4. System and User Initialization may also include the specification of algorithm preference and trusted parties.
5. In Section 4.1, clarify the use of ID material (passwords, PINs, and email addresses) in user registration.
6. In Section 4.2, initialization might include specifying user algorithm preferences, trusted parties, domain parameters, policies, and other trust parameters.
7. Ephemeral keys may not need to be associated with their domain parameters. The mechanism may provide the association.
8. Give examples of when shared secrets are retained and when they are not.
9. Note that password generation does not seem to be mentioned. Yet this might be the weakest security link.

Key Establishment

1. In Section 4.4.1, consider the distribution of a public key to a registration authority as well as distribution in certificate after it is signed.
2. In Section 4.4.2, add keys derived from a master key?
3. In Section 4.4.2, why is the random generation of symmetric keys left optional?
4. In Section 4.4.2.1 why is FIPS 140-2 only optional? Doesn't the standard require that all FIPS approved cryptographic functions such as key generation be performed in a FIPS 140-2 approved module?

5. The requirement for FIPS 140-2 or a controlled access facility does not make any sense. A controlled access facility offers some physical security. But FIPS 140-2 level 1 offers virtually no physical security. It seems as though you would at least want a FIPS 140-2 level that offered an equivalent amount of physical security. If on the other hand, you only want controlled access, then the FIPS 140-2 requirement is not necessary. What is the goal of this requirement?
6. Address the distribution of key shares for private keys.
7. Distinguish between the distribution of public keys to a registration authority from general distribution of the public key (e.g., in a certificate).
8. For key generation, include the derivation of a key by a master key.
9. Distinguish between ephemeral and long term key generation.
10. In Section 4.4.3.4, distinguish between seed and salt (i.e., salt can be made public where seed can be kept secret). However, ANSI and FIPS terminology often allows public seed values.
11. In Section 4.7, protect the integrity of the association as well as providing the association.
12. In Section 4.7.1.1, note that split knowledge systems can be *k* of *n* systems. Also there are split systems where an individual controls but does not know the actual secret share. See IKE in IPSEC.
13. In Section 4.7.1.2, note that integrity protection is not generally on IVs and ephemeral public keys.
14. In Section 4.7.1.4, add that private keys must be associated with their corresponding public keys.
15. In Section 4.7.1.6, add,as an example, that for a secret authentication key, the association must be maintained for as long as you need to sign data, and for a public authentication key, for as long as you need to verify data.
16. Keys may be associated with the context, destination, IP address, counters, etc. See RFC 2401 (Security Associations).
17. Consider other key types, such as encrypted keys.
18. Master keys may be a bad idea when doing a one-way transformation.
19. Discuss when a master key is saved and when it is destroyed while the derived keys are saved.
20. Define the meaning of “associate”.
21. Remove the “domain parameter” bullet.
22. Consider derived IVs.
23. The association of an IV to the protected data may be inherent in the scheme.
24. Examples of when and when not to store the shared secret should be given and the implications discussed.
25. A discussion of public and private seeds should be provided.
26. Consider “module storage”?

Storage of Keying Material

1. Define storage to be when keys reside outside of the cryptographic module.
2. In Section 4.7, define Operational Storage.

Backup Storage

1. In Section 4.7.3, define backup storage to be when keys are stored securely on an independent medium.
2. Backup secret authentication keys until ….. (cryptoperiod?)
3. More advice may be needed about when and when not to backup.
4. Backup of static key agreement private key may not be sufficient.
5. In Table 2, what does OK mean? Under what conditions is it OK to backup?

Key Archive Storage

1. Further differentiate between authentication and authorization keys.
2. You may want to archive authorization keys, but probably not authentication keys.
3. Will this guidance ever be used?
4. You don't need to say that archived public keys should be destroyed.
5. If you archive private signing keys
6. Authorization key may need to be archived.
7. Public auth(?) key may or may not need to be archived.
8. Identify what should or should not be archived.
9. Review the relationship between authorization and authentication.

Key Update

1. Clarify the definition of update versus rekey.
2. Easier to do but not as secure as rekey.
3. May be required when?
4. Discuss the effects of compromise. Protect back keys? Protect forward keys?
5. Consider a case in between key change and key update (i.e., Key + Random = New Key).

Key Recovery

1. The last sentence should begin with "The KRI may include the key ……"

Key De-Registration

1. Elaborate on meaning of "erase".

Key De-registration and Destruction

1. One may need to retain a record of keys that have been destroyed.
2. Should define what "erase" means?

Key Revocation

1. Change "notification" to "notification, if appropriate".
2. Clarify that a push system is not preferred over a pull system.
3. Just because a key is revoked does not necessarily mean that it should not be used.
4. The PKI may not know who is associated with a revoked key.

5. General Key Management Guidance

1. Add discussion as to why conformance testing of products to FIPS standards is important.
2. What should we do first? ANS: Restructure by (1) breaking storage to storage inside the module and storage outside the module; (2) explaining why things are important and what you should look out for; (3) explaining tables; and (4) discussing management infrastructure and roles.
3. Focus on evaluator checklist.
4. Give a sample draft of a key management practices statement.
5. There are two sections labeled as Section 5.1.3.
6. In the first Section 5.1.3, a suitably defined cryptoperiod helps to limit the listed items.
7. In the first Section 5.1.3, mention the security live of data as one of the (bulleted) factors affecting the risk of exposure.
8. In the second 5.1.3, not every ephemeral key is validated. Other ways to compensate if a PK is not validated include (1) use the cofactor, and (2) set up parameters to compensate. Another remark was to use "proof of possession" instead of domain parameter validation.
9. Public key validation should be optional.
10. In Section 5.1.6, distinguish between the audit of policy and the audit of practices.
11. Key recovery may involve more than just the recovery of keys from back up or archive. It might be the whole process by which keys and other key recovery information may be recovered. This involves backing up and storing the information in the first place.
12. Make sure that both insertion and retrieval are covered.

7. Selected Protocols

1. Add IPSEC to this section
2. Consider CMS (the superset of S/MIME)
3. Perhaps NIST could approve certain suites of TLS.

General Procedures, Questions, and other Comments

1. Provide drafts of each completed section for comment. Don't wait until the entire document is complete before making public.
2. Getting out parts that are stable will give reviewers confidence that work is getting done.
3. Will there be a large bibliography?
4. Add Key Establishment Scheme guidance that is not provided in schemes document.