Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 1 of the attack:
Set $c_0' = c_0 \oplus (0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "no error".

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 1 of the attack:

Set $c_0' = c_0 \oplus (0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "no error".

Set $c_0' = c_0 \oplus (0000 \mid 0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "no error".

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 1 of the attack:

Set $c_0' = c_0 \oplus (0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "no error".

Set $c_0' = c_0 \oplus (0000 \mid 0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "no error".

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "no error".

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 1 of the attack:
Set $c_0' = c_0 \oplus (0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "no error".

Set $c_0' = c_0 \oplus (0000 \mid 0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "no error".

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "no error".

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0000 \mid 0001 \mid 0000 \mid 0000 \mid 0000 \mid 0000)$.
Submit c_0', c_1 for decryption.
Response comes back "error".
Now we know there are 5 bytes of padding in m_1.

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 2 of the attack:
What does it take to create 6 bytes of padding?
$0110 = 0101 \oplus 0011$

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 2 of the attack:
What does it take to create 6 bytes of padding?
$0110 = 0101 \oplus 0011$

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0001 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = \quad 1011 \mid 1100 \mid 0011 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "error".

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 2 of the attack:
What does it take to create 6 bytes of padding?
$0110 = 0101 \oplus 0011$

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0001 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = \quad 1011 \mid 1100 \mid 0011 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "error".

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0010 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = \quad 1011 \mid 1100 \mid 0000 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "error".

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 2 of the attack:
What does it take to create 6 bytes of padding?
$0110 = 0101 \oplus 0011$

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0001 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = 1011 \mid 1100 \mid 0011 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "error".

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0010 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = 1011 \mid 1100 \mid 0000 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "error".

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = 1011 \mid 1100 \mid 0001 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "error".

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 2 of the attack:
What does it take to create 6 bytes of padding?
$0110 = 0101 \oplus 0011$

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0001 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = 1011 \mid 1100 \mid 0011 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "error".

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0010 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = 1011 \mid 1100 \mid 0000 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "error".

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = 1011 \mid 1100 \mid 0001 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "error".

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0100 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = 1011 \mid 1100 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "no error".

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 2 of the attack:
What does it take to create 6 bytes of padding?
$0110 = 0101 \oplus 0011$

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0100 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = \quad 1011 \mid 1100 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "no error".

Padding Oracle Attack Example

For the purpose of the example, let's assume the CPU processes 4 bit words. It will save some typing. That is, all values are represented using 4 bits, and XOR is performed on 4 bit values. Let's assume a block length of 8 words (32 bits).

Suppose the adversary holds ciphertext c_0, c_1, encrypting the message $m_1 = 1011 \mid 1100 \mid 0010$.

This gets padded to become:
$1011 \mid 1100 \mid 0010 \mid 0101 \mid 0101 \mid 0101 \mid 0101 \mid 0101$

Step 2 of the attack:
What does it take to create 6 bytes of padding?
$0110 = 0101 \oplus 0011$

Set $c_0' = c_0 \oplus (0000 \mid 0000 \mid 0100 \mid 0011 \mid 0011 \mid 0011 \mid 0011 \mid 0011)$.
$m_1' = \quad 1011 \mid 1100 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110 \mid 0110$
Submit c_0', c_1 for decryption. Response comes back "no error".

We now know that $B \oplus 0100 = 0110$.
Therefore: $B = 0110 \oplus 0100 = 0010$