Internet Engineering Task Force (IETF)
Request for Comments: 7146
Updates: 3720, 3723, 3821, 3822, 4018, 4172,
4173, 4174, 5040, 5041, 5042, 5043,
5044, 5045, 5046, 5047, 5048
Category: Standards Track
ISSN: 2070-1721

D. Black
EMC
P. Koning
Dell

April 2014

Securing Block Storage Protocols over IP: RFC 3723 Requirements Update for IPsec v3

Abstract

RFC 3723 specifies IPsec requirements for block storage protocols over IP (e.g., Internet Small Computer System Interface (iSCSI)) based on IPsec v2 (RFC 2401 and related RFCs); those requirements have subsequently been applied to remote direct data placement protocols, e.g., the Remote Direct Memory Access Protocol (RDMAP). This document updates RFC 3723's IPsec requirements to IPsec v3 (RFC 4301 and related RFCs) and makes some changes to required algorithms based on developments in cryptography since RFC 3723 was published.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7146.

Table of Contents

1. Introduction

[RFC3723] specifies IPsec requirements for block storage protocols over IP (e.g., iSCSI [RFC3720]) based on IPsec v2 ([RFC2401] and related RFCs); those requirements have subsequently been applied to remote direct data placement protocols, e.g., RDMAP [RFC5040]. This document updates RFC 3723's IPsec requirements to IPsec v3 ([RFC4301] and related RFCs) to reflect developments since RFC 3723 was published.

For brevity, this document uses the term "block storage protocols" to refer to all protocols to which RFC 3723's requirements apply; see Section 1.3 for details.

In addition to the IPsec v2 requirements in RFC 3723, IPsec v3, as specified in [RFC4301] and related RFCs (e.g., IKEv2 [RFC5996]), SHOULD be implemented for block storage protocols. Retention of the mandatory requirement for IPsec v2 provides interoperability with existing implementations, and the strong recommendation for IPsec v3 encourages implementers to move forward to that newer version of IPsec.

Cryptographic developments since the publication of RFC 3723 necessitate changes to the encryption transform requirements for IPsec v2, as explained further in Section 2.2; these updated requirements also apply to IPsec v3.

Block storage protocols can be expected to operate at high data rates (multiple gigabits/second). The cryptographic requirements in this document are strongly influenced by that expectation; an important example is that Triple Data Encryption Standard Cipher Block Chaining (3DES CBC) is no longer recommended for block storage protocols due to the frequent rekeying impacts of 3DES's 64-bit block size at high data rates.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2. Summary of Changes to RFC 3723

This document makes the following changes to RFC 3723:

- Adds requirements that IPsec v3 SHOULD be implemented (Encapsulating Security Payload (ESPv3) and IKEv2) in addition to IPsec v2 (see Section 1).
- Requires extended sequence numbers for both ESPv2 and ESPv3 (see Section 2).
- Clarifies key-size requirements for AES CBC MAC with XCBC extensions (MUST implement 128-bit keys; see Section 2.1).
- Adds IPsec v3 requirements for AES Galois Message Authentication Code (GMAC) and Galois/Counter Mode (GCM) (SHOULD implement when IKEv2 is supported; see Sections 2.1 and 2.2).
- Removes implementation requirements for 3DES CBC and AES in Counter mode (AES CTR) (changes requirements for both to "MAY implement"). Adds a "MUST implement" requirement for AES CBC (see Section 2.2).
- Adds specific IKEv2 implementation requirements (see Section 3).
- Removes the requirement that IKEv1 use UDP port 500 (see Section 3).
- Allows the use of the Online Certificate Status Protocol (OCSP) in addition to Certificate Revocation Lists (CRLs) to check certificates, and changes the Diffie-Hellman group size recommendation to a minimum of 2048 bits (see Section 3).

1.3. Other Updated RFCs

RFC 3723's IPsec requirements have been applied to a number of protocols. For that reason, in addition to updating RFC 3723's IPsec requirements, this document also updates the IPsec requirements for each protocol that uses RFC 3723; that is, the following RFCs are updated -- in each case, the update is solely to the IPsec requirements:

- [RFC3720] "Internet Small Computer Systems Interface (iSCSI)"
- [RFC3821] "Fibre Channel Over TCP/IP (FCIP)"
- [RFC3822] "Finding Fibre Channel over TCP/IP (FCIP) Entities Using Service Location Protocol version 2 (SLPv2)"

- [RFC4018] "Finding Internet Small Computer Systems Interface (iSCSI) Targets and Name Servers by Using Service Location Protocol version 2 (SLPv2)"

- [RFC4172] "iFCP - A Protocol for Internet Fibre Channel Storage Networking"

- [RFC4173] "Bootstrapping Clients using the Internet Small Computer System Interface (iSCSI) Protocol"

- [RFC4174] "The IPv4 Dynamic Host Configuration Protocol (DHCP) Option for the Internet Storage Name Service"

- [RFC5040] "A Remote Direct Memory Access Protocol Specification"

- [RFC5041] "Direct Data Placement over Reliable Transports"

- [RFC5042] "Direct Data Placement Protocol (DDP) / Remote Direct Memory Access Protocol (RDMAP) Security"

- [RFC5043] "Stream Control Transmission Protocol (SCTP) Direct Data Placement (DDP) Adaptation"

- [RFC5044] "Marker PDU Aligned Framing for TCP Specification"

- [RFC5045] "Applicability of Remote Direct Memory Access Protocol (RDMA) and Direct Data Placement (DDP)"

- [RFC5046] "Internet Small Computer System Interface (iSCSI) Extensions for Remote Direct Memory Access (RDMA)"

- [RFC5047] "DA: Datamover Architecture for the Internet Small Computer System Interface (iSCSI)"

- [RFC5048] "Internet Small Computer System Interface (iSCSI) Corrections and Clarifications"

[RFC3721] and [RFC5387] are not updated by this document, as their usage of RFC 3723 does not encompass its IPsec requirements.

In addition, this document's updated IPsec requirements apply to the new specifications for iSCSI [RFC7143] and iSCSI Extensions for RDMA (iSER) [RFC7145].

This document uses the term "block storage protocols" to refer to the protocols (listed above) to which RFC 3723's requirements (as updated by the requirements in this document) apply.

2. ESP Requirements

RFC 3723 requires that implementations MUST support IPsec ESPv2 [RFC2406] in tunnel mode as part of IPsec v2 to provide security for both control packets and data packets; and that when ESPv2 is utilized, per-packet data origin authentication, integrity, and replay protection MUST be provided.

This document modifies RFC 3723 to require that implementations SHOULD also support IPsec ESPv3 [RFC4303] in tunnel mode as part of IPsec v3 to provide security for both control packets and data packets; per-packet data origin authentication, integrity, and replay protection MUST be provided when ESPv3 is utilized.

At the high speeds at which block storage protocols are expected to operate, a single IPsec security association (SA) could rapidly exhaust the ESP 32-bit sequence number space, requiring frequent rekeying of the SA, as rollover of the ESP sequence number within a single SA is prohibited for both ESPv2 [RFC2406] and ESPv3 [RFC4303]. In order to provide the means to avoid this potentially undesirable frequent rekeying, implementations that are capable of operating at speeds of 1 gigabit/second or higher MUST implement extended (64-bit) sequence numbers for ESPv2 (and ESPv3, if supported) and SHOULD use extended sequence numbers for all block storage protocol traffic. Extended sequence number negotiation as part of security association establishment is specified in [RFC4304] for IKEv1 and [RFC5996] for IKEv2.

2.1. Data Origin Authentication and Data Integrity Transforms

RFC 3723 requires that:

- HMAC-SHA1 MUST be implemented in the form of HMAC-SHA-1-96 [RFC2404].

- AES CBC MAC with XCBC extensions SHOULD be implemented [RFC3566].

This document clarifies RFC 3723's key-size requirements for implementations of AES CBC MAC with XCBC extensions; 128-bit keys MUST be supported, and other key sizes MAY also be supported.

This document also adds a requirement for IPsec v3:

- Implementations that support IKEv2 [RFC5996] SHOULD also implement AES GMAC [RFC4543]. AES GMAC implementations MUST support 128-bit keys and MAY support other key sizes.

The rationale for the added requirement is that GMAC is more amenable to hardware implementations that may be preferable for the high data rates at which block storage protocols can be expected to operate.

2.2. Confidentiality Transform Requirements

RFC 3723 requires that:

- 3DES in CBC mode (3DES CBC) [RFC2451] [triple-des-spec] MUST be supported.
- AES in Counter mode (AES CTR) [RFC3686] SHOULD be supported.
- NULL encryption [RFC2410] MUST be supported.

The above requirements from RFC 3723 regarding 3DES CBC and AES CTR are replaced in this document by requirements that both 3DES CBC and AES CTR MAY be implemented. The NULL encryption requirement is not changed by this document. The 3DES CBC requirement matched the basic encryption interoperability requirement for IPsec v2. At the time of RFC 3723's publication, AES in Counter mode was the encryption transform that was most amenable to hardware implementation, as hardware implementation may be preferable for the high data rates at which block storage protocols can be expected to operate. This document changes both of these requirements, based on cryptographic developments since the publication of RFC 3723.

The requirement for 3DES CBC has become problematic due to 3DES's 64-bit block size; i.e., the core cipher encrypts or decrypts 64 bits at a time. Security weaknesses in encryption start to appear as the amount of data encrypted under a single key approaches the birthday bound of 32 GiB (gibibytes) for a cipher with a 64-bit block size; see Appendix A and [triple-des-birthday]. It is prudent to rekey well before that bound is reached, and 32 GiB or some significant fraction thereof is less than the amount of data that a block storage protocol may transfer in a single session. This may require frequent rekeying, e.g., to obtain an order-of-magnitude (10x) safety margin by rekeying after 3 GiB on a multi-gigabit/sec link. In contrast, AES has a 128-bit block size, which results in a much larger birthday bound (2^68 bytes); see Appendix A. AES CBC [RFC3602] is the primary mandatory-to-implement encryption transform for interoperability and hence is the appropriate mandatory-to-implement transform replacement for 3DES CBC.

AES in Counter mode (AES CTR) is no longer the encryption transform that is most amenable to hardware implementation. That characterization now applies to AES GCM [RFC4106], which provides both encryption and integrity protection in a single cryptographic

mechanism (in contrast, neither HMAC-SHA1 nor AES CBC MAC with XCBC extensions is well suited for hardware implementation, as both transforms do not pipeline well). AES GCM is also capable of providing confidentiality protection for the IKEv2 key exchange protocol, but not the IKEv1 protocol [RFC5282], and therefore the new AES GCM "SHOULD" requirement is based on the presence of support for IKEv2.

For the reasons described in the preceding paragraphs, the confidentiality transform requirements in RFC 3723 are replaced by the following:

- 3DES in CBC mode MAY be implemented (replaces RFC 3723's "MUST implement" requirement).
- AES in Counter mode (AES CTR) MAY be implemented (replaces RFC 3723's "SHOULD implement" requirement).
- AES in CBC mode MUST be implemented. AES CBC implementations MUST support 128-bit keys and MAY support other key sizes.
- Implementations that support IKEv2 SHOULD also implement AES GCM. AES GCM implementations MUST support 128-bit keys and MAY support other key sizes.
- NULL encryption [RFC2410] MUST be supported.

The requirement for support of NULL encryption enables the use of SAs that provide data origin authentication and data integrity, but not confidentiality.

Other transforms MAY be implemented in addition to those listed above.

3. IKEv1 and IKEv2 Requirements

Note: To avoid ambiguity, the original IKE protocol [RFC2409] is referred to as "IKEv1" in this document.

This document adds requirements for IKEv2 usage with block storage protocols and makes the following two changes to the IKEv1 requirements in RFC 3723 (the new Diffie-Hellman (DH) group requirement also applies to IKEv2):

- When DH groups are used, a DH group of at least 2048 bits SHOULD be offered as a part of all proposals to create IPsec security associations. The recommendation for the use of 1024-bit DH

groups with 3DES CBC and HMAC-SHA1 has been removed; the use of 1024-bit DH groups is NOT RECOMMENDED, and

- The requirement to use UDP port 500 is removed in order to allow NAT traversal [RFC3947].

There are no other changes to RFC 3723's IKEv1 requirements, but many of them are restated in this document in order to provide context for the new IKEv2 requirements.

RFC 3723 requires that IKEv1 [RFC2409] be supported for peer authentication, negotiation of security associations, and key management, using the IPsec domain of interpretation (DOI) [RFC2407], and further requires that manual keying not be used since it does not provide the rekeying support necessary for operation at high data rates. This document adds a requirement that IKEv2 [RFC5996] SHOULD be supported for peer authentication, negotiation of security associations, and key management. The prohibition of manual keying as stated in RFC 3723 is extended to IKEv2; manual keying MUST NOT be used with any version of IPsec for protocols to which the requirements in this document apply.

RFC 3723's requirements for IKEv1 mode implementation and usage are unchanged; this document does not extend those requirements to IKEv2 because IKEv2 does not have modes.

When IPsec is used, the receipt of an IKEv1 Phase 2 delete message or an IKEv2 INFORMATIONAL exchange that deletes the SA SHOULD NOT be interpreted as a reason for tearing down the block storage protocol connection (e.g., TCP-based). If additional traffic is sent, a new SA will be created to protect that traffic.

The method used to determine whether a block storage protocol connection should be established using IPsec is regarded as an issue of IPsec policy administration and thus is not defined in this document. The method used by an implementation that supports both IPsec v2 and v3 to determine which versions of IPsec are supported by a block storage protocol peer is also regarded as an issue of IPsec policy administration and thus is also not defined in this document. If both IPsec v2 and v3 are supported by both endpoints of a block storage protocol connection, the use of IPsec v3 is RECOMMENDED.

3.1. Authentication Requirements

The authentication requirements for IKEv1 are unchanged by this document but are restated here for context, along with the authentication requirements for IKEv2:

a. Peer authentication using a pre-shared cryptographic key MUST be supported. Certificate-based peer authentication using digital signatures MAY be supported. For IKEv1 [RFC2409], peer authentication using the public key encryption methods specified in Sections 5.2 and 5.3 of [RFC2409] SHOULD NOT be used.

b. When digital signatures are used for authentication, all IKEv1 and IKEv2 negotiators SHOULD use Certificate Request Payload(s) to specify the certificate authority and SHOULD check the certificate validity via the pertinent Certificate Revocation List (CRL) or the use of the Online Certificate Status Protocol (OCSP) [RFC6960] before accepting a PKI certificate for use in authentication. OCSP support within the IKEv2 protocol is specified in [RFC4806].

c. IKEv1 implementations MUST support Main Mode and SHOULD support Aggressive Mode. Main Mode with the pre-shared key authentication method SHOULD NOT be used when either the initiator or the target uses dynamically assigned IP addresses. While in many cases pre-shared keys offer good security, situations in which dynamically assigned addresses are used force the use of a group pre-shared key, which creates vulnerability to a man-in-the-middle attack. These requirements do not apply to IKEv2 because it has no modes.

d. In the IKEv1 Phase 2 Quick Mode, in exchanges for creating the Phase 2 SA, the Identification Payload MUST be present. This requirement does not apply to IKEv2 because it has no modes.

e. The following identification type requirements apply to IKEv1. ID_IPV4_ADDR, ID_IPV6_ADDR (if the protocol stack supports IPv6), and ID_FQDN Identification Types MUST be supported; ID_USER_FQDN SHOULD be supported. The IP Subnet, IP Address Range, ID_DER_ASN1_DN, and ID_DER_ASN1_GN Identification Types SHOULD NOT be used. The ID_KEY_ID Identification Type MUST NOT be used.

f. When IKEv2 is supported, the following identification requirements apply. ID_IPV4_ADDR, ID_IPV6_ADDR (if the protocol stack supports IPv6), and ID_FQDN Identification Types MUST be supported; ID_RFC822_ADDR SHOULD be supported. The ID_DER_ASN1_DN and ID_DER_ASN1_GN Identification Types SHOULD NOT be used. The ID_KEY_ID Identification Type MUST NOT be used.

The reasons for the identification requirements in items e and f above are as follows:

- IP Subnet and IP Address Range are too broad to usefully identify an iSCSI endpoint.
- The _DN and _GN types are X.500 identities; it is usually better to use an identity from subjectAltName in a PKI certificate.
- ID_KEY_ID is an opaque identifier that is not interoperable among different IPsec implementations as specified. Heterogeneity in some block storage protocol implementations can be expected (e.g., iSCSI initiator vs. iSCSI target implementations), and hence heterogeneity among IPsec implementations is important.

3.2. DH Group and PRF Requirements

This document does not change the support requirements for Diffie-Hellman (DH) groups and Pseudo-Random Functions (PRFs). See [RFC4109] for IKEv1 requirements and [RFC4307] for IKEv2 requirements. Implementers are advised to check for subsequent RFCs that update either of these RFCs, as such updates may change these requirements.

When DH groups are used, a DH group of at least 2048 bits SHOULD be offered as a part of all proposals to create IPsec security associations for both IKEv1 and IKEv2.

RFC 3723 requires that support for perfect forward secrecy in the IKEv1 Quick Mode key exchange MUST be implemented. This document extends that requirement to IKEv2; support for perfect forward secrecy in the CREATE_CHILD_SA key exchange MUST be implemented for the use of IPsec with block storage protocols.

4. Security Considerations

This entire document is about security.

The security considerations sections of all of the referenced RFCs apply, and particular note should be taken of the security considerations for the encryption transforms whose requirement levels are changed by this RFC:

- AES GMAC [RFC4543] (new requirement -- SHOULD be supported when IKEv2 is supported),
- 3DES CBC [RFC2451] (changed from "MUST be supported" to "MAY be supported"),

- AES CTR [RFC3686] (changed from "SHOULD be supported" to "MAY be supported"),
- AES CBC [RFC3602] (new requirement -- MUST be supported), and
- AES GCM [RFC4106] (new requirement -- SHOULD be supported when IKEv2 is supported).

Of particular interest are the security considerations concerning the use of AES GCM [RFC4106] and AES GMAC [RFC4543]; both modes are vulnerable to catastrophic forgery attacks if a nonce is ever repeated with a given key.

The requirement level for 3DES CBC has been reduced, based on considerations for high-speed implementations; 3DES CBC remains an optional encryption transform that may be suitable for implementations limited to operating at lower speeds where the required rekeying frequency for 3DES is acceptable.

The requirement level for AES CTR has been reduced, based solely on hardware implementation considerations that favor AES GCM, as opposed to changes in AES CTR's security properties. AES CTR remains an optional security transform that is suitable for use in general, as it does not share 3DES CBC's requirement for frequent rekeying when operating at high data rates.

Key sizes with comparable strength SHOULD be used for the cryptographic algorithms and transforms for any individual IPsec security association. See Section 5.6 of [SP800-57] for further discussion.

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2404] Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.

[RFC2406] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC2410] Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

[RFC2451] Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.

[RFC3566] Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.

[RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

[RFC3720] Satran, J., Meth, K., Sapuntzakis, C., Chadalapaka, M., and E. Zeidner, "Internet Small Computer Systems Interface (iSCSI)", RFC 3720, April 2004.

[RFC3723] Aboba, B., Tseng, J., Walker, J., Rangan, V., and F. Travostino, "Securing Block Storage Protocols over IP", RFC 3723, April 2004.

[RFC3821] Rajagopal, M., Rodriguez, E., and R. Weber, "Fibre Channel Over TCP/IP (FCIP)", RFC 3821, July 2004.

[RFC3822] Peterson, D., "Finding Fibre Channel over TCP/IP (FCIP) Entities Using Service Location Protocol version 2 (SLPv2)", RFC 3822, July 2004.

[RFC3947] Kivinen, T., Swander, B., Huttunen, A., and V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

[RFC4018] Bakke, M., Hufferd, J., Voruganti, K., Krueger, M., and T. Sperry, "Finding Internet Small Computer Systems Interface (iSCSI) Targets and Name Servers by Using Service Location Protocol version 2 (SLPv2)", RFC 4018, April 2005.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, June 2005.

[RFC4109] Hoffman, P., "Algorithms for Internet Key Exchange version 1 (IKEv1)", RFC 4109, May 2005.

[RFC4172] Monia, C., Mullendore, R., Travostino, F., Jeong, W., and M. Edwards, "iFCP - A Protocol for Internet Fibre Channel Storage Networking", RFC 4172, September 2005.

[RFC4173] Sarkar, P., Missimer, D., and C. Sapuntzakis, "Bootstrapping Clients using the Internet Small Computer System Interface (iSCSI) Protocol", RFC 4173, September 2005.

[RFC4174] Monia, C., Tseng, J., and K. Gibbons, "The IPv4 Dynamic Host Configuration Protocol (DHCP) Option for the Internet Storage Name Service", RFC 4174, September 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4304] Kent, S., "Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)", RFC 4304, December 2005.

[RFC4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.

[RFC4543] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.

[RFC5040] Recio, R., Metzler, B., Culley, P., Hilland, J., and D. Garcia, "A Remote Direct Memory Access Protocol Specification", RFC 5040, October 2007.

[RFC5041] Shah, H., Pinkerton, J., Recio, R., and P. Culley, "Direct Data Placement over Reliable Transports", RFC 5041, October 2007.

[RFC5042] Pinkerton, J. and E. Deleganes, "Direct Data Placement Protocol (DDP) / Remote Direct Memory Access Protocol (RDMAP) Security", RFC 5042, October 2007.

[RFC5043] Bestler, C. and R. Stewart, "Stream Control Transmission Protocol (SCTP) Direct Data Placement (DDP) Adaptation", RFC 5043, October 2007.

[RFC5044] Culley, P., Elzur, U., Recio, R., Bailey, S., and J. Carrier, "Marker PDU Aligned Framing for TCP Specification", RFC 5044, October 2007.

[RFC5046] Ko, M., Chadalapaka, M., Hufferd, J., Elzur, U., Shah, H., and P. Thaler, "Internet Small Computer System Interface (iSCSI) Extensions for Remote Direct Memory Access (RDMA)", RFC 5046, October 2007.

[RFC5048] Chadalapaka, M., "Internet Small Computer System Interface (iSCSI) Corrections and Clarifications", RFC 5048, October 2007.

[RFC5282] Black, D. and D. McGrew, "Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol", RFC 5282, August 2008.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, June 2013.

[RFC7143] Chadalapaka, M., Satran, J., Meth, K., and D. Black, "Internet Small Computer System Interface (iSCSI) Protocol (Consolidated)", RFC 7143, April 2014.

[RFC7145] Ko, M. and A. Nezhinsky, "Internet Small Computer System Interface (iSCSI) Extensions for the Remote Direct Memory Access (RDMA) Specification", RFC 7145, April 2014.

[SP800-57] Barker, E., Barker, W., Burr, W., Polk, W., and M. Smid, "NIST Special Publication 800-57: Recommendation for Key Management - Part 1: General (Revision 3)", July 2012, <http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf>.

[triple-des-birthday]
McGrew, D., "Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes (Cryptology ePrint Archive: Report 2012/623)", November 2012, <http://eprint.iacr.org/2012/623>.

[triple-des-spec]
American Bankers Association (ABA), "American National Standard for Financial Services X9.52-1998 - Triple Data Encryption Algorithm Modes of Operation", July 1998.

5.2. Informative References

[RFC3721] Bakke, M., Hafner, J., Hufferd, J., Voruganti, K., and M. Krueger, "Internet Small Computer Systems Interface (iSCSI) Naming and Discovery", RFC 3721, April 2004.

[RFC4806] Myers, M. and H. Tschofenig, "Online Certificate Status Protocol (OCSP) Extensions to IKEv2", RFC 4806, February 2007.

[RFC5045] Bestler, C. and L. Coene, "Applicability of Remote Direct Memory Access Protocol (RDMA) and Direct Data Placement (DDP)", RFC 5045, October 2007.

[RFC5047] Chadalapaka, M., Hufferd, J., Satran, J., and H. Shah, "DA: Datamover Architecture for the Internet Small Computer System Interface (iSCSI)", RFC 5047, October 2007.

[RFC5387] Touch, J., Black, D., and Y. Wang, "Problem and Applicability Statement for Better-Than-Nothing Security (BTNS)", RFC 5387, November 2008.

Appendix A. Block Cipher Birthday Bounds

This appendix provides the birthday bounds for the 3DES and AES ciphers based on [triple-des-birthday], which states: "Theory advises against using a w-bit block cipher to encrypt more than 2^(w/2) blocks with a single key; this is known as the birthday bound".

For a cipher with a 64-bit block size (e.g., 3DES), w = 64, so the birthday bound is 2^32 blocks. As each block contains 8 (2^3) bytes, the birthday bound is 2^35 bytes = 2^5 gibibytes, i.e., 32 GiB, where 1 gibibyte (GiB) = 2^30 bytes. Note that a gigabyte (decimal quantity) is not the same as a gibibyte (binary quantity); 1 gigabyte (GB) = 10^6 bytes.

For a cipher with a 128-bit block size (e.g., AES), w = 128, so the birthday bound is 2^64 blocks. As each block contains 16 (2^4) bytes, the birthday bound is 2^68 bytes = 2^8 exbibytes, i.e., 256 EiB, where 1 exbibyte (EiB) = 2^60 bytes. Note that an exabyte (decimal quantity) is not the same as an exbibyte (binary quantity); 1 exabyte (EB) = 10^9 bytes.

Appendix B. Contributors

David McGrew’s observations about the birthday bound implications of 3DES’s 64-bit block size on the ipsec@ietf.org mailing list led to changing from 3DES CBC to AES CBC as the mandatory-to-implement encryption algorithm, based on the birthday bound discussion in Appendix A.

The original authors of RFC 3723 were Bernard Aboba, Joshua Tseng, Jesse Walker, Venkat Rangan, and Franco Travostino. Comments from Francis Dupont, Yaron Sheffer, Tom Talpey, Sean Turner, and Tom Yu have improved this document and are gratefully acknowledged.

Authors' Addresses

David L. Black
EMC Corporation
176 South St.
Hopkinton, MA 01748
USA

Phone: +1 508 293-7953
EMail: david.black@emc.com

Paul Koning
Dell
300 Innovative Way
Nashua, NH 03062
USA

Phone: +1 603 249-7703
EMail: paul_koning@Dell.com