School of Computing Sciences

Module: CMP-7038B – DEVELOPING SECURE SOFTWARE
Assignment 001: Individual Reassessment

Set by: Debbie Taylor
Contact Email: Debbie.taylor@uea.ac.uk

Date Set: 16 July 2021
Value: 60%
Submission: Blackboard upload

Learning outcomes

- Importance of designing software with security in mind
- Develop a secure and usable website that meets the needs of the user
- Analyse the effectiveness of a range of security methods and tools
- Analyse the evolving range of threats associated with the internet

Specification

Overview

The aim of this assignment is to discuss a variety of authentication methods that can be used to secure systems, as well as to research some common types of malware.

You will create a report which compare three different authentication methods. You will need to use academic literature to research the ways in which these authentication methods work, their accuracy, their usability, and their advantages and disadvantages generally. Your report will additionally need to discuss three types of malware, including the attack vectors and associated risks.

The report will be a **maximum of 12 pages** and must be written using the **UEAcmpstyle LaTeX template with Harvard/APA referencing**, an example has already been uploaded to Blackboard. Any references used must be of good quality and relevant. They will be excluded from the maximum 12-page restriction

Description

Your report will include in-depth academic research into both types of authentication and malware.

Part 1:

This section will discuss types of authentication. At minimum you should research and discuss the following:

- Discuss how two different authentication methods work
- The accuracy of these two methods
- The usability implications of these two methods
- Critical analysis of advantages and disadvantages for these two methods
- *MSc:* Detailed analysis and comparison of *three* other types of authentication methods
- *MSc Only:* Critical analysis of *which* method is best for securing software systems and why

Potential authentication methods include passwords, specific biometrics, and swipe patterns. Part 1 should conclude with a critical analysis of which method would best secure a piece of software.

Part 2:

This section will involve you discussing types of malware. At minimum you should research and discuss the following:

- The common attack vectors for all types of malware
- The basics of how each malware process works e.g. Worms, Viruses, Trojan Horses, and Ransomware
- The risks associated with each type of malware (the damage the malware can cause)
- The threat actors associated with type of malware

Relationship to formative and summative assessment

This assignment builds on the formative work you complete during your weekly lectures and lab sessions

Deliverables

You should upload a PDF copy of your LaTeX report to blackboard

Resources

Lecture notes and previous lab sessions are highly relevant to this work.

UEAcmpstyle LaTeX document has been uploaded to Blackboard.

Erickson J., (2008) *Hacking: The art of exploitation*. 2nd edition San Francisco: No Start Press

• OWASP Top 10 – 2020. Available at: https://owasp.org/www-project-top-ten/

• Anderson R. (2008) Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, and also available on the author's website (https://www.cl.cam.ac.uk/~rja14/book.html)

The DBLP bibliography server (https://dblp.org/) is an excellent resource for most topics (it holds bibliographic data and links to 4.8M computing publications)

A note on use of additional sources and plagiarism

Please note that while use of texts, or online sources, is encouraged in order to learn design and programming principles, use of functions, lists, etc; they are not a substitute for completing the work yourself. It is not appropriate to find solutions or part solutions to assignments and submit

them as your own work. Neither is it allowed to post questions on online forums requesting help or solutions to specific assignment tasks. To do either (copying/requesting) would be in breach of the university's regulations on plagiarism and collusion (General Regulation 18).

In the instances where you do use code (or any other work) copied from any source, you must acknowledge the source (e.g. including a comment with the URL and author alongside the copied sections) If in doubt, approach the coursework setter to discuss what is appropriate

Marking scheme – Individual Reassessment 60%

1st Marker Name	Student Number
Date:	

Marking Details	Mark %	Marking Comments
Part 1: Authentication For each authentication method • How the two methods work – 8 • Accuracy of the two methods – 6 • Usability of the two methods – 7 • Critical analysis of Advantages/disadvantages - 9 • MSc: Method comparisons for three other authentications – 15 • *MSc:* Critical analysis of best authentication system and why - 10	55%	
Part 2: Malware For each malware: • Attack vectors – 6 • How malware works – 16 • Risks – 7 • Threat actors – 6	35%	
Report Writing • Grammar and Spelling – 3 • Structure – 3 • Referencing - 4	10%	

Extra Comments:

Total Score