Author: Uzan Moshé Mentor: Arie Haenel 01/05/2017 Version: 2

COURS: THE FOUNDATION OF SOFTWARE SECURITY

RED = DONE

Timing Attack Project 10

The goal of the project it's uses timing measurement to "try" different input with one board, and get the password that will keep by an other board. Also I decided to use TI board for my platform attack and target platform will be Arduino Uno.
For this project I use one TI board and three Arduino Uno (one for each step). I would write, debug and test the program in my Macintosh with these software: Arduino for Arduino Uno, Energia for TI board and Sublime Text for both of them.

1. Step One: Write an algorithm allowing a simple timing attack.
   a) Search documentation on a simple timing attack.
   b) Write a program on the Arduino Uno that keeps a message thanks to a password.
   c) Using a keypad to trying password.
   d) Using a Lcd screen on the Arduino Uno to see if it's the right password or not.
   e) Simulating keypad on the TI to trying password in the Arduino.
   f) Write a program on the TI board that allowing simple temporal attack on the Arduino Uno. (to test)

2. Step Two: Write an algorithm allowing a timing attack in despite of the insertion of a random delay.
   a) Search documentation on a timing attack despite of the insertion of a random delay.
   b) Write a program on the Arduino Uno that keeps a message thanks to a password and with insertion of a random delay.
   c) c) of step 1
   d) d) of step 2
   e) Write a program on the TI board that allowing a timing attack in spite of the insertion of a random delay on the Arduino Uno.

3. Step Three: Write an algorithm allowing a basic timing attack despite an RSA type encryption.
   a) Search documentation on a timing attack despite an RSA type encryption.
   b) Use openssl library for RSA encryption on Arduino Uno, if it's not possible I would write RSA encryption.
   c) Write a program on the Arduino Uno that keeps a message thanks to a password encrypt with RSA.
   d) c) of step 1
   e) d) of step 1
   f) Write a program on the TI board that allowing simple timing attack with password encrypt with RSA on the Arduino Uno.