Authenticated encryption

[1]**Authenticated Encryption** (**AE**) and **Authenticated Encryption with Associated Data** (**AEAD**) are forms of encryption which simultaneously assure the confidentiality and authenticity of data.

Programming interface

A typical programming interface for an AE implementation provides the following functions:

- Encryption
  - Input: *plaintext*, *key*, and optionally a *header* in plaintext that will not be encrypted, but will be covered by authenticity protection.
  - Output: *ciphertext* and *authentication tag* (message authentication code or MAC).
- Decryption
  - Input: *ciphertext*, *key*, *authentication tag*, and optionally a *header* (if used during the encryption).
  - Output: *plaintext*, or an error if the *authentication tag* does not match the supplied *ciphertext* or *header*.

The *header* part is intended to provide authenticity and integrity protection for networking or storage metadata for which confidentiality is unnecessary, but authenticity is desired.

History

The need for authenticated encryption emerged from the observation that securely combining separate *confidentiality* and *authentication* block cipher operation modes could be error prone and difficult.[1][2] This was confirmed by a number of practical attacks introduced into production protocols and applications by incorrect implementation, or lack of authentication (including SSL/TLS).[3]

Around the year 2000, a number of efforts evolved around the notion of standardizing modes that ensured correct implementation. In particular, strong interest in possibly secure modes was sparked by the publication of Charanjit Jutla's integrity-aware CBC and integrity-aware parallelizable, IAPM, modes[4] in 2000 (see OCB and chronology[5]). Six different authenticated encryption modes (namely offset codebook mode 2.0, OCB 2.0; Key Wrap; counter with CBC-MAC, CCM; encrypt then authenticate then translate, EAX; encrypt-then-MAC, EtM; and Galois/counter mode, GCM) have been standardized in ISO/IEC 19772:2009.[6] More authenticated encryption methods were developed in response to NIST solicitation.[7] Sponge functions can be used in duplex mode to provide authenticated encryption.[8]

Bellare and Namprempre (2000) analyzed three compositions of encryption and MAC primitives, and demonstrated that encrypting a message and subsequently applying a MAC to the ciphertext (the Encrypt-then-MAC approach) implies security against an adaptive chosen ciphertext attack, provided that both functions meet minimum required properties. Katz and Yung investigated the notion under the name "unforgeable encryption" and proved it implies security against chosen ciphertext attacks.[9]

In 2013, the CAESAR competition was announced to encourage design of authenticated encryption modes.[10]

In 2015, ChaCha20-Poly1305 is added as an alternative AE construction to GCM in IETF protocols.

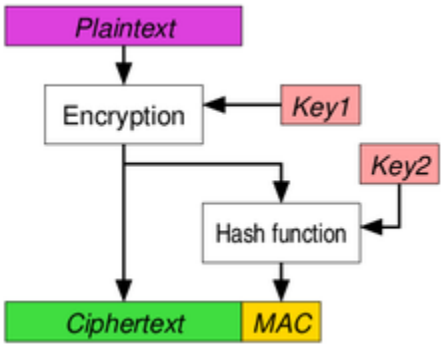
Authenticated encryption with associated data (AEAD)

AEAD is a variant of AE that allows a recipient to check the integrity of both the encrypted and unencrypted information in a message.[11] AEAD binds associated data (AD) to the ciphertext and to the context where it is supposed to appear so that attempts to "cut-and-paste" a valid ciphertext into a different context are detected and rejected.

It is required, for example, by network packets or frames where the header needs visibility, the payload needs confidentiality, and both need integrity and authenticity.

Approaches to authenticated encryption

Encrypt-then-MAC (EtM)

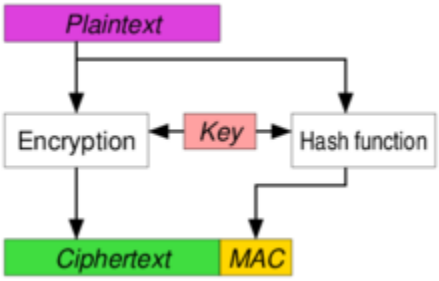


EtM approach

The plaintext is first encrypted, then a MAC is produced based on the resulting ciphertext. The ciphertext and its MAC are sent together. Used in, e.g., IPsec.[12] The standard method according to ISO/IEC 19772:2009.[6] This is the only method which can reach the highest definition of security in AE, but this can only be achieved when the MAC used is "strongly unforgeable".[13] In November 2014, TLS and DTLS extension for EtM has been published as RFC 7366 (https://datatracker.ietf.org/doc/html/rfc7366) . Various EtM ciphersuites exist for SSHv2 as well (e.g., `hmac-sha1-etm@openssh.com`).

Note that key separation is mandatory (distinct keys must be used for encryption and for the keyed hash), otherwise it is potentially insecure depending on the specific encryption method and hash function used.

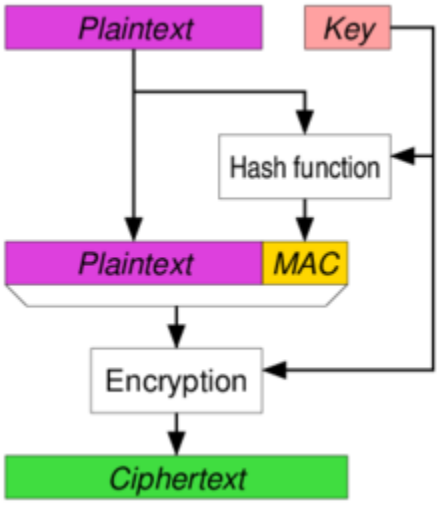
Encrypt-and-MAC (E&M)



E&M approach

A MAC is produced based on the plaintext, and the plaintext is encrypted without the MAC. The plaintext's MAC and the ciphertext are sent together. Used in, e.g., SSH.[14] Even though the E&M approach has not been proved to be strongly unforgeable in itself,[13] it is possible to apply some minor modifications to SSH to make it strongly unforgeable despite the approach.[15]

MAC-then-Encrypt (MtE)



MtE approach

A MAC is produced based on the plaintext, then the plaintext and MAC are together encrypted to produce a ciphertext based on both. The ciphertext (containing an encrypted MAC) is sent. AEAD is used in SSL/TLS.[16] Even though the MtE approach has not been proven to be strongly unforgeable in itself,[13] the SSL/TLS implementation has been proven to be strongly unforgeable

by Krawczyk who showed that SSL/TLS was, in fact, secure because of the encoding used alongside the MtE mechanism.[17] Despite the theoretical security, deeper analysis of SSL/TLS modeled the protection as MAC-then-pad-then-encrypt, i.e. the plaintext is first padded to the block size of the encryption function. Padding errors often result in the detectable errors on the recipient's side, which in turn lead to padding oracle attacks, such as Lucky Thirteen.

See also

- Block cipher mode of operation
- CCM mode
- CWC mode
- OCB mode
- EAX mode
- GCM
- GCM-SIV
- ChaCha20-Poly1305
- SGCM
- Signcryption

References

1. *M. Bellare; P. Rogaway; D. Wagner. "A Conventional Authenticated-Encryption Mode" (http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/eax/eax-spec.pdf) (PDF). NIST. Retrieved March 12, 2013. "people had been doing rather poorly when they tried to glue together a traditional (privacy-only) encryption scheme and a message authentication code (MAC)"*
2. *T. Kohno; J. Viega & D. Whiting. "The CWC Authenticated Encryption (Associated Data) Mode" (http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/cwc/cwc-spec.pdf) (PDF). NIST. Retrieved March 12, 2013. "it is very easy to accidentally combine secure encryption schemes with secure MACs and still get insecure authenticated encryption schemes"*
3. *"Failures of secret-key cryptography" (https://web.archive.org/web/20130418063008/http://cr.yp.to/talks/2013.03.12/slides.pdf) (PDF). Daniel J. Bernstein. Archived from the original (https://cr.yp.to/talks/2013.03.12/slides.pdf) (PDF) on April 18, 2013. Retrieved March 12, 2013.*

4. *Jutl, Charanjit S. (2000-08-01). "Encryption Modes with Almost Free Message Integrity" (https://eprint.iacr.org/2000/039) . Cryptology ePrint Archive: Report 2000/039. Proceedings IACR EUROCRYPT 2001. IACR. Retrieved 2013-03-16.*

5. *T. Krovetz; P. Rogaway (2011-03-01). "The Software Performance of Authenticated-Encryption Modes" (https://web.cs.ucdavis.edu/~rogaway/papers/ae.pdf) (PDF). Fast Software Encryption 2011 (FSE 2011). IACR.*

6. *"Information technology -- Security techniques -- Authenticated encryption" (https://www.iso.org/iso/catalogue_detail.htm?csnumber=46345) . 19772:2009. ISO/IEC. Retrieved March 12, 2013.*

7. *"Encryption modes development" (http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html) . NIST. Retrieved April 17, 2013.*

8. *The Keccak Team. "Duplexing The Sponge" (http://sponge.noekeon.org/SpongeDuplex.pdf) (PDF).*

9. *Katz, J.; Yung, M. (2001). B. Schneier (ed.). Unforgeable Encryption and Chosen Ciphertext Secure Modes of Operation. Fast Software Encryption (FSE): 2000 Proceedings. Lecture Notes in Computer Science. Vol. 1978. pp. 284–299. doi:10.1007/3-540-44706-7_20 (https://doi.org/10.1007%2F3-540-44706-7_20) . ISBN 978-3-540-41728-6.*

10. *"CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness" (https://competitions.cr.yp.to/caesar.html) . Retrieved March 12, 2013.*

11. *"NIST Issues First Call for 'Lightweight Cryptography' to Protect Small Electronics" (https://www.nist.gov/news-events/news/2018/04/nist-issues-first-call-lightweight-cryptography-protect-small-electronics) . 2018-04-18. Retrieved 2019-09-04.*

12. *"Separate Confidentiality and Integrity Algorithms" (https://tools.ietf.org/html/rfc4303#section-3.3.2.1) . RFC 4303. Internet Engineering Task Force (IETF). Retrieved 2018-09-12.*

13. *"Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm" (https://cseweb.ucsd.edu/~mihir/papers/oem.html) . M. Bellare and C. Namprempre. Retrieved April 13, 2013.*

14. *"Data Integrity" (https://tools.ietf.org/html/rfc4253#section-6.4) . RFC 4253. Internet Engineering Task Force (IETF). Retrieved 2018-09-12.*

15. *Bellare, Mihir; Kohno, Tadayoshi; Namprempre, Chanathip. "Breaking and Provably Repairing the SSH Authenticated Encryption Scheme: A Case Study of the Encode-then-Encrypt-and-MAC Paradigm" (https://homes.cs.washington.edu/~yoshi/papers/SSH/ssh.pdf) (PDF). ACM Transactions on Information and System Security. Retrieved 30 August 2021.*

16. *"Record Payload Protection" (https://tools.ietf.org/html/rfc5246#section-6.2.3) . RFC 5246. Internet Engineering Task Force (IETF). Retrieved 2018-09-12.*

17. *"The Order of Encryption and Authentication for Protecting Communications (Or: How Secure is SSL?)" (https://www.iacr.org/archive/crypto2001/21390309.pdf)* *(PDF)*. *H. Krawczyk*. *Retrieved April 13, 2013*.

General

- Bellare, M.; Namprempre, C. (2000), T. Okamoto (ed.), "Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm" (https://link.springer.com/content/pdf/10.1007/3-540-44448-3_41.pdf) (PDF), *Extended Abstract in Advances in Cryptology: Asiacrypt 2000 Proceedings*, Lecture Notes in Computer Science, Springer-Verlag, **1976**: 531, doi:10.1007/3-540-44448-3_41 (https://doi.org/10.1007%2F3-540-44448-3_41) , ISBN 978-3-540-41404-9

External links

- NIST: Modes Development
- How to choose an Authenticated Encryption mode

Last edited 10 days ago by 209.35.169.13