Northumbria University NEWCASTLE
Newcastle • London • Amsterdam

COURSEWORK ASSESSMENT SPECIFICATION	
Module Title:	Network Security
Module Number:	LD7007
Module Tutor Name(s):	Umair Chaudhry
Academic Year:	2023-24
% Weighting (to overall module):	30% GROUP WORK
Coursework Title:	SSL PKI Implementation & Threat Modelling

Dates and Mechanisms for Assessment Submission and Feedback

Date of Handout to Students: 01/06/24
Mechanism for Handout to Students: Via Blackboard; briefing via online blackboard collaborate and face 2 face session
Date and Time of Submission by Student: Submitted on 29 August 2024 (no later than 16:00)
Mechanism for Submission of Work by Student: The report in electronic format must be submitted Turnitin on Module Blackboard site.
Date by which Work, Feedback and Marks will be returned to Students: Within 20 working days after the submission date.
Mechanism for return of assignment work, feedback and marks to students: Formal feedback will be made available via Blackboard following completion of all reviews and internal moderation of results.

Learning Outcomes tested in this assessment:

The following learning outcomes will be assessed by this assignment:

- Apply appropriate theory, practices, and tools to the design/development of network security solutions.
- Critically evaluate the legal, ethical, and social implications of security

Introduction

In this task you will create a Certification Authority (CA) which will act as a subordinate Enterprise Certification Authority to issue certificate for web communication for an organisation called SELDOM. An offline root Certification Authority is expected to be installed and configured to establish the fundamentals in the PKI architecture to. You will also demonstrate a comprehensive threat modelling. The group is advised to use Windows 2012 server or later release. Groups are free to completely virtualise the testing environment.

Assignment Tasks:

Your work must be presented in the form of a Project Report and be no longer than **4500 words (excl. references, figures, tables and appendices)** plus a facing page that includes the executive summary. This should be typed on A4 paper and use a font size Arial 10 single spacing. For completeness, you may if you wish include additional material in an appendix but this will not contribute to the marks.

Section 1: SSL PKI Design & Implementation

The **technical requirements** are listed as follows:

1. Install and configure an offline Root Certification Authority
2. Configure the appropriate certificate templates of the issuing CA
3. Create a fully operational TLS-enabled Web page
4. Observe encrypted traffic using Wireshark

Section 2: SSL PKI Threat Modelling & Ethical Considerations

The **non-technical Requirements** are listed as follows:

1. **SSL PKI threat model:** Identify the threats, attacks arising from the proposed description of the SSL PKI security issues raised in your design/proposal. Create and discuss a taxonomy of those threats relevant to your design and propose suitable mitigation plans with clear references to the literature. You are required to threat model only against identity spoofing and certificate authority threats using a standardised methodology to identify and rank the threats identified.

2. **Threat Ranking:** Define, adopt, and validate the appropriate method to rank threats in SSL PKI architecture.
3. **Threat mitigation Plan:** A detailed threat mitigation plan is also required as part of your deliverables. Clear evidence of a systematic approach taken to validate threats identified must be clearly articulated as part of your analysis.
4. **PKI Risks:** Critically discuss at least two (2) significant risks/attacks/threats to PKI and link these to privacy (confidentiality/Integrity). What kind of ethical and legal concerns are raised in the context of PKI and identified risks/attacks/threats?

Project Deliverables: Written Group Report (max 3 students per group)

Project Report: The project report should provide your design and recommendations for the planned exercise. Please pay attention to the following points in designing your PKI security solution and preparation of report; at its basic form, the report should be structured as follows:

1. **Executive Summary:** Provide an executive summary [~150 words]
2. **Introduction:** An introduction using appropriate information and problem statement from the team. [~200 words]
3. **SSL PKI Design & Implementation:** In this section you address all technical requirements in Section 1 of the brief with a clear articulation of the process followed to achieve the outcomes requested. [~1500 words, excl. figures, diagrams and tables]
4. **SSL PKI threat modelling & Ethical Considerations:** This section must include a systematic approach on the identification of threats, methodologies used to rank them and a detailed mitigation plan against the threat vectors given in the brief. You should also discuss ethical and legal implications of risks/attacks/threats by the adaptation of PKI. [~2500 words excl. figures and tables]
5. **Conclusion:** Design recommendations, summary of key points/findings from your investigation [~150 words]

IMPORTANT NOTE: The project report must be based on academic references. Please use IEEE explore, ACM, ELSEVIER databases for references related to threat models, security technologies, cloud computing etc. **CAUTION: Merely providing a generic answer without addressing the project deliverables will result in a very low mark. A single file submission must be made ONLY by a delegated group member including any appendices, tables, diagrams, etc (No word limitation for appendices). Feedback will be distributed to all group members as appropriate.**

Assessment criteria:

Important Note: As part of the marking process, the group members must fully complete the peer assessment for each student in the group via Microsoft Forms Survey available via Blackboard. If there are four students in your group you should complete three forms, then you should assess your own performance.

The completed peer assessments award each group member a score out of 100. Every group member is awarded a score out of 100 by the remaining group members. These scores are used to calculate an average teamwork score. The average score is then be used to weight the mark achieved for the group elements of the assessment.

Assessment Criteria Section	Possible marks	Actual Marks
Executive Summary	5	
Introduction	5	
SSL PKI Design & Implementation • Install and configure an offline Root Certification Authority • Configure the appropriate certificate templates of the issuing CA. • Create a fully operational TLS-enabled Web page. • Observe encrypted traffic using Wireshark.	45	
SSL PKI Threat Modeling & Ethical Considerations • SSL PKI Threat modelling approach (threat identification, validation) • PKI security issues relevant to the case with discussion • Threat mitigation plan in the context of SSL PKI • Critical discussion on ethical and legal issues.	35	
Conclusion	5	
References	5	
Marks deducted in case of poorly structured reports, layout, word count (15 marks)		
Total	100	

ASSESSMENT REGULATIONS

You are advised to read the guidance for students regarding assessment policies. They are available online here.

Academic Misconduct

The Assessment Regulations for Taught Awards (ARTA) contain the ***Regulations and procedures applying to cheating, plagiarism, the use of Artificial Intelligence (AI) Systems, and other forms of academic misconduct***.

The full policy is available here

You are reminded that plagiarism, collusion, the use of Artificial Intelligence (AI) Systems, and other forms of academic misconduct, as referred to in the Academic Misconduct procedure of the assessment regulations, are taken very seriously. Assignments in which evidence of plagiarism or other forms of academic misconduct is found may receive a mark of zero.

Late submission of work

Where coursework is submitted without approval, after the published hand-in deadline, the following penalties will apply. For coursework submitted up to 1 working day (24 hours) after the published hand-in deadline without approval, **10% of the total marks available for the assessment** (i.e.100%) **shall be deducted** from the assessment mark.

For clarity: a late piece of work that would have scored 65%, 55% or 45% had it been handed in on time will be awarded 55%, 45% or 35% respectively as 10% of the total available marks will have been deducted.

The Penalty does not apply to Pass/Fail Modules, i.e. there will be no penalty for late submission if assessments on Pass/Fail are submitted up to 1 working day (24 hours) after the published hand-in deadline.

Coursework submitted more than 1 day (24 hours) after the published hand-in deadline without approval will be marked as zero but will be eligible for referral. The reassessment should where appropriate, and as determined by the Module Leader, be the same method (e.g. essay) but maybe with a different task (e.g. different essay title) or with the same task (e.g. the same essay title) as indicated in the Module handbook.

The full policy can be found here

Word limits

The word count is to be declared on the front page of your assignment and the assignment cover sheet. The word count does not include:

Please note, in text citations [e.g. (Smith, 2011)] and direct secondary quotations [e.g. "*dib-dab nonsense analysis*" (Smith, 2011 p.123)] are INCLUDED in the word count.

If this word count is falsified, students are reminded that under ARTA this will be regarded as academic misconduct.

For those assessments where students are required to keep to the word limit, it is proposed that they should be informed that the marker will stop reading at the point when they judge that the word limit exceeds the recommended word count by more than 10%. The marker will indicate the point at which they stop reading on the text.

Students must retain an electronic copy of this assignment (including ALL appendices) and it must be made available within 24hours of them requesting it be submitted.

The full Word Limit Policy is available here

The time allocated for the presentation must be adhered to. At the end of this time, the presentation will be stopped and will be marked based on what has been delivered within the time limit.

Group Work

The group work policy can be found here

e Submission of Work.