Network Working Group
Request for Comments: 2411
Category: Informational

R. Thayer
Sable Technology Corporation
N. Doraswamy
Bay Networks
R. Glenn
NIST

November 1998

IP Security
Document Roadmap

Status of this Memo

Copyright Notice

Abstract

The IPsec protocol suite is used to provide privacy and authentication services at the IP layer. Several documents are used to describe this protocol suite. The interrelationship and organization of the various documents covering the IPsec protocol are discussed here. An explanation of what to find in which document, and what to include in new Encryption Algorithm and Authentication Algorithm documents are described.

Table of Contents

1. Introduction

This document is intended to provide guidelines for the development of collateral specifications describing the use of new encryption and authentication algorithms with the ESP protocol, described in [ESP] and new authentication algorithms used with the AH protocol, described in [AH]. ESP and AH are part of the IP Security architecture described in [Arch]. There is a requirement for a well-known procedure that can be used to add new encryption algorithms or authentication algorithms to ESP and AH, not only while the initial document set is undergoing development but after the base documents have achieved RFC status. Following the guidelines discussed below simplifies adding new algorithms and reduces that amount of redundant documentation.

The goal in writing a new Encryption Algorithm or Authentication Algorithm document is to concentrate on the application of the specific algorithm within ESP and AH. General ESP and AH concepts, definitions, and issues are covered in the ESP and AH documents. The algorithms themselves are not described in these documents. This gives us the capability to add new algorithms and also specify how any given algorithm might interact with other algorithms. The intent is to achieve the goal of avoiding duplication of information and excessive numbers of documents, the so-called "draft explosion" effect.

2. Interrelationship of IPsec Documents

The documents describing the set of IPsec protocols are divided into seven groups. This is illustrated in Figure 1. There is a main Architecture document which broadly covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology.

There is an ESP Protocol document and an AH Protocol document which covers the packet format and general issues regarding the respective protocols. These protocol documents also contain default values if appropriate, such as the default padding contents, and mandatory to implement algorithms. These documents dictate some of the values in the Domain Of Interpretation document [DOI]. Note the DOI document is itself part of the IANA Assigned Numbers mechanism and so the values described in the DOI are well-known. See [DOI] for more information on the mechanism.

The "Encryption Algorithm" document set, shown on the left, is the set of documents describing how various encryption algorithms are used for ESP. These documents are intended to fit in this roadmap, and should avoid overlap with the ESP protocol document and with the

Authentication Algorithm documents. Examples of this document are the [DES-Detroit] and [CBC] documents. When these or other encryption algorithms are used for ESP, the DOI document has to indicate certain values, such as an encryption algorithm identifier, so these documents provide input to the DOI.

The "Authentication Algorithm" document set, shown on the right, is the set of documents describing how various authentication algorithms are used for both ESP and AH. These documents are intended to fit in this roadmap, and should avoid overlap with the AH protocol document and with the Encryption Algorithm documents. Examples of this document are the [HMAC-MD5], and [HMAC-SHA-1] documents. When these or other algorithms are used for either ESP or AH, the DOI document has to indicate certain values, such as algorithm type, so these documents provide input to the DOI.

The "Key Management Documents", shown at the bottom, are the documents describing the IETF standards-track key management schemes. These documents provide certain values for the DOI also. Note that issues of key management should be indicated here and not in, for example, the ESP and AH protocol documents. Currently this box represents [ISAKMP], [Oakley], and [Resolution].

The DOI document, shown in the middle, contains values needed for the other documents to relate to each other. This includes for example encryption algorithms, authentication algorithms, and operational parameters such as key lifetimes.

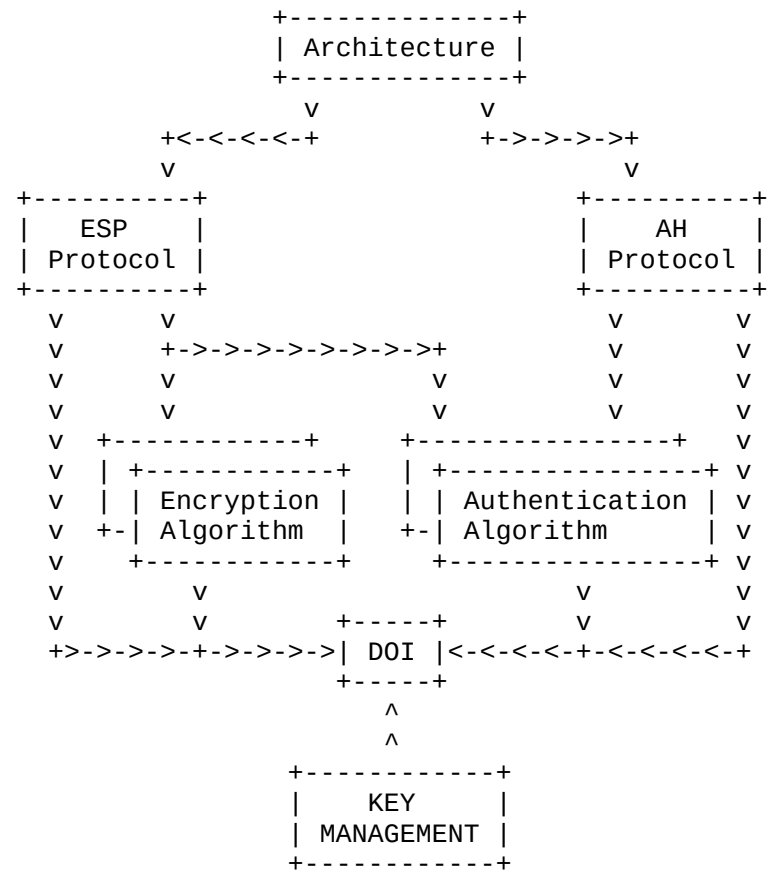

Figure 1. IPsec Document Roadmap.

3. Keying Material

Describing the encryption and authentication algorithms in different documents raises the issue of how the key management protocols knows the required keying material length for the desired algorithms when used together with ESP. It also raises the issue of how to divide the keying material. This is known as the "slicing and dicing" information.

Each Encryption Algorithm and Authentication Algorithm document should specify their respective key attributes (e.g. how to pad, location of parity bits, key order for multi-keyed algorithms, and length). The key management protocols should use the length of the keys specified in the respective Algorithm documents to generate the keying material of required length.

The key management protocol generates keying material with enough strength and size to generate keys for individual algorithms. The IPsec Architecture document specifies how keys are extracted from a single block of keying material when multiple keys are required (e.g. ESP with authentication). The Encryption Algorithm and

Authentication Algorithm documents are responsible for specifying the key sizes and strengths for each algorithm. However, whether the entire keying material is passed down to the kernel to perform slicing and dicing or if the keys are sliced and diced by key management protocol is an implementation issue. The AH protocol document has no such requirement.

4. Recommended Content of Algorithm Documents

The document describing how a specific encryption or authentication algorithm is used should contain information appropriate to that encryption or authentication algorithm. This section enumerates what information should be provided. It is the intention of the document roadmap that:

- General protocol information goes in the respective ESP or AH protocol documents.
- Key management information goes in the key management documents.
- Assigned values and constants of negotiable items go in the DOI document.

Encryption and authentication algorithms require some set of optional parameters or have optional modes of operation (e.g. IVs, authentication data lengths, and key lengths). To help eliminate some complexity involved with key management having to negotiate large numbers of algorithm-specific parameters, encryption and authentication algorithm documents will select fixed values for these parameters when it is deemed technically reasonable and feasible.

Note, the following information is intended as a general guideline only.

4.1 Encryption and Authentication Algorithms

This section describes the information that should be included in both Encryption Algorithm and Authentication Algorithm documents.

Keying Material

- Size of keys, including minimum, maximum, recommended and/or required sizes. Note: the security considerations section should address any weakness in specific sizes.

- Recommended or required pseudo-random number generator techniques and attributes to provide sufficiently strong keys. [RANDOM] provides recommendations on generating strong randomness for use with security.
- Format of keying material.
- Known weak keys or references to documentation on known weak keys.
- Recommended or required processing of input keying material such as parity generation or checking.
- Requirements and/or recommendations on how often the keying material should be refreshed.

Performance Considerations

- Any available estimates on performance of this algorithm.
- Any available comparison data (e.g., compared against DES or MD5).
- Input size or other considerations that could improve or degrade performance.

ESP Environmental Considerations

- Any known issues regarding interactions between this algorithm and other aspects of ESP, such as use of certain authentication schemes. Note: As new encryption and authentication algorithms are applied to ESP, the later documents will be required to address interactions with previously specified algorithms.

Payload Content and Format Description

- Specification of size, placement, and content of algorithm-specific fields not defined in the ESP or AH protocol documents (e.g., IV).

Security Considerations

- Discuss any known attacks.
- Discuss any known common implementation pitfalls, such as use of weak random number generators.
- Discuss any relevant validation procedures, such as test vectors. [RFC-2202] is an example document containing test vectors for a set of authentication algorithms.

4.2 Encryption Algorithms

This section describes the information that should be included in the Encryption Algorithm documents.

Encryption Algorithm Description

- General information how this encryption algorithm is to be used in ESP.
- Description of background material and formal algorithm description.

- Features of this encryption algorithm to be used by ESP, including encryption and/or authentication.
- Mention of any availability issues such as Intellectual Property considerations.
- References, in IETF style, to background material such as FIPS documents.

Algorithm Modes of Operation

- Description of how the algorithm is operated, whether it is block mode or streaming mode or other.
- Requirements for input or output block format.
- Padding requirements of this algorithm. Note: there is a default for padding, specified in the base ESP document, so this is only needed if the default cannot be used.
- Any algorithm-specific operating parameters, such as number of rounds.
- Identify optional parameters and optional methods of operation and pick reasonable fixed values and methods with explicit technical explanations.
- Identify those optional parameters in which values and methods should remain optional with explicit technical explanations on why fixed values and methods should not be used.
- Defaults and mandatory ranges on algorithm-specific optional parameters that could not be fixed.

4.3 Authentication Algorithms

This section describes the information that should be included in the Authentication Algorithm documents. In most cases, an authentication algorithm will operate the same whether it is used for ESP or AH. This should be represented in a single Authentication Algorithm document.

Authentication Algorithm Description

- General information on how this authentication algorithm is to be used with ESP and AH.
- Description of background material and formal algorithm description.
- Features of this authentication algorithm.
- Mention of any availability issues such as Intellectual Property considerations.
- References, in IETF style, to background material such as FIPS documents and definitive descriptions of underlying algorithms.

Algorithm Modes of Operation

- Description of how the algorithm is operated.

- Algorithm-specific operating parameters, such as number of rounds, and input or output block format.
- Implicit and explicit padding requirements of this algorithm. Note: There is a default method for padding of the authentication data field specified in the AH protocol document. This is only needed if the default cannot be used.
- Identify optional parameters and optional methods of operation and pick reasonable fixed values and methods with explicit technical explanations.
- Identify those optional parameters in which values and methods should remain optional with explicit technical explanations on why fixed values and methods should not be used.
- Defaults and mandatory ranges on algorithm-specific optional parameters that could not be fixed.
- Authentication data comparison criteria for this algorithm. Note: There is a default method for verifying the authentication data specified in the AH protocol document. This is only needed if the default cannot be used (e.g. when using a signed hash).

5. Security Considerations

This document provides a roadmap and guidelines for writing Encryption and Authentication Algorithm documents. The reader should follow all the security procedures and guidelines described in the IPsec Architecture, ESP Protocol, AH Protocol, Encryption Algorithm, and Authentication Algorithm documents. Note that many encryption algorithms are not considered secure if they are not used with some sort of authentication mechanism.

6. Acknowledgments

Several Internet drafts were referenced in writing this document. Depending on where the documents are on (or off) the IETF standards track these may not be available through the IETF RFC repositories. In certain cases the reader may want to know what version of these documents were referenced. These documents are:

- DES-Detroit: this is the ANX Workshop style of ESP, based on the Hughes draft as modified by Cheryl Madson and published on the ANX mailing list.
- DOI: draft-ietf-ipsec-ipsec-doi-02.txt.
- 3DES: this is <the Triple-DES shim document>.
- CAST: this is draft-ietf-ipsec-esp-cast-128-cbc-00.txt, as revised to relate to this document.
- ESP: draft-ietf-ipsec-esp-04.txt, mailed to the IETF mailing list in May/June 1997.
- AH: draft-ietf-ipsec-auth-05.txt, mailed to the IETF mailing list in May/June 1997.

. HUGHES: this is draft-ietf-ipsec-esp-des-md5-03.txt
. ISAKMP: There are three documents describing ISAKMP. These are draft-ietf-ipsec-isakmp-07.txt, draft-ietf-ipsec-isakmp-oakley-03.txt, and draft-ietf-ipsec-ipsec-doi-02.txt.

7. References

[CBC] Periera, R., and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[Arch] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[DES-Detroit] Madson, C., and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm With Explicit IV", RFC 2405, November 1998.

[DOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[AH] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[ESP] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[HMAC] Krawczyk, K., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[HMAC-MD5] Madson, C., and R. Glenn, "The Use of HMAC-MD5 within ESP and AH", RFC 2403, November 1998.

[HMAC-SHA-1] Madson, C., and R. Glenn, "The Use of HMAC-SHA-1 within ESP and AH", RFC 2404, November 1998.

[RANDOM] Eastlake, D., Crocker, S., and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[RFC-2202] Cheng, P., and R. Glenn, "Test Cases for HMAC-MD5 and HMAC-SHA-1", RFC 2202, March 1997.

8. Authors' Addresses

Rodney Thayer
Sable Technology Corporation
246 Walnut Street
Newton, Massachusetts 02160

EMail: mailto:rodney@sabletech.com

Naganand Doraswamy
Bay Networks

EMail: naganand@baynetworks.com

Rob Glenn
NIST

EMail: rob.glenn@nist.gov

9. Full Copyright Statement