CBC Byte Flipping

September 12, 2018

1 Mathematics of CBC

These are notes as to how byte flipping works. The mathematical formula are as follows.

$$P_i = D_K(C_i) \oplus C_{i-1}$$

$$C_i = E_K(P_i \oplus C_{i-1})$$

$$C_0 = IV$$

Therefore to break it we can represent it as :

$$P' = D_K(C_n) \oplus C'$$

$$C_n = E_K(P_n \oplus C_{n-1})$$

Where C' is block with the flipped bytes, C_n is the block that is used to be decypted and xored with C' to form P'.

Combining the two formulas,

$$P' = D_K(E_K(P_n \oplus C_{n-1})) \oplus C'$$

Simplifying it,

$$P' = P_n \oplus C_{n-1} \oplus C'$$

Notice that we have the ciphertext when we intercept or are presented with one.This means we can know and determine what the values of C_n and C' is. Here P_n is what we are looking for according to the padding rule. This means all we need to find out from the equation is P'.Here, we will know if the padding is correct or wrong according to the pading oracle(a program that will tell us if padding is right or wrong).

2 Last Word Algorithm

We have the simplified formula:

$$P' = P_n \oplus C_{n-1} \oplus C'$$

which when P' is equals to the padding, we can retrieve the plaintext since C' and C_{n-1} and P_n are known. All we need to do is to try out value from 0 - 255 for C' (The block we want to hack). So

$$P'[K] = P_n[K] \oplus C_{n-1}[K] \oplus C'[K]$$

where K is the last byte and that $P'[K] = 0\text{x}1$. Rearranging this formula with $P'[K] = 0\text{x}1$, we get,

$$P_n[K] = 1 \oplus C_{n-1}[K] \oplus C'[K]$$

leaving only the plaintext as the unknown!

All we need to do is to repeat for the every subsequent letter until we have decoded a block. So lets go on to the next plaintext letter, we will need wait for $P'[K]$ to return two 0x02s as padding when we mess with $C'[K]$. This will give us:

$$P_n[K-1] = 2 \oplus C_{n-1}[K-1] \oplus C'[K-1]$$

and so on for $P_n[K-2], P_n[K-3] \cdots$

3 References

1. https://www.youtube.com/watch?v=pEdGUSGi1iM

2. https://www.youtube.com/watch?v=QhuUvrrGJbE

3. https://resources.infosecinstitute.com/cbc-byte-flipping-attack-101-approach/