MTG

AEAD-to-CBC Downgrade Attacks on CMS

Johannes Roth[1], **Falko Strenzke**[2]

Work sponsored by German Federal Office for Information Security (BSI)

MTG AG, Darmstadt, Germany

[1] johannes.roth@mtg.de
[2] falko.strenzke@mtg.de

Decryption oracle attack from literature

MTG

1. Original CBC-encrypted message to victim:

   > *Your personal secret identification code is 1234. Do not reveal it.*

2. Victim receives modified (blocks reordered) CBC-encrypted message from Eve displayed as:

   ```
   ^R`<9d>è{w^A<85>^S¡<9f>:<8d>£<98>
   ^Fá¿<9c><9c>sE,cp÷á^SR:^F<95>Û¦Û<
   ```

3. Victim replies:

   > *Dear Eve, there seems to have been a decryption error:*
   >
   > ```
   > > ^R`<9d>è{w^A<85>^S¡<9f>:<8d>£<98>
   >   ^Fá¿<9c><9c>sE,cp÷á^SR:^F<95>Û¦Û<
   > ```

4. Eve learns the original message[3]

[3] CBC decryption $D_k^{\mathrm{CBC}} = D_k(C_i) \oplus C_{i-1}$

Literature for this type of attack

[1] Katz, J., Schneier, B.: A Chosen Ciphertext Attack Against Several E-Mail En- cryption Protocols. In: 9th USENIX Security Symposium (USENIX Security 00), Denver, CO, USENIX Association (August 2000)

[2] Jallad, K., Katz, J., Schneier, B.: Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG. In Chan, A.H., Gligor, V., eds.: Information Security, Berlin, Heidelberg, Springer Berlin Heidelberg (2002) 90–101

AEAD-to-CBC downgrade attack against CCM and GCM in CMS

- AES-based modes CCM, GCM
  - Both modes use CTR mode encryption
  - Key stream: $S_i = E_k(\underbrace{f(\text{nonce}, i)}_{H_i \text{ (public)}})$
  - CTR en- & decryption $C_i = P_i \oplus S_i$
- Legacy mode in CMS: CBC
  - CBC decryption: $D_k^{\text{CBC}} = D_k(C_i) \oplus C_{i-1}$
- Idea of the attack on a CCM or GCM message to victim
  - Decrypt low entropy plaintext block
  - Guess for P_t implies guess for $S_t = C_t \oplus P_t$
  - Let the victim block-decrypt n guesses $\{S_{t,j} \mid j = 1, \ldots, n\}$ with CBC mode and compare $D_k(S_{t,j})$ against known H_t
    - (CBC decr. oracle is block decr. oracle: simply undo $\oplus C_{i-1}$)
  - When the attacker finds $H_t = D_k(S_{t,j})$, then $P_t = C_t \oplus S_{t,j}$
- Padding check may increase number of queries

Example Attack: reply with original message

MTG

1. Original AEAD message to victim:

   > *Your personal secret identification code is 1234. Do not reveal it to anyone.*

2. Eve knows the message template, but not the secret code
3. Victim receives CBC-encrypted message from Eve displayed as:

   ```
   ^R`<9d>è{w^A<85>^S¡<9f>:<8d>£<98>
   ^Fá¿<9c><9c>sE,cp÷á^SR:^F<95>Û¦Û<
   ```

4. Victim replies:

   > *Dear Eve, there seems to have been a decryption error:*
   >
   > > ```
   > > ^R`<9d>è{w^A<85>^S¡<9f>:<8d>£<98>
   > > ^Fá¿<9c><9c>sE,cp÷á^SR:^F<95>Û¦Û<
   > > ```

5. Eve learns the secret code

Example attack: observing traffic between MUA and server

MTG

- S/MIME block decryption oracle attack without user interaction [3]
- seems to make attacks on S/MIME messages feasible

[3] Ising, F., Poddebniak, D., Kappert, T., Saatjohann, C., Schinzel, S.: Content-Type: multipart/oracle - tapping into format oracles in email End-to-End encryption. In: 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USENIX Association (August 2023) 4175–4192

Fixing it for KEM-RI

MTG

- not the right place
- advantage: takes effect whenever KEM encryption is used

Fixing it generally: introduce key separation for AEAD

MTG

one possibility (just for illustration):

- Deprecate AES-CCM and AES-GCM in CMS
- Release new modes AES-CCM-KD and AES-GCM-KD with key derivation
  - At minimum: key separation between AEAD and legacy modes
  - Better: key derivation based on input of `contentEncryptionAlgorithm` (CEA)
    - Carefully crafted key derivation, ideally **not based on AES**
    - Otherwise, can possibly be "emulated" by legacy mode oracle
    - e.g., using $k'_{\mathrm{bad}} = E_k(0 \ldots 0 < \mathrm{CEA} >)$ would be vulnerable to decryption with CFB, CTR
    - (e.g., let the victim encrypt the counter block $0 \ldots 0 < \mathrm{CEA} >$ within CTR decryption and leak the k'_{bad})
    - (even if there is only CBC legacy mode, there might be custom extensions of CMS introducing other legacy modes)

Signatures don't help

MTG

- signatures cannot protect integrity of ciphertexts
  - attacker doesn't have to consider signatures of original message
  - attacker can apply own outer signature
  - even if victim's MUA enforces inner signatures, there may be vulnerabilities [4]
    - verification of inner signature happens *after* vulnerable padding check

[4] Ising et al. describe attack against Google's hosted mail service with S/MIME support

Practical relevance

MTG

- S/MIME unlikely to be subject to straightforward attack
  - "garbage bytes detection"
  - missing S/MIME header

    ```
    Content-Type: text/plain; charset=us-ascii
    Content-Transfer-Encoding: 7bit
    ```
- S/MIME might be vulnerable to application specific attacks as in [3]
- AEAD still not widely supported by S/MIME clients

Summary / Overview

MTG

- The new attack is an *inverse* oracle attack
  - attacks the block encryption with a block-decryption oracle
  - assumes a fully revealing oracle
  - limited to decrypting low entropy blocks
  - actually vulnerable systems are unknown
- The previously known are *forward/direct*
  - attacked operation and the oracle have the same cipher direction
  - variants
    - fully revealing oracle attacks
    - padding oracle attacks (CBC padding, format oracle)
- Solution is key separation
  - OpenPGP crypto-refresh introduces key separation together with AEAD encryption in v2 SEIPD packets[5], cross-mode attacks are given as the reason

[5] `https://datatracker.ietf.org/doc/html/draft-ietf-openpgp-crypto-refresh-12#section-5.13.2-3`

Feedback / comments ?