Network Working Group D. McGrew
Internet-Draft A. Grieco
Intended status: Experimental Cisco
Expires: July 29, 2013 Y. Sheffer
Porticor
January 25, 2013

Selection of Future Cryptographic Standards
draft-mcgrew-standby-cipher-00

Abstract

The Advanced Encryption Standard (AES) is extensively used and is widely believed to provide security that is more than adequate. Several other cipher designs have been proposed for use in standards, and new designs continue to be developed, while consideration of cost and complexity impels that the number of mandatory-to-implement ciphers be minimized. This note outlines an approach to the selection of cryptographic algorithms that best serves the needs of the users of cryptography: AES should continue in its role as the mandatory-to-implement cipher, while other cipher designs should be reviewed with the goal of selecting a single standby cipher. If future advances in the science of cryptanalysis uncover security issues with the AES, the standby cipher will be ready for adoption as its replacement.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

1.1. Requirements Language

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

2. Background

The modern cryptography industry relies on peer-reviewed algorithms and protocols. The robustness of a cryptographic algorithm can only be established after experts have reviewed it and no weakness in the algorithm has been found. Many advanced techniques have been developed for designing algorithms and analyzing their security.

The reliance that the cryptographic industry has on expert review has caused it to put a premium value on open publication, open peer review, and open standards. The process that selected the Advanced Encryption Standard (AES, [FIPS-197]), was open and transparent. Fifteen submissions were accepted from around the world (though the process was managed by the National Institute of Standards and Technology (NIST) of the United States), and their security and efficiency was widely analyzed and discussed at three public workshops and other peer- reviewed venues over the course of four years, before the Belgian submission was selected. The caution, thoroughness, and openness of the selection process inspired confidence on the part of standards organizations, and the AES cipher was adopted by many international standards, including those in the IETF and the IEEE.

Standards organizations are free to select the cryptographic algorithms that meet their requirements for security and efficiency. Currently, AES is the most commonly used cipher, because of the confidence that the industry has in its design and because its wide use ensures wide availability of implementations. The Triple Data Encryption Standard (3DES) is a legacy algorithm that is still in use, as is the RC4 stream cipher.

3. The (Over)abundance of Ciphers

> The nice thing about standards is that there are so many of them to choose from. - Andrew S. Tanenbaum

Several other ciphers have been proposed for use in IETF protocols in recent years, including SEED, ARIA, Camellia, CLEFIA and GOST. In

some other instances, new ciphers have been introduced as unpublished extensions to IETF standards (as was originally the case with ARIA) or as part of new, non-standard protocols (such as WAPI). These ciphers, as well as other ones, have been proposed in other contexts, such as ISO/IEC JTC 1/SC 27 Working Group on Cryptography and Security Mechanisms, the Japanese Cryptography Research and Evaluation Committees (CRYPTREC), and the European Network of Excellence in Cryptology (ECRYPT) II project. The availability of so many cipher designs that appear to have adequate security is encouraging. However, it would be counterproductive to require or urge that every implementation of security protocols such as IPsec or TLS include multiple new ciphers. That would increase the cost and complexity of those protocols while contributing little benefit to the Internet community.

Each additional cipher that an implementation supports will increase the cost of its development, testing, and validation. Implementations that use hardware to achieve scalability and throughput will require additional circuits for each cipher. Additionally, architectures deployed today rely on more than just two endpoints having the same cipher support. Instead, they involve ecosystems of capabilities to deliver secured communications. For example, devices such as load balancers, authentication servers, etc. are all required to support large scale deployments of services in many architectures, and these devices would be required to implement all possible ciphers. Finally, if a multiplicity of ciphers is used in practice, it will drive up operational costs as well, because the policy that determines when the new cipher must be used will need to be put into effect.

4. Algorithm Agility and Security Policies

Standard cryptographic protocols, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec), include functionality that allows two endpoints to dynamically negotiate the algorithms that are used in a particular session. This feature is called algorithm agility, and it is important because it enables a new algorithm to be easily introduced in a protocol, while preserving interoperability between devices that support the new algorithm and ones that do not. Algorithm agility is crucial to security because it allows for the replacement of algorithms that are found to have cryptographic weaknesses.

The algorithm negotiation capability can also be used to allow implementations to support multiple algorithms, and dynamically decide which algorithms to use. In principle, it is possible to have different devices each support different sets of algorithms, as long

as each pair of sets is overlapping. However, it is highly desirable to minimize the number of algorithms that must be supported by an implementation, because of the complexity and administrative burden of managing the policy associated with a multitude of algorithms. Because of these factors, most standards choose to mandate only a single algorithm that must be implemented by all devices, despite the availability of a negotiation mechanism. In addition, cryptographic negotiation also establishes other algorithms and parameters to be used, such as key establishment, authentication, pseudorandom functions, and key sizes.

Algorithm agility also allows the use of ciphers other than the mandatory-to-implement cipher within specialized communities of interest. This is a valid use of that capability, but it should be noted, however, that there is complexity and cost in the use of elaborate security policies. If a community of interest requires that a particular cipher be used within that community, but allows the use of other ciphers when devices from that community communicate outside that community, it will need to put this policy into practice on all devices within the community. This process will not be trivial or easy to execute; there will need to be a mechanism by which devices in the community can identify whether or not a communicant is also inside the community. The situation is simpler when a cipher is used only within a community of interest, and the devices in that community are used to communicate only with other devices in the same community. In this case, there is no need for a mechanism that determines which other devices are also in the community; each device in the community can be configured to only use the favored cipher.

5. Cryptographic Protocols

The IETF should allow the use of specialized algorithms within the cryptographic protocol standards that it defines. To do otherwise could encourage the proliferation of protocol standards, which is a worse situation than the proliferation of cipher standards. It is highly desirable to limit the number of cryptographic protocols. It is much harder to replace a protocol, or to support multiple protocols, as opposed to replacing a cryptographic algorithm. An algorithm may have high complexity, but the complexity is well isolated through a simple interface. In contrast, the complexity of a protocol is not at all isolated; it touches the protocol layers above and below it, and an efficient protocol implementation will closely interact with the system on which it runs.

It is far better to add a new feature or algorithm to an existing cryptographic protocol than to introduce an entirely new protocol.

By way of example, the TLS protocol was extended so that it can protect UDP traffic as well as TCP traffic, resulting in the Datagram TLS (DTLS) protocol. This standards action was widely perceived as being preferable to the introduction of a new protocol that would protected only UDP.

6. A Standby Algorithm

The industry is in the fortunate position that the main requirements for a mandatory global cipher and algorithm agility are met by current standards for communication security protocols. Many additional ciphers have been proposed for use in these standards. It may be useful for the global crypto standards community to seek algorithm diversity by selecting a cipher to be used as a standby or fallback, in case of the possibility that future advances in the science of cryptanalysis might uncover security issues with the current global standard cipher. The implementation of the standby cipher should not be required, but could be recommended for implementation by security protocol standards. In the terms of RFC 2119, the standby algorithm SHOULD be implemented.

The process for the selection of a standby should meet the same Exacting criteria as the global standard cipher, to assure its technical merit. Ideally, a standby cipher should be selected in advance of when it is needed. That cipher should be chosen after extensive public review and analysis, in which time is allowed for significant scientific scrutiny and investigation. The cipher should demonstrate its strength through the publication of attacks that work only against a small number of rounds, since an absence of published attacks may indicate an absence of cryptanalysis instead of an absence of weaknesses. The best cipher designs from around the world should be considered, and analyses should be openly published and widely disseminated. Only a single standby cipher should be recommended, to minimize the cost of implementation and maximize interoperability. To be recommended as a standby, an algorithm should meet all of the criteria set out for the AES:

- security,
- computational efficiency,
- memory requirements,
- hardware and software suitability,
- simplicity,
- flexibility, and
- licensing requirements; in particular, it should be available worldwide on a royalty-free basis.

In addition to the AES requirements, there are requirements that are

particular to a cipher that would serve as a standby to the AES:

- o it should have a design that is as independent of that of the AES as is possible, so that advances in cryptanalysis that lower the effective security of one design have as little effect as possible on the other one, and
- o it should also perform well on existing hardware that is optimized for AES implementation.

The final criterion, performance on existing AES optimized hardware, refers to the consideration for standby algorithm performance when executing in existing hardware today. The goal of this criteria would be to select a cipher that performs well today on existing hardware implementations, many of which have optimized AES implementations. This constraint would provide for a more timely transition to the standby cipher because no new hardware optimization would be needed. However, this criteria is focused on short term deployment and does so at a cost of constraining the design of the standby cipher. A longer term view would remove this criteria and consider all ciphers that are practical to implement without specific consideration to applicability to existing hardware optimization. In doing so, designs considered for the standby cipher would be more flexible and likely positively impact considerations in other criteria categories, but could also increase adoption time. The authors note this inherent conflict associated with this criteria and request the community's opinion about resolution to this issue.

The Triple-DES (TDES) algorithm has a 64-bit block size, and because of this, is not suitable for securing very large volumes of data [coll64bit]. It also is significantly slower in software, and less efficient in hardware. Thus TDES is not a suitable standby cipher. This is an additional motivation for the selection of a new standby algorithm.

6.1. Security Considerations

There is no known weakness in AES that affects its practical security. Biclique cryptanalysis add citation can be used to shave one or two bytes off of the theoretical strength of the cipher, in scenarios in which the attacker can cause the encryption/decryption of 2^88 chosen plaintexts/ciphertexts of its choice. This attack has no relevance on the uses of AES in conventional block cipher modes of operation, in which 2^64 blocks is the accepted maximum number that should be encrypted with any key. There have been related key attacks against AES-192 and AES-256, and suggestions that the key schedule of that algorithm is not as strong as would be desirable. Thus three important criteria for a standby cipher are that there should be an absence of related key attacks against it, there should

be especially high confidence in its 192 and 256 bit variants, and the key schedule should be perceived to be strong. The major goal of a standby cipher is to be secure even if the AES proves vulnerable to future advances in cryptanalysis. Thus, a standby cipher should not follow a design strategy that is identical to that of the AES. Block ciphers with a 64-bit block have a very significantly lower security level than those with a 128-bit block, and thus should be strongly discouraged.

7. Recommendations

The industry and the IETF should encourage the use of existing security protocols, and to this end, the IETF should allow the publication of documents describing the use of ciphers in IETF standards, even when those ciphers have only a small community of interest. This policy was clarified by the Security Area Directors at IETF78, and it should be continued. However, the IETF should explicitly reject the idea that each community of interest gets to have its favored cipher be added to the list of mandatory-to-implement ciphers. It is important to clarify the difference between algorithms that MUST be implemented in a particular protocol from the algorithms that MAY be implemented. We suggest that:

- The IETF and IRTF Crypto Forum Research Group (CFRG) should identify the technical requirements that a standby cipher should meet, and provide this input to the international cryptographic community. This effort will be led by the CFRG, with the goal that the requirement document be published as an RFC no later than XXX months after the current document is published.
- The IETF and IRTF Crypto Forum Research Group (CFRG) should identify the technical requirements that a standby cipher should meet, and provide this input to the international cryptographic community.
- Ideally, the process will result in the IETF-wide selection of a single standby cipher, followed by a lengthy process of individual working groups adopting this choice for their specific protocols. However the CFRG may also reach the unfortunate conclusion that no current algorithm fulfills the requirements.
- The IETF should encourage and support the discussion and analysis of a standby cipher through open and public processes.
- Communities of interest that seek to introduce new ciphers to the industry should be encouraged to participate in international standards and other public processes for discussion, review, analysis, presentation, and dissemination of results.

8. Other Considerations

Above we discussed only symmetric ciphers. Similar considerations apply to hashing, message authentication, signatures, key exchange, and asymmetric encryption. It is highly desirable to limit the number of new cryptographic algorithms that are introduced into standards. The Galois/Counter Mode (GCM) of operation for block ciphers and the Counter and CBC-MAC (CCM) Mode of operation for block ciphers provide both encryption and authentication; they do away with the need to implement a separate message authentication code such as HMAC. This is a strong advantage in the context of limiting the number of algorithms.

It could reasonably be argued that instead of selecting a block cipher, the standards community should be selecting an Authenticated Encryption with Associated Data (AEAD) mechanism [RFC5116]. The cryptographic algorithm design community has identified AEAD as the best paradigm for symmetric cryptography, and there is theoretical interest in the development of new algorithms in this area, as indicated by the recent Directions in Authenticated Ciphers workshop. However, it is not yet clear that such a mechanism could be adopted as easily as a new block cipher.

The hash algorithm contest recently completed by NIST created a selection for SHA-3. SHA-256 remains the standard, mandatory to implement hash algorithm, but SHA-3 could be considered the standby hash algorithm.

9. IANA Considerations

This memo includes no request to IANA.

10. Security Considerations

This note analyzes the considerations in the selection of cryptographic algorithms for future use. The appropriate selection of algorithms is important for security.

11. Acknowledgements

This document was prepared using the lyx2rfc tool, and we would like to thank Nico Williams, its author.

12. References

12.1. Normative References

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

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

12.2. Informative References

[FIPS-197]
National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001.

[coll64bit]
McGrew, D., "Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes", IACR Eprint Archive 2012/623, November 2012, <http://eprint.iacr.org/2012/623.pdf>.

Authors' Addresses

David McGrew
Cisco Systems, Inc.
13600 Dulles Technology Drive
Herndon, VA 20171
USA

Email: mcgrew@cisco.com

Anthony Grieco
Cisco Systems, Inc.
7025 Kit Creek Road
RTP, NC 27709
USA

Email: agrieco@cisco.com

Yaron Sheffer
Porticor
10 Yirmiyahu St.
Ramat HaSharon 47298
Israel

Email: yaronf.ietf@gmail.com