Authenticated Encryption

CBC paddings attacks

Recap

Authenticated encryption: CPA security + ciphertext integrity

- Confidentiality in presence of **active** adversary
- Prevents chosen-ciphertext attacks

Limitation: cannot help bad implementations … (this segment)

Authenticated encryption modes:

- Standards: GCM, CCM, EAX
- General construction: encrypt-then-MAC

The TLS record protocol (CBC encryption)

Decryption: **dec($k_{b\to s}$, record, $ctr_{b\to s}$)** :

step 1: CBC decrypt record using k_{enc}

step 2: check pad format: abort if invalid

step 3: check tag on [++$ctr_{b\to s}$ || header || data]
abort if invalid

Two types of error:

- **padding error**
- **MAC error**

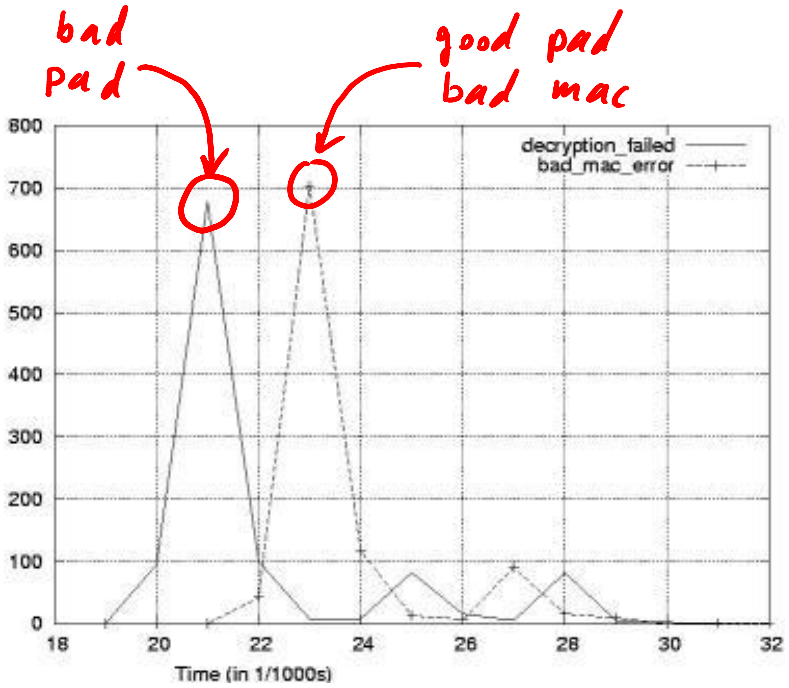
Padding oracle

Suppose attacker can differentiate the two errors
(pad error, MAC error):

⇒ **Padding oracle**:
attacker submits ciphertext and learns if
last bytes of plaintext are a valid pad

Nice example of a
chosen ciphertext attack

Padding oracle via timing OpenSSL



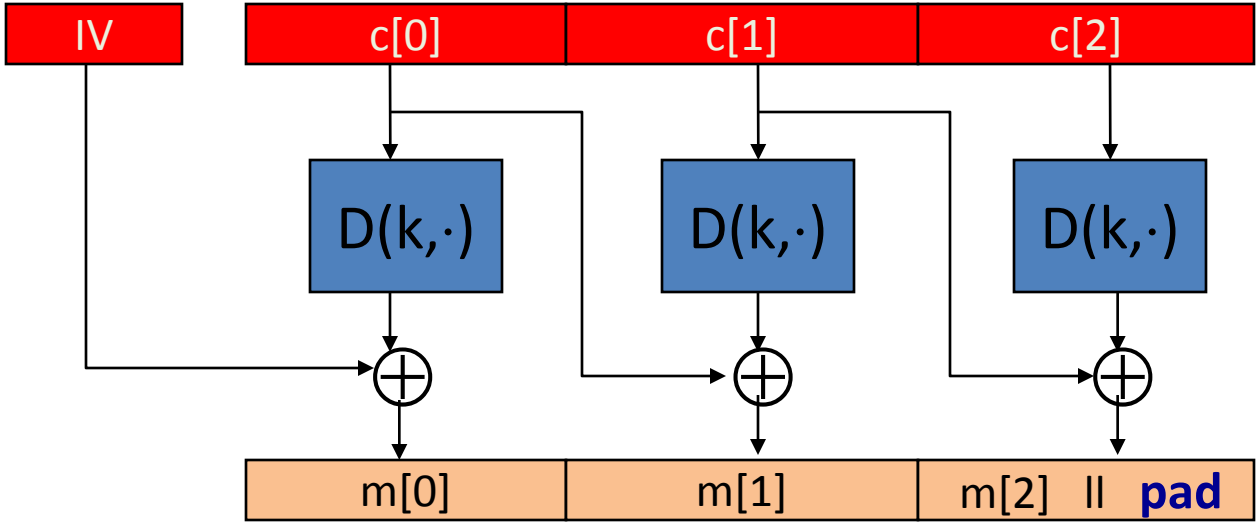
Credit: Brice Canvel

(fixed in OpenSSL 0.9.7a)

In older TLS 1.0: padding oracle due to different alert messages.

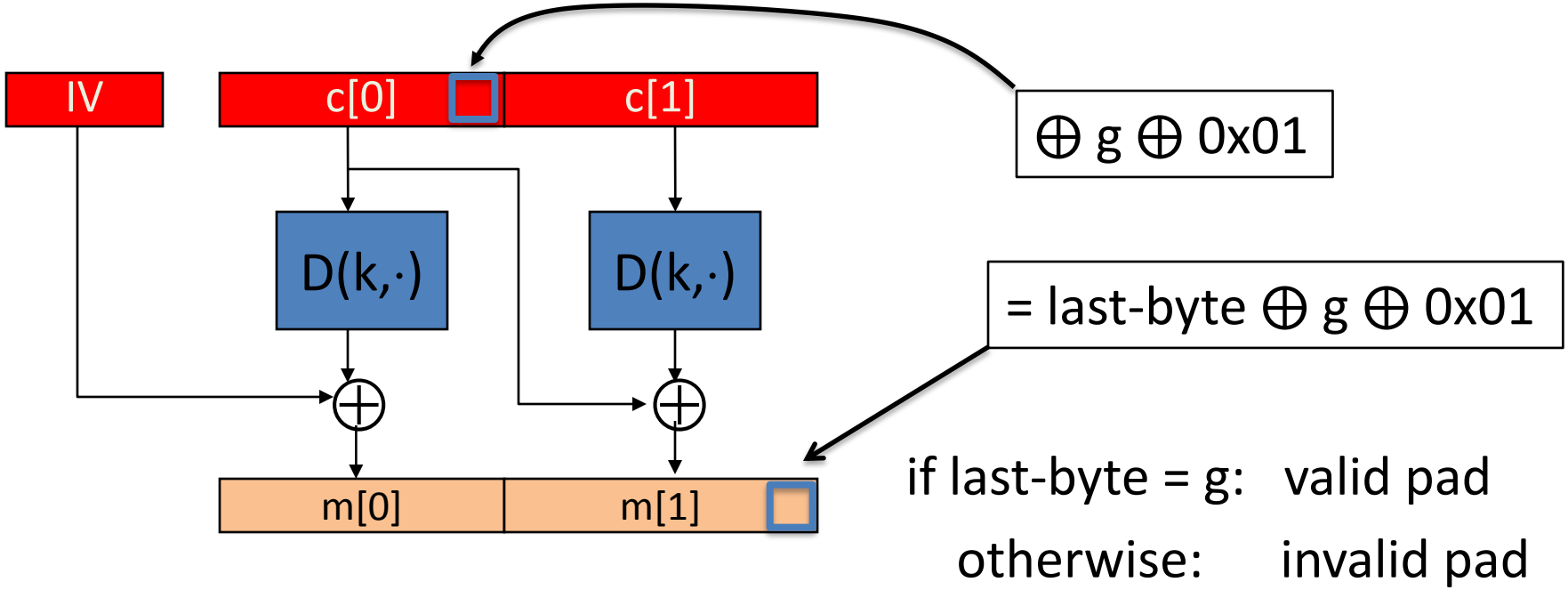
Using a padding oracle (CBC encryption)

Attacker has ciphertext **c = (c[0], c[1], c[2])** and it wants **m[1]**



Using a padding oracle (CBC encryption)

step 1: let **g** be a guess for the last byte of m[1]



if last-byte = g: valid pad

otherwise: invalid pad

Using a padding oracle (CBC encryption)

Attack: submit **(IV, c'[0], c[1])** to padding oracle

$\Rightarrow$ attacker learns if last-byte = g

Repeat with g = 0,1, …, 255 to learn last byte of m[1]

Then use a (02, 02) pad to learn the next byte and so on …

IMAP over TLS

Problem: TLS renegotiates key when an invalid record is received

<u>Enter IMAP over TLS</u>: (protocol for reading email)

- Every five minutes client sends login message to server:

  LOGIN "username" "password"

- Exact same attack works, despite new keys

  ⇒ recovers password in a few hours.

Lesson

1. Encrypt-then-MAC would completely avoid this problem:

   MAC is checked first and ciphertext discarded if invalid

2. MAC-then-CBC provides A.E., but padding oracle destroys it

Will this attack work if TLS used counter mode instead of CBC?

(i.e. use MAC-then-CTR)

- Yes, padding oracles affect all encryption schemes
- It depends on what block cipher is used
- No, counter mode need not use padding
-

End of Segment