# Cardiff School of Computer Science and Informatics

## Coursework Assessment Pro-forma

**Module Code**: CMT310
**Module Title**: Developing Secure Systems and Applications
**Lecturer**: Dr Neetesh Saxena
**Assessment Title**: Technical Report
**Assessment Number**: 1
**Date Set**: 5 October 2019
**Submission Date and Time**: 11 November at 9:30am
**Return Date**: 9 December 2019

This assignment is worth **40%** of the total marks available for this module. If coursework is submitted late (and where there are no extenuating circumstances):

1. If the assessment is submitted no later than 24 hours after the deadline, the mark for the assessment will be capped at the minimum pass mark;
2. If the assessment is submitted more than 24 hours after the deadline, a mark of 0 will be given for the assessment.

Your submission must include the official Coursework Submission Cover sheet, which can be found here:

https://docs.cs.cf.ac.uk/downloads/coursework/Coversheet.pdf

## Submission Instructions

All submission must be via Central Learning. Failure to do so will incur in a penalty. Each submission must have the following submitted files:

| Description | | Type | Name |
|---|---|---|---|
| Cover sheet | Compulsory | One PDF (.pdf) file | [student number].pdf |
| Report | Compulsory | Only One PDF (.pdf) or Word file (.doc or .docx) | CMT310_[student number].pdf/doc/docx |

Incomplete submission (missing the report): the final mark will be 0/100.
Not following the structure of the report (mentioned on page 2): the mark awarded will reduce by 10%.

Staff reserves the right to invite students to a meeting to discuss coursework submissions

## Assignment

**INSTRUCTIONS**
Consider yourself employed with an organisation established and working in a specific domain (such as IT, healthcare, banking, smart grid, social network, etc.). You can choose **ANY ONE** of the domains for this work. You are free to choose **ANY ONE** of the following topics to explore the current state of cyber security:

- Ransomware attacks in practice
- Data breaches in practice
- Online financial scams in practice
- Critical infrastructure attacks in practices

**STRUCTURE OF THE REPORT**
Once you have chosen a topic to work on, you need to complete both tasks as mentioned below as a **single report of 2000 words** (maximum, including all except references). There should not be any appendix attached or included to this report.

**Task-1:** ***[Indicative length, 1000 words]***
**Goal: Validation -** "Are we trying to make the right thing?", i.e., is the product specified to the user's actual needs?

- **(T1.1)** Consider any TWO variants of the attack (or any TWO attacks scenarios in the system). ***[Indicative length, 700 words]***
  **(a)** Narrate both scenarios and highlight the associated risk in each scenario (as text)
  **(b)** Analyse ONE security vulnerability and ONE threat in each scenario (as text)
  **(c)** Suggest and discuss any ONE suitable security control for each scenario. (as text)
- **(T1.2)** Create a flow chart to show the overall flow of the secured system. (Clearly show the flow of data along with validation of the suitable security control(s); consider both scenarios/variants as a part (attack) of a single system). (as a diagram) ***[Indicative equivalent length, 300 words]***

**Task-2:** ***[Indicative length, 1000 words]***
**Goal: Verification -** "Have we made what we were trying to make?", i.e., does the product conform to the specifications?

- **(T2.1)** Develop (design) a cryptographic security protocol (with your choice of cryptosystem), which implements the suggested security controls and defeats both the attack scenarios/variants. (as a diagram). Also, demonstrate with an example the implementation aspect (code) of any ONE security control (e.g., Python code for AES-CBC encryption). ***[Indicative equivalent length, 600 words]***
- **(T2.2)** Critically analyse the verification of the final developed system. (Discuss any TWO security properties that are preserved by the developed protocol) (as text) ***[Indicative length, 400 words]***

**References (any)**

References are not counted in word limit.
**Note:** It is expected you will develop a code by following the secure programming standards.

**HELPING NOTES**

- **Vulnerability:** A weakness in any aspect or feature of a system that makes an exploit possible.
- **Threat:** a potential cause of an unwanted incident, which may result in harm to a system.
- **Attack:** an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
- **Risk:** an intersection of assets, threats and vulnerabilities.
- **Examples:** http://www.ques10.com/p/8993/explain-with-examples-vulnerability-threat-and-att/
- **System or system model:** We consider system model as the system that attackers target for attacks (one of the topics listed).
- A sample example will be provided in one of the lectures for better understanding of what is expected to cover and how to complete the given tasks.

## Learning Outcomes Assessed

This ***individual*** assignment contributes to the assessment of the following Learning Outcomes (LO) 3 and 4 of the unit:
3. Deliver systems assured to have met their security profile using accepted methods and development processes.
4. Critically analyse the formal correctness of software systems

## Criteria for assessment

Credit will be awarded against the following criteria.

| Criteria/aspects | Comments | Available Marks (100) |
|---|---|---|
| **(T1.1) (a)** Narrate both scenarios and highlight the associated risk in each scenario (as **text**) | Explain any TWO attack scenarios or any TWO variants of an attack (such as Ransomware); clearly mention the associated risk attached to the scenarios.<br>[**Pass** – narrate TWO attack scenarios with risks (marks < 4);<br>**Merit** – clearly narrate both scenario with risks inline with a system model (marks 4-5);<br>**Distinction** – clearly narrate both scenario inline with a system model, associated risks and their impact on the system (marks 6-8)] | 8 |
| **(b)** Analyse ONE security vulnerability and ONE threat in both | Security vulnerabilities and threats are listed and detailed inline with the topic chosen<br>[**Pass** – list and explain security vulnerabilities and threats in both scenarios (marks < 7); | 12 |

| | | |
|---|---|---|
| scenarios/variants (as **text**) | **Merit** – clearly explain reasons for such vulnerabilities and name potential threats (marks 7-8);<br>**Distinction** – clearly explain reasons for such vulnerabilities and name potential threats with some specific technical details, such as CVE) (marks 9-12)] | |
| **(c)** Suggest and discuss any ONE suitable security control for each scenario. (as **text**) | Name the security control and explain its working and implementation aspects for each scenario, bearing in mind the usability and user-friendliness.<br>[**Pass** – for each scenario, name the security control and explain what it does (marks < 6);<br>**Merit** – for each scenario, name the security control, clearly explain what it does, how it will mitigate/remove the associated risk (marks 6);<br>**Distinction** – for each scenario, name the security control, clearly explain what it does, how it will mitigate/remove the associated risk, and where you will implement it in the system (marks 7-10)] | 10 |
| **(T1.2)** Create a flow chart to show the overall flow of the secured system. (as a **diagram**) | Clearly show the flow of data along with validation of the suitable security control for both scenarios in the system.<br>[**Pass** – for each scenario, clearly show the flow of data and validation of the suitable security control (marks < 12);<br>**Merit** – for each scenario, clearly show the flow of data and validation of the suitable security control with at least one test case (conditional, expected input, expected output) (marks 12-13);<br>**Distinction** – for each scenario, clearly show the flow of data and validation of the suitable security control with more than one test cases (conditional, expected input, expected output) (marks 14-20)] | 20 |
| **(T2.1)** Develop a cryptographic security protocol, which implements the suggested security controls and defeats both attack scenarios (as a **diagram**). Also, demonstrate with an example the implementation aspect (code) of any | Mention which cryptosystem you have used for developing the protocol; clearly mention notations used and what they refer to; clearly show what pieces of information will be exchanged between the entities of the system. Write a Python code for a security control.<br>[**Pass** – mentioned a name of the cryptosystem used and proper notations used in the diagram, clearly show what pieces of information will be exchanged between the entities. A Python code for ONE security control. (marks < 18);<br>**Merit** – mentioned a name of the cryptosystem used and proper notations used in the diagram, clearly | 30 |

| | | |
|---|---|---|
| ONE security control (e.g., encryption AES-CBC). | show what pieces of information will be exchanged between the entities with added comments. A Python code for One security control with output. (marks 18-20);<br>**Distinction** – mentioned a name of the cryptosystem used and proper notations used in the diagram, clearly show what pieces of information will be exchanged between the entities with added comments and computation details. A Python code for One security control with output and line comments. (marks 21-30)] | |
| **(T2.2)** Critically analyse the verification of the final developed system. (as **text**) | Define any TWO security properties and discuss how these properties are preserved by the developed protocol (hint: by defeating these attacks).<br>[**Pass** – Define any TWO security properties and discuss how these properties are preserved by the developed protocol (marks < 12);<br>**Merit** – Define any TWO security properties and discuss how these properties are preserved by the developed protocol; narrate what an attacker can try (marks 12-13);<br>**Distinction** – Define any TWO security properties and discuss how these properties are preserved by the developed protocol; narrate what an attacker can try; explain how this protocol defeats the attacker’s attempts under the given properties (marks 14-20)] | 20 |

A student is considered “fail” if the total mark obtained in this assessment is less than 50.
Assessment marks award:
Distinction (70-100%)
Merit (60-69%)
Pass (50-59%)
Fail (0-49)

## Feedback and suggestion for future learning

Feedback on your coursework will address the above criteria. Feedback and marks will be returned digitally on 9 December 2019 via Learning Central.

Feedback from this assignment will be useful for attempting any security related master project.