Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 23, 2016

H. Halpin, Ed.
W3C/MIT
G. Steel
Cryptosense/INRIA

November 20, 2015

Security Guidelines for Cryptographic Algorithms in the W3C Web Cryptography API
draft-irtf-cfrg-webcrypto-algorithms-00

Abstract

This overview document provides information on the current state of algorithms made available by the W3C Web Cryptography API, including whether protocols have security proofs or known weaknesses.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 23, 2016.

Copyright Notice

Table of Contents

1. Introduction

While cryptography is a small part of security, choosing the right cryptographic algorithm is an important part of deploying cryptography. Many developers find it difficult to follow the current state of cryptanalytic research regarding particular algorithms. This document gives a concise overview of known weaknesses and the state of security proofs in standard developer-facing APIs such as the W3C Web Cryptography API [W3CWebCryptoLC]. This analysis may also be useful in analyzing the properties of protocols given in the algorithms used by the IETF JSON Web Algorithms [JWA].

This overview provides no substitute for a detailed analysis of a particular protocol: when deploying cryptographic algorithms in Web and Internet applications, developers should strictly follow the instructions given by the cryptographic protocol and avoid creating

new protocols. Developers should also be aware of the intended threat models of the cryptographic protocols they are implementing and note that some aspects of deploying a protocol in the context of an internet application, such as the use of Javascript and the Web, may change some of its security properties. For example, Javascript code is always ultimately controlled by the origin, thus making end-to-end encryption without a trusted origin of the code impossible. Questions about and proposals to improve the Web Security Model should be sent to the W3C Web Security Interest Group at "public-web-security@w3.org"

In this review, we limit ourselves to peer-reviewed results on the algorithms which have been included in the latest public draft of the W3C Crypto API [W3CWebCryptoLC]. Where appropriate we also comment on the status of the algorithm in other standards. Note that this represents a point-in-time snapshot of the state of the art in cryptanalysis and provable security results, which is a complex area subject to (sometimes rapid) change. There is at least one annual publication, the ENISA Algorithms, Key Size and Parameters Report, whose aim is to track these developments [enisa13]. That document discusses a much larger set of algorithms in much greater depth that we do here.

Please discuss this draft on the mailing list "cfrg@ietf.org". Note that draft, while attempting to gather consensus of the cryptographic literature, may not be complete and there may be disagreement, so that readers should view the archives of the CFRG mailing list to be aware of debates and ongoing analysis.

2. Overview

This following table summarizes the results. The marks for legacy and future applications are the same as in the 2013 ENISA report [enisa13], except for those algorithms (PBKDF2 and AES-KW) which are not covered by the report where the marks represent interpretation of the available literature.

Algorithm/Mode	OK Legacy	OK Future	Note
RSAES-PKCS1-v1_5	YES	NO	
RSA-OAEP	YES	YES	
RSASSA-PKCS1-v1_5	YES	NO	No public security proof
RSA-PSS	YES	YES	
ECDSA	YES	YES	Controversy
ECDH	YES	YES	Controvery
AES-CBC	YES	YES	NB not CCA secure
AES-CFB	YES	YES	NB not CCA secure
AES-CTR	YES	YES	NB not CCA secure
AES-GCM	YES	YES	
AES-CMAC	YES	YES	
AES-KW	YES	NO	No public security proof
HMAC	YES	YES	
DH	YES	YES	Only using strong parameters
SHA-1	YES	NO	Known weaknesses (see text)
SHA-256	YES	YES	
SHA-384	YES	YES	
SHA-512	YES	YES	
CONCAT	YES	YES	
HKDF-CTR	YES	YES	
PBKDF2	YES	NO	Known weaknesses (see text))

The Algorithm/Mode is the title by the W3C Web Cryptography API [W3CWebCryptoCR]. Whether or not the protocol is considered secure for legacy use or for future protocols is given next, followed by notes regarding its security properties (such as security proofs).

Table 1: Algorithm Summary Table

3. Conformance Criteria

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].

4. Algorithm Review

In this review, we overview the following algorithms listed in the table. They are all currently given in the W3C Web Cryptography API, although RSAES-PKCS1-v1_5 (present in an earlier version of the Web Cryptography API [W3CWebCryptoLC].) was withdrawn from the W3C Web Cryptography API [W3CWebCryptoCR]. This analysis originates in work done by Graham Steel [SteelChoice]. If algorithms are added, we will attempt to add them to this analysis in due course.

5. RSAES-PKCS1-v1_5

This encryption scheme has been known to be vulnerable to a chosen ciphertext attack (CCA) since 1998 [bleichenbacher98]. The attack has recently been improved to require a median of less than 15,000 chosen ciphertexts on the standard oracle [bardou12padding]. Instances of the attack in widely-deployed real-world systems continue to be found [jager12bleichenbacher].

Since version 2.0 (September 1998), the RSA PKCS#11 standard contains the text: "RSAES-PKCS1-v1_5 is included only for compatibility with existing applications, and is not recommended for new applications" [PKCS11].

TLS up to version 1.2. supports RSAES-PKCS1-v1_5, but using specific countermeasures that 1) substitute a message with a random value in the event of a padding error and 2) require the client to display knowledge of the plaintext before proceeding with the protocol. These countermeasures are not trivially transposable to other applications.

The RSAES-PKCS1-v1_5 scheme was removed from the draft during the Last Call review period of the W3C Web Cryptography API. Despite this, it is still to be found in the Trusted Platform Module (TPM) standard, PKCS#11, Java JCE/JCA, MS-CAPI all support it. TPM 1.2 did not support it, favouring OAEP (below), but it may be included in TPM 2.0 (see section 14.2.1, Level 00 Revision 01.07).

6. RSA-OAEP

Has a security proof of preservation of indistinguishability under chosen ciphertext attacks (IND-CCA, the standard desirable notion of security for an encryption scheme) [fujisaki04OAEP]. Indeed, the proof has been formalised in the Coq proof assistant [barthe2009POPL]. These proofs assume that a well-known implementation pitfall leading to an efficient attack [manger01] is avoided.

Using OAEP implies using a hash function. A recent report recommends using SHA-1 inside OAEP for legacy applications only and using SHA-2/3 for future applications [enisa13].

7. RSASSA-PKCS1-v1_5

There are no publicly known attacks on this scheme. However, there are also no security proofs and no advantages compared to other RSA-based schemes such as PSS (below) [enisa13].

An RSA Laboratories memo by Burt Kaliski, dated February 26 2003, states "'While the traditional and widely deployed PKCS#1 v1.5 signature scheme is still appropriate to use, RSA Laboratories encourages a gradual transition to RSA-PSS as new applications are developed" [email].

8. RSA-PSS

Has a security proof due to Bellare and Rogaway [bellare96eurocrypt] in the random oracle model.

9. ECDSA

ECDSA schemes have some provable security results but only in weak models [enisa13].

10. ECDH

ECDH has provable security results [boneh01crypto] but is subject to attacks due to groups not being well-specified. Like other plain DH modes it offers no authenticity, this must be taken care of separately.

11. AES-CBC, AES-CFB, AES-CTR

There are known cryptanalytic attacks on AES that are not currently believed to pose a practical threat [kaminsky10]. The following results assume that AES is a secure block cipher. Keyed MACS are necessary for use with any AES block cipher in a mode that is not AES-GCM.

AES-CBC mode is not CCA secure. It is secure against chosen plaintext attacks (CPA-secure) if the IV is random, but it is not enough if the IV is a possibly non-random nonce [rogaway11evaluation].

It does not tolerate a padding oracle [vaudenay02] - indeed, in practice, padding oracle attacks are common

[paterson04padding][mitchell05cbc][rizzo10USENIX] and the padding mode suggested in the current draft is exactly that which gives rise to most of these attacks.

AES-CFB is not CCA secure. It is CPA-secure if the IV is random, but not if the IV is a nonce [rogaway11evaluation].

AES-CTR is not CCA secure. It is CPA-secure but not CCA-secure [rogaway11evaluation].

For a summary of the properties of these modes and the dangers of using ciphers with only CPA-security, the following excerpt from Rogaway's review [rogaway11evaluation] is apposite:

"I am unable to think of any cryptographic design problem where, absent major legacy considerations, any of CBC, CFB, or OFB would represent the mode of choice. I regard CTR as easily the "best" choice among the set of the confidentiality modes (meaning the set of schemes aiming only for message privacy, as classically understood). It has unsurpassed performance characteristics and provable-security guarantees that are at least as good as any of the "basic four" modes with respect to classical notions of privacy. The simplicity, efficiency, and obvious correctness of CTR make it a mandatory member in any modern portfolio of SemCPA-secure schemes. The only substantial criticisms of CTR center on its ease of misuse. First, it is imperative that the counter-values that are enciphered are never reused. What is more, these values are 'exposed' to the user of CTR, offering ample opportunity to disregard the instructions. Second, the mode offers absolutely no authenticity, nonmalleability, or chosen-ciphertext-attack (CCA) security. Users of a symmetric scheme who implicitly assume such properties of their confidentiality-providing mode are, with CTR, almost certain to get caught in their error."

12. AES-GCM

GCM mode has a security proof - the security notion is AEAD (Authenticated Encyrption with Associated Data), which (loosely speaking) means that the encryption part is CCA-secure and the message and associated data are unforgeable. There are some cryptanalytic results on certain instantiations of the scheme, those these are not currently thought to pose a practical threat [enisa13].

Standardised by NIST, GCM is gaining traction in standards such as IPsec, MACSec, P1619.1, and TLS [rogaway11evaluation].

13. AES-CMAC

AES-CMAC has good security proofs (i.e. it has well studied proofs with reasonable bounds under standard assumptions) [rogaway11evaluation].

14. AES-KW

AES-KW has received various criticisms, for example being inconsistent in its notions of security (requiring IND-CCA from a deterministic mode) and restrictions on the size of the input data. Although it has no public security proof, it has no known attacks either [rogaway06deterministic]. There are alternative standards with security proofs and less restrictions such as SIV mode (RFC 5297)[RFC5297], but SIV is not currently supported by the WebCrypto API.

15. HMAC

HMAC has well-studied security proofs, even if the underlying hash function is not (weak) collision resistant [bellare06HMAC].

16. DH

The security of Diffie-Hellman key agreement maps closely to the difficulty of the Diffie-Hellman problem. There are known attacks on weak parameters for Diffie-Hellman key agreement [weakdh]. Like other plain DH modes it offers no authenticity, this must be taken care of separately.

17. SHA1

A procedure is known to obtain SHA-1 collisions in less than 2^62 operations [wang2005] (since SHA-1 has a fixed 160 bit output, the theoretical lower bound is 2^80). A talk by Marc Stevens outlines a procedure requiring 2^60 operations [stevens]. Speculation about when practical collisions will be seen ranges from 2018-21 [schneier].

Preimage calculation attacks on reduced round SHA-1 currently require 2^146.2 steps on 44 round SHA-1 and 2^150.6 steps on 48 round (full SHA-1 has 80 rounds) and Simon Knellwolf, who worked on these latest attacks, notes that given the current rate of progress, efficient preimage attacks will be seen in 2020 [knellwolf12].

Finally, some authors consider even the theoretical lower bound on collision attacks (2^80) to be too low a security parameter for future applications [enisa13].

18. SHA-256, SHA-384, SHA-512

There are collision and preimage attacks reported on reduced-round versions of the SHA-2 family, but currently no practical attacks [enisa13].

19. HKDF-CTR

Security models for password-based key derivation functions are still in a state of flux [wen12framework]. However, we note that HKDF has security proofs [krawczyk10HKDF].

20. PBKDF2

PBKDF2 has known weaknesses [yao05kdf] and @@ minimum iterations should be used.

21. CONCAT

CONCAT (which refers to the key derivation function defined in Section 5.8.1 of NIST SP 800-56A) does not appear to have any independent analysis, but is simple and receives approval in the ENISA report [enisa13].

22. Security Considerations

This informational overview lists some well-known security considerations for algorithms in the W3C Web Cryptographic API. We expect these algorithms to be used in particular applications with a wide variety of differing threat models for various attacks. Thus, the attacks in-scope and out-of-scope depend on the particular protocol, as well as the attacks a protocol is susceptible to and those which it protects against. This note documents per algorithm known attacks that are generic to an algorithm, but does not deal with the particular level.

23. IANA Considerations

This memo includes no request to IANA. For the algorithms inspected in this review, the central authority governing their identifiers is the W3C Web Cryptography Working API [W3CWebCryptoCR]. Note that the W3C Web Cryptography API does map a subset of these algorithm identifiers (with additional parameters for the ciphersuites) to the IANA registry of JOSE identifiers for algorithms [JWA].

24. References

24.1. Normative References

[JWA] Jones, M., "JSON Web Algorithms (JWA)", IETF Internet Draft, October 2014, <http://www.w3.org/TR/2014/WD-WebCryptoAPI-20140325/>.

[PKCS11] Gleeson, S. and C. Zimman, "OASIS PKCS 11", OASIS Working Draft draft, November 2014, <https://www.oasis-open.org/committees/download.php/54455/pkcs11-base-v2.40-wd11.pdf>.

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

[RFC5297] Harkins, D., "Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)", RFC 5297, October 2008.

[W3CWebCryptoCR] Sleevi, R. and M. Watson, "Web Cryptography API", W3C Candidate Recommendation , November 2014, <http://www.w3.org/TR/WebCryptoAPI>.

[W3CWebCryptoLC] Sleevi, R. and M. Watson, "Web Cryptography API", W3C Last Call Working Draft , March 2014, <http://www.w3.org/TR/2014/WD-WebCryptoAPI-20140325/>.

24.2. Informative References

[bardou12padding] Bardou, R., Focardi, R., Kawamoto, Y., Simionato, L., Steel, G., and Joe-Kai-Tsay, "Efficient padding oracle attacks on cryptographic hardware", In Advances in Cryptology: Proceedings of CRYPTO '12, volume 7417 of LNCS, pages 608-625. Springer, 2012. , 2012.

[barthe2009POPL] Barthe, G., Gregoire, B., and S. Zanella-Beguelin, "Formal certification of code-based cryptographic proofs", In 36th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2009, pages 90-101. ACM, 2009. , 2009, <http://dx.doi.org/10.1145/1480881.1480894>.

[bellare06HMAC]
Bellare, M., "New proofs for MAC and HMAC: security without collision-resistance", In Cynthia Dwork, editor, CRYPTO, volume 4117 of Lecture Notes in Computer Science, pages 602-619. Springer, 2006 , 2006.

[bellare96eurocrypt]
Bellare, M. and P. Rogaway, "The exact security of digital signatures-how to sign with rsa and rabin", In Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques, EUROCRYPT'96, pages 399-416, Berlin, Heidelberg, 1996. Springer-Verlag. , 1996, <http://dl.acm.org/citation.cfm?id=1754495.1754541>.

[bleichenbacher98]
Bleichenbacher, D., "Chosen ciphertext attacks against protocols based on the RSA encryption standard", In Advances in Cryptology: Proceedings of CRYPTO '98, volume 1462 of Lecture Notes in Computer Science,pages 1-12, 1998. , 1998.

[boneh01crypto]
Boneh, D. and I. Shparlinski, "On the unpredictability of bits of the elliptic curve diffie-hellman scheme", In Joe Kilian, editor, Advances in Cryptology - CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 201-212. Springer Berlin Heidelberg, 2001. , 2001, <http://dx.doi.org/10.1007/3-540-44647-8_12>.

[email] Kaliski, B., "Raising the Standard for RSA Signatures: RSA-PSS", Accessed: 11-Nov-2014, 2003, <https://web.archive.org/web/20130523004555/http://www.rsa.com/rsalabs/node.asp?id=2005>.

[enisa13] Smart, N., Rijmen, V., Warinschi, B., and G. Watson, "Algorithms, key sizes and parameters report: 2013 recommendations", Technical report, October 2013. ENISA Report. Version 1.0. , 2013.

[fujisaki04OAEP]
Fujisaki, E., Okamoto, T., Pointcheval, D., and J. Stern, "RSA-OAEP is secure under the RSA assumption", Journal. Cryptol., 17(2):81-104, March 2004 , 2004, <http://dx.doi.org/10.1007/s00145-002-0204-y>.

[jager12bleichenbacher]
Jager, T., Schinzel, S., and J. Somorovsky, "Bleichenbacher's attack strikes again: breaking PKCS#1 v1.5 in XML encryption", In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, Computer Security - ESORICS 2012, volume 7459 of Lecture Notes in Computer Science, pages 752-769. Springer Berlin Heidelberg, 2012. , 2012, <http://dx.doi.org/10.1007/978-3-642-33167-1_43>.

[kaminsky10]
Kaminsky, A., Kurdziel, M., and S. Radziszowski, "An overview of cryptanalysis research for the advanced encryption standard", In Military Communications Conference, 2010 - MILCOM 2010. , 2010.

[knellwolf12]
Knellwolf, S. and D. Khovratovich, "New Preimage Attacks against Reduced SHA-1", In Advances in Cryptology - CRYPTO 2012, volume 7417 of Lecture Notes in Computer Science, pages 367-383. Springer Berlin Heidelberg, 2012. , 2012, <http://www.iacr.org/cryptodb/data/paper.php?pubkey=24323>.

[krawczyk10HKDF]
Krawczyk, H., "Cryptographic extraction and key derivation: the HKDF scheme", In Tal Rabin, editor, CRYPTO, volume 6223 of Lecture Notes in Computer Science, pages 631-648. Springer, 2010. , 2010.

[manger01]
Manger, J., "A chosen ciphertext attack on rsa optimal asymmetric encryption padding (OAEP) as standardized in PKCS #1 v2.0", In Joe Kilian, editor, Advances in Cryptology CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 230-238. Springer Berlin / Heidelberg, 2001 , 2001.

[mitchell05cbc]
Mitchell, C., "Error oracle attacks on CBC mode: is there a future for CBC mode encryption?", In J. et al. Zhou, editor, ISC 2005, volume 3650 in Lecture Notes in Computer Science, pages 244-258, 2005. , 2005.

[paterson04padding]
Paterson, K. and A. Yau, "Padding oracle attacks on the ISO CBC mode encryption standard", In T. Okamoto, editor, RSA '04 Cryptography Track, number 2964 in LNCS, pages 305-323. Springer, 2004. , 2004.

[rizzo10USENIX]
Rizzo, J. and T. Duong, "Practical padding oracle attacks", WOOT'10, pages 1-8, Berkeley, CA, USA, 2010. USENIX Association , 2010, <http://portal.acm.org/citation.cfm?id=1925004.1925008>.

[rogaway06deterministic]
Rogaway, P. and T. Shrimpton, "Deterministic authenticated-encryption: a provable-security treatment of the key-wrap problem", In Advances in Cryptology (EUROCRYPT '06), volume 4004 of LNCS, pages 373-390, 2006. , 2006, <https://eprint.iacr.org/2006/221.pdf>.

[rogaway11evaluation]
Rogaway, P., "Evaluation of some blockcipher modes of operation", Technical report, University of California, Davis, February 2011. Evaluation carried out for the Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan. , 2011.

[schneier]
Schneier, B., "When Will We See Collisions for SHA-1?", Accessed: 11-Nov-2014, 2012, <https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html>.

[SteelChoice]
Steel, G., "Choice of Algorithms in the W3C Crypto API", Accessed: 20-Nov-2014, 2014, <http://cryptosense.com/choice-of-algorithms-in-the-w3c-crypto-api/>.

[stevens] Stevens, M., "Cryptanalysis of MD5 and SHA-1", Accessed: 11-Nov-2014, 2012, <http://2012.sharcs.org/slides/stevens.pdf>.

[vaudenay02]
Vaudenay, S., "Security flaws induced by CBC padding - applications to SSL, IPSEC, WTLS ...", In Lars R. Knudsen, editor, EUROCRYPT, volume 2332 of Lecture Notes in Computer Science, pages 534-546. Springer, 2002. , 2002.

[vaudenay03PKC]
Vaudenay, S., "The security of DSA and ECDSA", In Yvo G. Desmedt, editor, Public Key Cryptography - PKC 2003, volume 2567 of Lecture Notes in Computer Science, pages 309-323. Springer Berlin Heidelberg, 2002 , 2002, <http://dx.doi.org/10.1007/3-540-36288-6_23>.

[wang2005]
Wang, X., Yin, Y., and H. Yu, "Finding collisions in the full SHA-1", In Proceedings of the 25th Annual International Conference on Advances in Cryptology, CRYPTO'05, pages 17-36, Berlin, Heidelberg, 2005. Springer-Verlag , 2005, <http://dx.doi.org/10.1007/11535218_2>.

[weakdh] Adrian, D., Bhargavan, K., and et. al., "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice", In Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS '15), Denver, CO, October 2015 , 2015, <http://weakdh.org>.

[wen12framework]
Wen, C., Dawson, E., Nieto, J., and L. Simpson, "A framework for security analysis of key derivation functions", In Mark Dermot Ryan, Ben Smyth, and Guilin Wang, editors, ISPEC, volume 7232 of Lecture Notes in Computer Science, pages 199-216. Springer, 2012 , 2012.

[yao05kdf]
Yao, F. and Y. Yin, "Design and analysis of password-based key derivation functions", In Alfred Menezes, editor, CT-RSA, volume 3376 of Lecture Notes in Computer Science, pages 245-261. Springer, 2005 , 2005.

Appendix A. Acknowledgments

Special thanks to Ryan Sleevi and Mark Watson for their work on the Web Cryptography API, as well as Rich Salz for bringing up the issue of algorithm-specific security considerations. Thanks to Kelsey Cairns for helping with the formal analysis. Graham Steel authored the original version of this report [SteelChoice], and Harry Halpin from W3C/MIT agreed to edit and keep the document up to date.

Authors' Addresses

Harry Halpin (editor)
W3C/MIT

Email: harry@w3c.org
URI: http://www.ibiblio.org/hhalpin/

Graham Steel
Cryptosense/INRIA

Email: Graham.Steel@inria.fr
URI: http://www.lsv.ens-cachan.fr/~steel/