AEAD

Notes on January 28 2022 training

Jeffrey Goldberg
jeffrey@goldmark.org

May 8, 2024

Notional review

Security goals

Example goals

IND Indistinguishability

NM Non-malleability

SUF Strong Unforgeability

Attacker models

Example models

CPA Chosen Plaintext Attack

CCA Chosen Ciphertext Attack

CMA Chosen Message Attack

Notions as games

If there is no polynomial time/space $\mathcal{A}$ (Adversary, Algorithm) that can win the "game" at a meaningfully better than chance rate, then the scheme is secure.

History lesson

Triggering a history lesson

> *[Why] don't SSH and TLS use encrypt-then-MAC? The simple answer is that when SSH and TLS were created, other approaches appeared adequate—not because theoretical weaknesses didn't exist but because theoretical weaknesses don't necessarily become actual vulnerabilities. [Aum17, ch. 8]*

That passage motivates my history lesson.

History lesson

Proofs

NM and CCA

1990 Naor and Yung [NY90] created a provably IND-CCA scheme (using non-malleability)

1990–1998 Refining both NM and CCA goals

1998 Bellare et al. [Bel+98] proved that you can't have IND-CCA without NM-CCA.

Some integrity notions

INT-PTXT Integrity of plaintexts. $\mathcal{A}$ cannot produce a ciphertext decrypting to a message that the sender never encrypted.

INT-CTXT Integrity of ciphertexts. $\mathcal{A}$ cannot produce ciphertext not previously produced by the sender.

AE with MAC

In 2000 Bellare and Namprempre [BN00] prove the security properties of various combinations of an IND-CPA encryption scheme with a Strongly Unforgeable MAC.

Construction	IND-CPA	IND-CCA	NM-CPA	INT-PTXT	INT-CTXT
Enc-and-MAC	×	×	×	✓	×
MAC-then-enc	✓	×	×	✓	×
Enc-then-MAC	✓	✓	✓	✓	✓

Table 1: Security properties of compositions of encryption and message authentication under the assumption that the encryption scheme meets IND-CPA and the MAC meets SUF.

History lesson

Proofs of Concept

RSA Padding Oracle

1998 Bleichenbacher [Ble98] showed how padding in an RSA scheme and an oracle that says where decryption is properly formatted can lead to decryption of the message.

2001 OAEP (Optimal Asymmetric Encryption Padding) mode published to fix this.

2002 Manger [Man01] shows that OAEP must be implemented very, very carefully to not create a format oracle of its own.

Later OAEP implemented very very carefully.

CBC Padding Oracle

2002 Vaudenay [Vau02] lays out the basic structure of a CCA against CBC-mode.

2010 Rizzo and Duong [RD10] expand on the attack, and show how it can be used to break more than confidentiality. Saying,

And what they said (2002)

Vaudenay [Vau02]:

> *[Authentocation] still has an optional status in IPSEC. As already recommended by Bellovin [Bel96], authentication should be mandatory.*

Black and Urtubia [BU02]

> *[We] argue that the best way to prevent all of these attacks is to insist on integrity of ciphertexts [BN00] in addition to semantic security as the "proper" notion of privacy for symmetric encryption schemes.*

What they continued to say

Rizzo and Duong [RD10]:

> *If encrypted messages are not authenticated, data integrity cannot be guaranteed which makes systems vulnerable to practical and dangerous chosen-ciphertext attacks.*

History lesson

Attacks and responses

2011–2014

Lots of attacks. Often involved downgrade attacks to older versions of TLS.

Responses

- Standard libraries still not supporting authenticated encryption mode.
- “CBC bad; CTR good!”
- Specific hacks to thwart the very specific attack on CBC padding.
- We roll our own Encrypt-then-MAC construction for OPVault. [Agi12]

Lessons of history

- Provable security matters. Listen to the mathematicians!
- “Theoretical vulnerability” just means a vulnerability that hasn’t been exploited yet.
- Beware downgrade attacks. Backwards compatibility and long transition periods for security updates leave everyone vulnerable.

Notes on Chapter 7

Verify then decrypt

I sometimes call encrypt-then-MAC “verify-then-decrypt” as it better communicates why it works and why no processing of the ciphertext should occur before the MAC is verified.

AE, ED, and AEAD

AE Authenticated Encryption

AD Authenticated Decryption [in Aum17]

AEAD Authenticated Encryption with *Associated Data*

Two-layer

We run into problems with GCM for large Documents. Because no processing of the ciphertext should be done before the the integrity is checked, there are limits how much data can be decrypted at once. We really should move away from GCM for documents (there are modes better suited for data of that size) or use “chunked GCM.”

Polynomial multiplication typo

Should be

$$(1 + X + X^2) \otimes (X + X^3)$$

Notes on Chapter 7

xor refersher

Hash key recovery

> *Now what happens if you get two tags, T_1 and T_2, computed with the same nonce N? Right, the AES part will vanish.*

Way back in August, I asked everyone to get comfortable with xor …

Bit facts

Notation: '0^n' means a string of n bits, all of which are zero. Eg, $0^5 = 00000$.

Property	Definition	Example
Commutative	$a \oplus b = b \oplus a$	$01 \oplus 11 = 11 \oplus 01 = 10$
Associative	$(a \oplus b) \oplus c = a \oplus (b \oplus c)$	
Zero identity	$a \oplus 0^n = a$	$0110 \oplus 0000 = 0110$
Own inverse	$a \oplus a = 0^n$	$10 \oplus 00 = 10$

Table 2: Properties of xor: For all a, b, and c bit strings of length n.

Task

Convince yourself that

$$(a \oplus b) \oplus (c \oplus a) = c \oplus b$$

for any bit sequences a, b, and c of the same length.

You can do this either algebraically using the properties of xor, or you can do it by constructing a few examples and working through them.

Do both.

OCB v GCM

Even when everyone is trying to be nice, patents suck. GCM is available in all the places, platforms, and toolkits that we need it in. OCB is not.

Questions?

References I

[Agi12] AgileBits. ***OPVault design.*** First release November 2012. Minor fixes since then. Nov. 2012. URL: `https://support.1password.com/cs/opvault-design/` (visited on 01/28/2022).

[Aum17] Jean-Philippe Aumasson. ***Serious cryptography: a practical introduction to modern encryption.*** No Starch Press, 2017.

[Bel+98] Mihir Bellare et al. **"Relations Among Notions of Security for Public-Key Encryption Schemes".** In: *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*. 1998, pp. 26–45.

[Bel96] Steve Bellovin. **"Problem Areas for the IP Security Protocols".** In: *6th USENIX Security Symposium (USENIX Security 96)*. San Jose, CA: USENIX Association, July 1996.

References II

[Ble98] Daniel Bleichenbacher. **“Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1”.** In: *Annual International Cryptology Conference*. Springer. 1998, pp. 1–12.

[BN00] Mihir Bellare and Chanathip Namprempre. **“Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm”.** In: *Advances in Cryptology — ASIACRYPT 2000*. Ed. by Tatsuaki Okamoto. Vol. 1976. Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, Dec. 2000, pp. 531–545.

[BU02] John Black and Hector Urtubia. **“Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption.”.** In: *USENIX Security Symposium*. Aug. 2002, pp. 327–338.

References III

[Man01] James Manger. **“A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1 v2.0”.** English. In: *Advances in Cryptology — CRYPTO 2001*. Ed. by Joe Kilian. Vol. 2139. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2001, pp. 230–238.

[NY90] Moni Naor and Moti Yung. **“Public-key cryptosystems provably secure against chosen ciphertext attacks”.** In: *Proceedings of the twenty-second annual ACM symposium on Theory of computing*. 1990, pp. 427–437.

[RD10] Juliano Rizzo and Thai Duong. **“Practical Padding Oracle Attacks”.** In: *4th USENIX Workshop on Offensive Technologies (WOOT 10)*. Washington, DC: USENIX Association, Aug. 2010.

References iv

[Vau02] Serge Vaudenay. **“Security Flaws Induced by CBC Padding – Applications to SSL, IPSEC, WTLS ...”.** In: *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology*. EUROCRYPT ’02. Berlin, Heidelberg: Springer-Verlag, 2002, pp. 534–546.