Born to Learn

October 29, 2016 #CTF | #Forensics | #Crypto

HITCON 2016 - Hackpad

In cryptography, a padding oracle attack is an attack which is performed using the padding of a cryptographic message.

# Problem

> Hackpad
> 65 Teams solved.
>
> Description
> My site was hacked. The secret was leaked.
> hackpad.pcap.xz
>
> Hint
> None

# Solution

Load the pcap file in Wireshark. It contains series of HTTP requests. Most of the response codes are 500s with some 200s in between. Below are some examples.

```
GET /
200 OK: encrypt(secret): 3ed2e01c1d1248125c67ac637384a22d997d9369c74c82abba4cc3b1bfc65f0

POST /
msg=3ed2e01c1d1248125c67ac637384a22d997d9369c74c82abba4cc3b1bfc65f02...
```

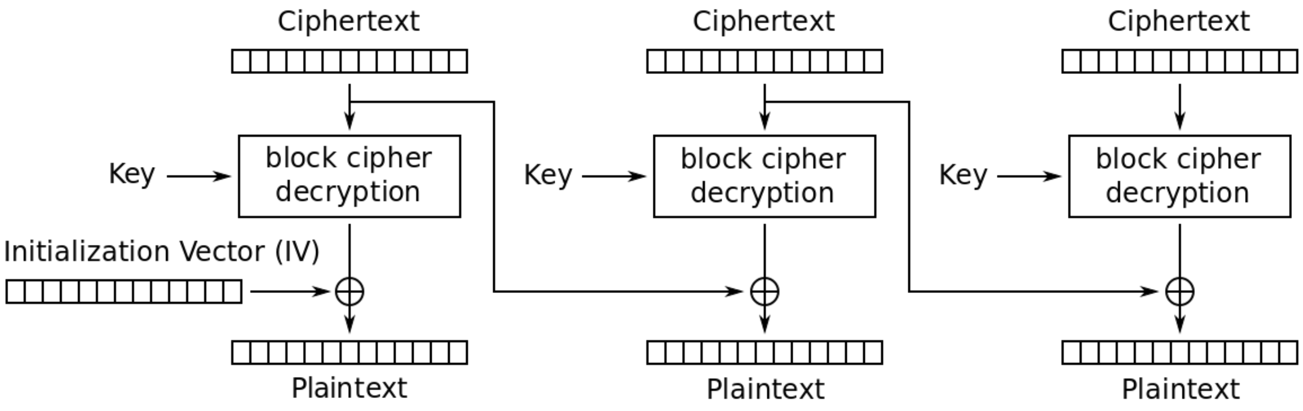
```
200 OK: md5(decrypt(msg)) = e5d3583f3e05b9242a1933fd5d245200

POST /
msg=000000000000000000000000000000ff997d9369c74c82abba4cc3b1bfc65f02
500 Internal Server Error

POST /
msg=000000000000000000000000000000fe997d9369c74c82abba4cc3b1bfc65f02
500 Internal Server Error

POST /
msg=000000000000000000000000000000fd997d9369c74c82abba4cc3b1bfc65f02
500 Internal Server Error

...

POST /
msg=67acd06f7f7b28762310ce1213fccb11997d9369c74c82abba4cc3b1bfc65f02
200 OK: md5(decrypt(msg)) = d41d8cd98f00b204e9800998ecf8427e
```

It’s pretty easy to guess what the server was doing:

1. It returns encrypted message on GET request
2. It decrypts the message in POST request and returns hash of plain message.
3. However, if the encrypted message in the POST request was malformed, it returns 500 Internal Server Error.

This is a typical Padding Oracle Attack.

In CBC mode decryption: $P_i = D(C_i) \oplus C_{i-1}$ where $C_0 = IV$.



Cipher Block Chaining (CBC) mode decryption

We know `67acd06f7f7b28762310ce1213fccb11997d9369c74c82abba4cc3b1bfc65f02` is a valid encrypted message, it’s padding is `10101010101010101010101010101010`. As a result:

D(`997d9369c74c82abba4cc3b1bfc65f02`) ⊕ `67acd06f7f7b28762310ce1213fccb11` = `10101010101010101010101010101010`

P_1 = D(`997d9369c74c82abba4cc3b1bfc65f02`) ⊕ `3ed2e01c1d1248125c67ac637384a22d`

Let’s give it a quick try.

```
>>> a = 0x67acd06f7f7b28762310ce1213fccb11 ^ 0x10101010101010101010101010101010 ^ 0x3ed2e
>>> hex(a)[2:-1].decode('hex')
'In cryptography,'
```

Well, seems like we’re on the right track. The rest is simply cutting the original encrypted messages into 16 bytes blocks and xor-ing it with the first block of every successful padding oracle attack result.

You can use `strings hackpad.pcap | grep msg=` to extract all messages and do some pre-processing to get a list of succesful padding oracle attacks.

```
In cryptography,
 a padding oracl
e attack is an a
ttack which is p
erformed using t
he padding of a 
cryptographic me
ssage.
hitcon{H4
cked by a de1ici
0us pudding '3'}
```

Flag: `hitcon{H4cked by a de1ici0us pudding '3'}`

Credits to team member @jina.

0 Comments **jiulongw** 1 **Login**

♡ **Recommend** **Share** **Sort by Best**

Start the discussion…

Be the first to comment.

Subscribe **Add Disqus to your site Add Disqus Add** **Privacy**