University of Southampton	School of Electronics and Computer Science	Coursework Instructions
Module Code: ELEC6237	Module Title: Secure Hardware and Embedded Devices	Lecturer: Dr Basel Halak
Deadline: 11/12/2020 At 4 pm	Feedback: 25/01/2021	Weighting: 20%

Learning Outcomes (LOs)

1. To describe the principles of timing-based side channel attacks.
2. To perform security analysis for a given system.
3. To design and verify cryptographic primitives.

Marking Scheme

Criterion	Description	LOs	Total
Section A	Thoroughness of methodology and the accuracy of the solution	1	20%
Section B	Thoroughness of security analysis methodology and the accuracy of the solutions	2,3	40%
Section C	Thoroughness of design methodology and the accuracy of the solution in relation to the specification	2,3	40%

Section A

Timing Attacks are one of the most prominent form of side channel analysis. You are asked to follow a step-by-step the timing-attack tutorial (attached with this document), and answer all questions included in tasks 1, 2 and 3.

Section B

Answer ONE of the following two questions:

Question B-1

In this exercise you will be doing security analysis of a hardware design. Read the detailed system description and answer all the questions that follows:

System description:
The multi-international nature of the IC supply chain has led to a number of security threats, one of which is hardware Trojans. You are now working for a design company has recently bought a firm IP block from a third party. The IP implements a traffic light controller. Your boss suspects that the third party IP provider may have inserted some malicious circuitry in the design which affects his correct behavior and may cause deadly accidents The third party has provided five versions of the design, which are supposed to have identical behavior but different performance and power metrics. You are asked to analyze those designs, then decide if any of which exhibits an abnormal behavior or contains a Trojan. You need to provide experimental evidence for your analysis. You are provided with the following information:

- Detailed description of the expected behavioral specifications of the design in Appendix 1
- HDL library files for AMS 0.35 um technology which was used to implement the design
- A netlist of each version of the traffic light controllers
- The operation frequency of the design is 100 MHz

A tip: If the output of the design is in an illegal state for less than one clock cycle you may assume that this is not caused by a Trojan but by logic delays. So you can treat such behavior as unsuspicious.
Based on the above description, answer all the questions below:

- Explain using experimental supportive evidence whether or not the design (v1) has a hardware Trojan.
- Explain using experimental supportive evidence whether or not the design (v2) has a hardware Trojan.
- Explain using experimental supportive evidence whether or not the design (v3) has a hardware Trojan.
- Explain using experimental supportive evidence whether or not the design (v4) has a hardware Trojan.
- Explain using experimental supportive evidence whether or not the design (v5) has a hardware Trojan.

Question B-2
In this exercise, you will be carrying security analysis of a smart home implementation provided by an imaginary company called "TRUSTME". You will be given a high level description of the system, which you will use to identify any security risks that might be present. Read the description below and provide answers to all the questions that follows.

System Description
This implementation of smart home consists of three subsystems:

- *Control points* which interact with the end users and issue the commands, in this case this consists of a smart home application called (*HomeApp*), which is installed on two devices an i-PHONE 5c and a SAMSUNG Galaxy Tab A 10.1.
- *Smart Devices*: in this case, this include
  1. A security camera, which allows live monitoring and intruder's detection. This device consists of a motion detection sensor, a control system (implemented using a *Raspberry-Pi*), a storage memory, and camera. The device is connected to both the home Wi-Fi network and to the GSM mobile phone network. It operates in two mode:
     a. Non-Intrusion (i.e. motion detector is not activated): the device transmits a live stream, which can accessed form the (*HomeApp*).
     b. Intrusion mode: which is activated if a movement is detected, in which case, in addition to live streaming, the device will place the captured images in the local storage (for further investigations) and will send a text message to the user's phone, to alert them of the intrusion.
  2. A smart speaker device such as that described in the lecture.
  3. Smart bulbs which can be switched on/off remotely using the *HomeApp*
  4. A smart heating system which can be controlled remotely using the *HomeApp*
  5. A smart fridge, embedded with an artificial intelligence technology that is capable of identifying all the types of food stored in the fridge and their corresponding quantities. Such information can be accessed through the *HomeApp*. In addition, the user can turn the fridge on/off and control its temperature remotely.
- The Hub which relays communications between the smart devices, the control points and the cloud.
  Communication between the smart devices/control points and the HUB is conducted using the Wi-Fi technology. The Hub is connected to the internet via Ethernet.

The TRUSTME Company collects all the information captured from the deployed devices for analysis to improve their products. Such information will not include users' private data (e.g. names), but will include home addresses.

Note that you are allowed to make assumptions about the implementation/functionality of the system's components of that systems that have not be explicitly mentioned above. Please make sure such assumptions are plausible, and documented clearly in your analysis.

Based on the above description, answer all the questions below:

- Draw a Data Flow Diagram, using the suggestions and guidance from the lecture notes, which shows the system on a level that is appropriate for meaningful threat analysis.
- Identify ten assets in the system, and justify your choice in each case.
- For each asset you have chosen, identify one security threat, based on the STRIDE model, explaining how such threat might materialize (i.e. give example of a relevant security attack technique when possible).
- For each identified security threat, provide a possible countermeasure.

Section C

Answer ONE of the following two questions:

Question C-1

Galois fields mathematics form the basis of a number of modern ciphers including AES, you are required to design a circuit to multiply two element of $GF(2^3) = Z_2[X]/X^3 + X + 1$ modulo the primitive polynomial. The circuits should have two 3-bit data inputs and one 3-bit data output

Describe the above multiplier using a hardware description language (HDL) language (e.g. System Verilog, Verilog, VHDL...).

Please note the design should be synchronous. So you need to include a clock and a synchronous reset inputs to your design.

- Explain how you designed your circuit in order to meet the specifications with appropriate supportive evidence (e.g. simulations)
- Is your design vulnerable to timing analysis attacks? Explain your answer.

Question C-2

Develop an implementation of a mini AES encryption system using in C, C++, Python or any other programming language. **Please note you cannot use HDL languages in this exercise**

The operation of this algorithm is explained in the document "*miniAES.pdf*" provided with this coursework.

- Explain how you designed your algorithm in order to meet the specifications with appropriate supportive evidence (e.g. simulations)
- Is your design vulnerable to timing analysis attacks? Explain your answer.

What to submit

1. Your completed answer sheet with the specific structure provided with the coursework. Your answer sheet will need to be submitted in PDF format.
2. A Zip folder containing ALL HDL, C code or other source files you have written or used to complete this assignment

Please note failure to submit sufficient evidence to support your solutions will lead to loss of marks

Late submissions will be penalised at 10% per working day. No work can be accepted after feedback has been given.

Academic Integrity (AI)

Plagiarism will be tested in the usual rigorous manner. If you are suspected of an academic integrity breach (e.g. copying solutions or source files), you will be invited to a meeting with course leader, during which you will have to explain your solutions, you may also be asked other questions form the course to assess your general understanding. Your case may be escalated to the AI officer who can decide on an appropriate punishment. This could lead to a mark of zero on this coursework or a termination of study in more serious cases. For more details on this, please refer to the University regulations regarding academic integrity.

Appendix 1

This section explain the expected normal behaviour of the traffic light controller

The design is supposed to control two set of traffic lights deployed at four-way intersection with the main street going east-west and a side street going north-south. Each set contains three lights (Green, Yellow and Red) as shown in figure 1.

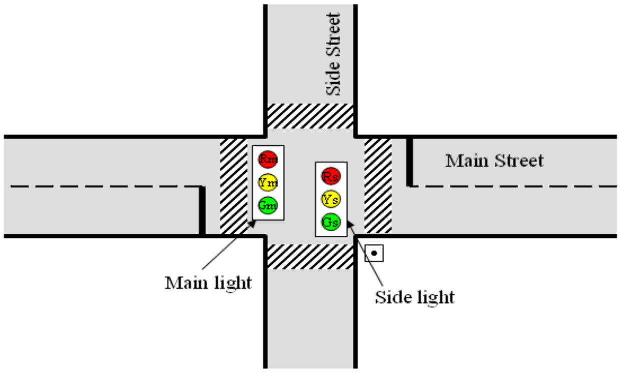

Figure 1: Diagram of four-way intersection

The traffic controller has two inputs clock (clk) and clear (clr) and one output (lights) which control the lights. The normal behaviour of the design is shown using the sate machine graph in figure 2 where count is an internal parameter. It can be described as follows: The design should be first reset to the default state (S0) by providing a pulse on the input clear (the width of the pulse last approximately 2 clock cycle). The design stays in state (S0) for 16 clock cycle (a functionality achieved using an internal counter (count)), then it moves to state (S1) and stays for 4 clock cycles and so on.

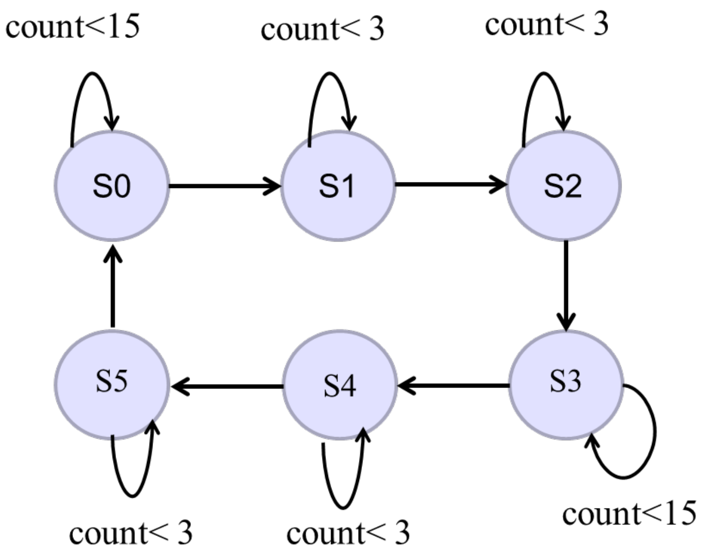

Figure 2: State Machine Graph of the traffic light controllers

The expected output of the traffic light controller in each of these states is summarised in Table 1

Table 1: The expected outputs of the traffic light controller

State	Output (lights)	Main street lights	Side Street Lights
S0	100001	Red	Green
S1	100010	Red	Yellow
S2	100100	Red	Red
S3	001100	Green	Red
S4	010100	Yellow	Red
S5	100100	Red	Red