Programming: Padding Oracle Attack

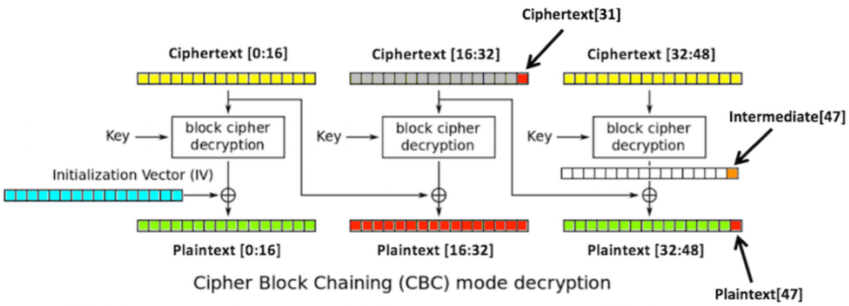
•NTNU : http://140.122.185.210:8080/oracle/xxx

•Reference : https://samsclass.info/141/proj/p14pad.htm

作法:

將 ciphertext 分成 9 組，其中第一組為加密後回傳的 IV，後面 8 組是我們真正想要解出來的 ciphertext，因為 block cipher 的加密方式會把上一個 block 加密後的結果和下一個 block 的 plaintext 經過 AES(DES 或任意加密法) 加密後所得到的值做 XOR 依序下去，所以我們每次都將 c1 和 c2 送進去。

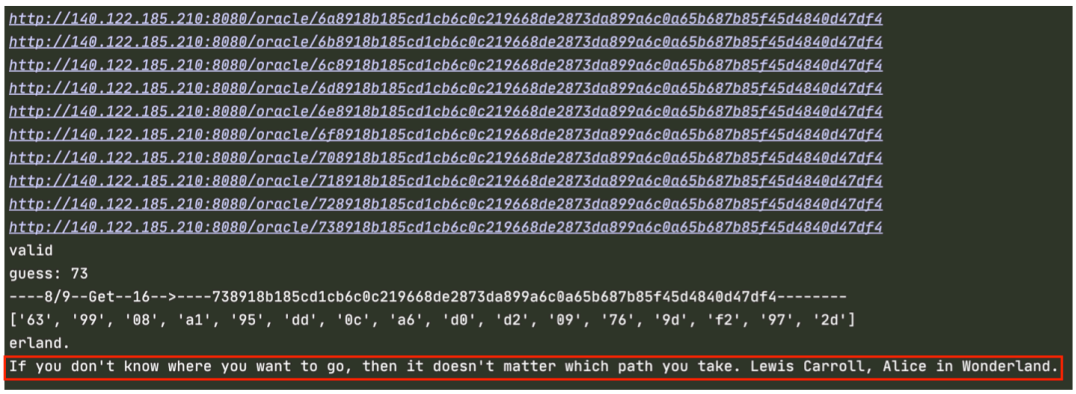
並對 c1 的每個位置先都設成 0 甚至是任何數，因為我們並不需要他，甚至不希望他干擾我們的猜測，只是由 c1 最後一個 byte 開始依序做猜測，目的是希望透過 Oracle 解密時查看送回來的 ciphertext 經過解密後最後所產生的 padding 結果是否符合 padding 規則且 padding 值為正確(由 0x01 至 0x16)的資訊，我們就可以猜出 c1 在該位置應該填入的值，並將此值和 padding byte 做 XOR 來找出 $D_k(C_2)$，所以透過此公式 $\begin{cases} P_i = D_k(C_i) \oplus C_{i-1} \\ D_k(C_i) = C_{i-1} \oplus Pbyte \end{cases}$ 我們就能依序解出整個 plaintext。



以此圖舉例:

我們想破解 C2: ciphertext[32:48]找出 P2: plaintext[32:48]，此時將先對 C1:ciphertext[16:32]設成全零並從最後一個 byte 將 0 到 255 依序填入 ciphertext[31] 猜測，並對 ciphertext[16:32]+ ciphertext[32:48]進行 Oracle，如果回傳的是 valid 代表我們找到 ciphertext[31]應該填入的猜測值使得解密後 padding 結果為 valid，此時我們透過將 ciphertext[31]和 padding byte 做 XOR 即可得到 Intermediate[47]，當 我們得到 Intermediate[47]，這時候要進行下一輪之前，我們必須將 C1 的最後一個 byte 設為我們已知的 Intermediate[47]和下

一個 padding byte 的 XOR 值，才接著 把 C1 的 ciphertext[30]做填值和 C2 送入 Oracle，解出下一個 Intermediate[46]，如 此一來當我們解出整個 Intermediate[32:48]後，將 Intermediate[32:48]和 ciphertext[32:48]做 XOR 即可得到 plaintext[32:48]。



在解密過程中，因為 sever 是老師提供的並且在學校的網域，所以發現如果使用非學校的網路會解到一半就被擋下來，所以非常困擾，因為會沒辦法 Debug，如果有一樣的問題必須使用 VPN 連學校網域，雖然網速慢了點，但至少可以好好的 Debug 把程式刻出來之後，再找時間來學校一次跑完。