Durham University

Computer Science

Summative Assignment

Module code and title	COMP3657 Security Engineering
Academic year	2022/23
Submodule title	
Coursework title	SE Coursework
Coursework credits	10 credits
Lecturer	Maximilien Gadouleau and Ryan Crosby
Deadline*	Tuesday, May 02, 2023 14:00
Hand in method	Ultra

Additional coursework files	
Required submission items and formats	*Submission: one zip file*

*** This is the deadline for all submissions except where an approved extension is in place. Late submissions received within 5 working days of the deadline will be capped at 40%. Late submissions received later than 5 days after the deadline will received a mark of 0.**

COMP3657 Security Engineering Academic Year 2022-23 Coursework

This coursework is split into three main parts, assessed by Dr Maximilien Gadouleau (part 1) and Dr Ryan Crosby (parts 2 and 3) respectively. The description given here is purposefully short: further details will be provided in an FAQ hosted on Ultra.

Your submission will be on Ultra. You need to upload a unique zip file containing your whole submission.

1 Threat Modelling (MG)

The Newcastle Clean Air (NCA) zone is a policy whereby certain vehicles will have to pay to be allowed to drive in a designated geographical zone located in Newcastle City Centre. We are interested in the whole NCA system (hardware and software) that enforces the policy.

The system needs to authenticate the vehicles driving in the NCA zone, determine whether or not this vehicle is liable to paying a fee, and whether that fee has been paid already. It also needs to issue requests for payments to the vehicle's owner if need be.

In this task, you will act as the security architect of the Newcastle Clear Air system.

1.1 Assumptions (10 Marks)

Make 5 further assumptions about the system, together with their justification. These assumptions may or may not be implemented in the actual NCA system.

Make sure your answer to part 1.1 does not exceed one A4 page.

1.2 Attack tree (10 Marks)

Prepare an attack tree. Include at least 20 nodes in the tree. These nodes should be both general threats (such as protocol failure, wiretapping and alike) and scenario–specific ones (such as social engineering emails and insider threats). Submit the tree in 1 page PDF (it is alright if the page size is larger than A4). Make sure the text in the file is readable and in high resolution.

1.3 Risk assessment (20 Marks)

Prepare a risk assessment on two major threats that will endanger the NCA system.

Explain the risk assessment procedure and your findings in your research and provide your countermeasures. Remember that you need to provide some design assumptions for your assessment. These assumptions should be aligned to the design choices explained above and your own research on how similar technologies work.

The style of the analysis should be technical, rather than verbose. This should be understandable by someone with a good knowledge of the security of the system. Be concise and straight to the point. Make sure your answer to part 1.3 does not exceed 2 A4 pages, including the citations. Appropriate sources include research papers, textbook chapters, lecture notes, etc.

2 Certificate Authority and PKI (RC)

2.1 PKI Infrastructure (20 Marks)

In task two you will create a PKI infrastructure for a new start up company called TechnoWizard. TechnoWizard wants to get a public key certificate from our CA. You are responsible to get that certificate and verify if it works well.

For simplicity, you create digital certificates without going to pay any commercial CA. You should become a root CA yourself, and then use this CA to issue certificate for anyone (including TechnoWizard servers). You are also allowed to register the certificate in a combination including your own name. Therefore, the name used in the TechnoWizard server certificate must contain TechnoWizard, your last name and the current year. The registered URL will be "www. technowizard.com".

Name the CA's public-key certificate and private key as "ca.crt" and "ca.key". Also, the server's public-key certificate and private key should be named as "server.crt" and "server.key".

For this task you will need to submit evidence of your certificate as well as your public keys. Do not submit your private keys.

2.2 Man in the middle (20 Marks)

After you have generated your own certificate authority and the certificates for server, you will be implementing a secure channel between server and client (in presence of a powerful Man-in-the-middle). You should use system A as client, and system B as server. Store the CA's certificate in the "./client-certs"folder on the client device (A) and use it for your handshake requests. Use the python packages"socket" and "ssl" for your implementation (other packages are not allowed to be used).

For this task you should submit all code created and evidence of your successful man in the middle attack.

3 File Integrity (RC)

3.1 File integrity code (10 Marks)

In your assessment folder on blackboard you will find two files given by TechnoWizard. One of these files has been stored on a secure folder and has not been tampered with. The other was stored on an unsecure server and has been tampered. Identify without opening said files, which file has been tampered with.

As with task two you should use python for your code.

Submission requirements are the generated code files.

3.2 File integrity report (10 Marks)

Write a one page report detailing which file was tampered with, how you identified the file and why you created the identification as you did.

Submit files as a PDF.