Faculty of Engineering and Technology

Electrical and Computer Engineering Department

INFORMATION SECURITY AND COMPUTER NETWORK LABORATORY ENCS5121

Report II

Experiment # 2: Padding Oracle Attack

Student Name: Yara Darabumukho

Student Number: 1211269

Instructor: Dr. Ahmad Alsadeh

Teaching Assistant: Eng. Tariq Odeh

Section No: 1

Date: 30/10/2024

Abstract

In this experiment the main aim is to understand and apply the padding and learn about the Padding Oracle Attack.

Table of Contents

Table of Figures

Table of Tables

Plaintext

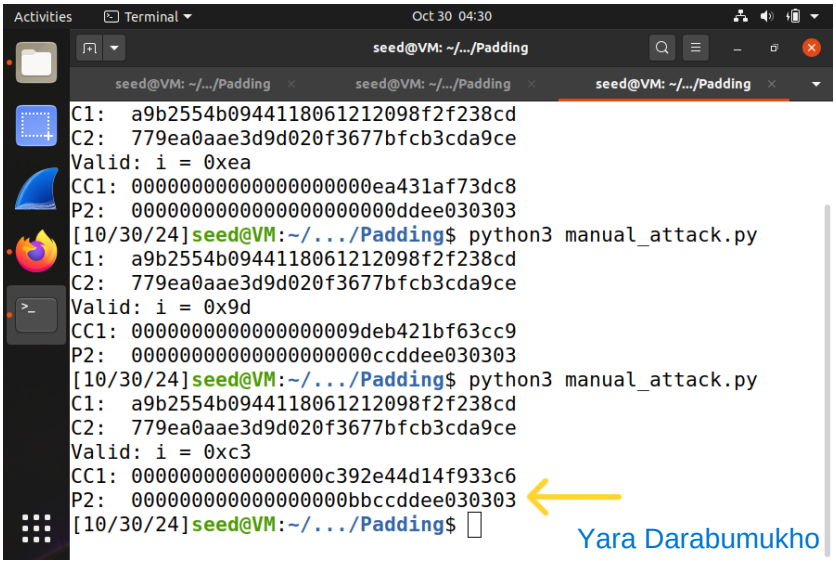

Figure 1: Plaintext.

As shown in the previous figure, the last 7-bytes of the plain test is:

0x**********bbccddee030303

From the plaintext we can notice that the padding done for 3-bytes only, that's mean the encrypted block contains 13-Bytes.

Block Cipher (D)

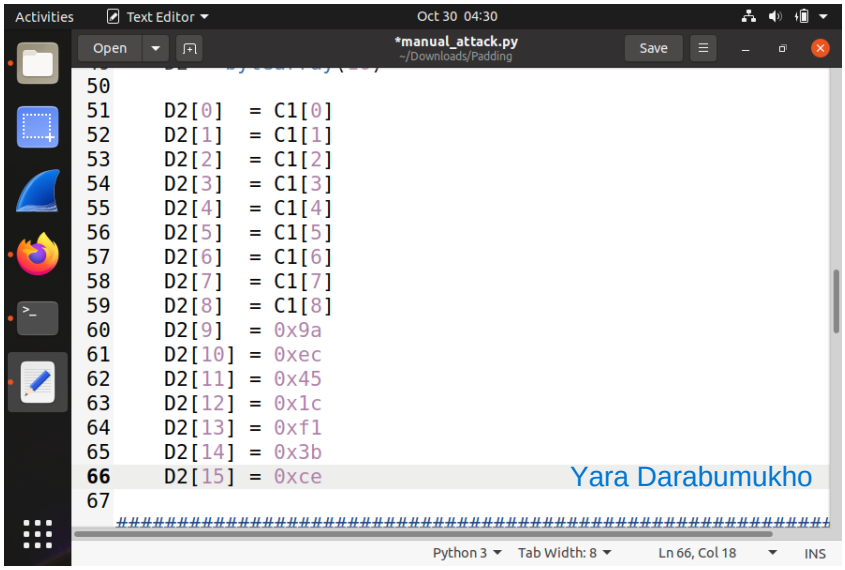

Figure 2: Block Cipher Values.

We get one value of the Block Cipher data in each iteration; after running the code we got a valid value, after that we just find the result of xoring this valid value with the iteration number "Key number".

This is the valid value for Key equal to 7. "Seventh iteration"

```
C1:   a9b2554b09441180612120 98f2f238cd
C2:   779ea0aae3d9d020f3677bfcb3cda9ce
Valid: i = 0x9d ←        Yara Darabumukho
CC1:  00000000000000000009deb421bf63cc9
P2:   00000000000000000000ccddee030303
```

Figure 3: Valid Value.

- ⇨ Valid value from the last figure is 0x9d if u check the value of its xoring with the iteration number which is 7 u will get 0x9a. "The value of D2[9] in the Block Cipher Values figure"

CC1 Values

CC1 values in each iteration is the Block Cipher values xoring with the previous iteration number.

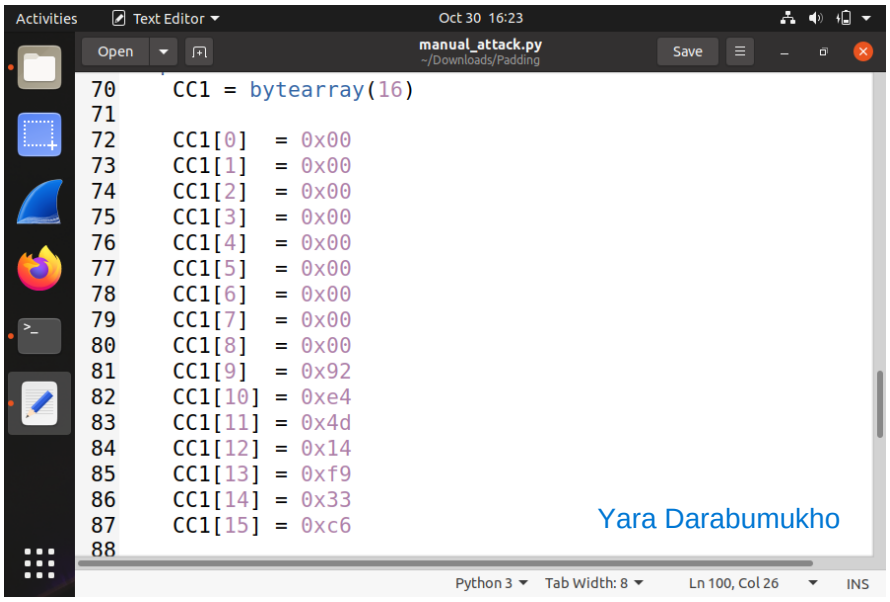

Figure 4: CC1 values for the last iteration.

	K = 1	K = 2	K = 3	K = 4	K = 5	K = 6	K = 7	K = 8
CC1[0]	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x00
…	…	…	…	…	…	…	…	…
CC1[9]	0x00	0x00	0x00	0x00	0x00	0x00	0x00	0x92
CC1[10]	0x00	0x00	0x00	0x00	0x00	0x00	0xeb	0xe4
CC1[11]	0x00	0x00	0x00	0x00	0x00	0x43	0x42	0x4d
CC1[12]	0x00	0x00	0x00	0x00	0x19	0x1a	0x1b	0x14
CC1[13]	0x00	0x00	0x00	0xf5	0xf4	0xf7	0xf6	0xf9
CC1[14]	0x00	0x00	0x38	0x3f	0x3e	0x3d	0x3c	0x33
CC1[15]	0x00	0xcc	0xcd	0xca	0xcb	0xc8	0xc9	0xc6

Table 1: CC1 values.

Let's take K = 4 for example "Which is the Fourth iteration":

- ⇨ From the first Key we got D = 0xce, 0x3b from the second one, and 0xf1 from the third one.
- ⇨ To calculate the values of CC1 we just do xoring for the previous determined values in D with K = 4.