STAFFORDSHIRE UNIVERSITY

Module Code:	COMP70035
Title of Assignment:	CRITICAL SYSTEMS AND APPLICATIONS
Assignment Weighting:	PRACTICAL ASSESSMENT - 15 MINUTE PRESENTATION weighted at 80% PRESENTATION - 15 MINUTE PRESENTATION weighted at 20%
Submission Date:	*Shared later*
Learning outcomes	1. Demonstrate a systematic understanding of the current theory and practice of critical systems application development. University Learning outcomes: Knowledge and Understanding, Enquiry 2. Analyse, design, implement, test and prove a software solution to a critical application problem working within a team setting. University Learning outcomes: Application, Analysis, Problem Solving 3. Demonstrate a systematic understanding of system architectures and underlying technologies and protocols used to support critical systems. University Learning outcomes: Knowledge and Understanding, Learning 4. Reflect critically on skills developed during the production and proving of the critical system using industry standard techniques. University Learning outcomes: Communication, Reflection.

1. Coursework Details

Contact: *Dr. Ateeq Ur Rehman, Bob Hobs, Dr. Tharaka*
Assessment weighting:

1. PRACTICAL ASSESSMENT - 15 MINUTE PRESENTATION weighted at 80%
2. PRESENTATION - 15 MINUTE PRESENTATION weighted at 20%

2. Notes on Plagiarism

- Your report must have citations and the references should be in Harvard style. You are recommended to use a referencing tool e.g. Mendeley, Zotero etc.

- You are expected to explain the concepts in your own words or rephrase and avoid quotes. You are referred to the University's regulations on plagiarism available at https://www.staffs.ac.uk/students/course-administration/academic-policies-and-regulations/academic-conduct-procedure

  If the Turnitin system detects plagiarism, it will be reported to the school and appropriate actions will be taken.

3. Fundamental Guidelines and requirements

In this assignment, you must satisfy **all** the following fundamental requirements, otherwise you could be awarded zero marks for the assignment

- You must be the only author of the work you submit for assessment. You must not have help with this assignment from any person except for members of the regular teaching team. You are reminded of the university's policy about academic misconduct, as described at: http://www.staffs.ac.uk/support_depts/info_centre/handbook/academic-life.jsp
- During the demonstration, if asked, you must be able to explain in detail the software you present for assessment.
- You must submit your assignment via this module's Blackboard presence using the link provided in the Assessment section. Follow the instructions given with the link.
- See University Regulations at https://www.staffs.ac.uk/students/course-administration/academic-policies-and-regulations/academic-conduct-procedure
- Ensure that all work submitted is original and your own. Plagiarism will not be tolerated and will result in a fail grade for the assessment.
- **See University Regulations at** http://www.staffs.ac.uk/assets/Procedure%20for%20Dealing%20with%20Breaches%20of%20Assessment%20Regulations-Academic%20Misconduct%202016-17%20v1_tcm44-91272.pdf

- Use industry-standard software and tools for design, modelling, and validation.
- Follow best practices in software engineering and project management.
- Make sure all reports and presentations are professionally formatted and free of grammatical and typographical errors.

4. Support and Resources:

- Access to university libraries and online databases for research and reference.
- Workshops and tutorials on system design, modelling, and validation techniques.
- Office hours and consultation sessions with instructors for guidance and feedback.
- Access to software tools and development environments necessary for the project.

5. Submission Instructions:

- All submissions are done using the link provided on the module assessment menu in Blackboard
- All reports / designs must be uploaded in word or PDF format and readable on a PC
- All zipped files must be in a compressed format (such as .zip, .rar, .7z, etc.)
- All links must be available to staff until results are released (when you have received your official result for the module) unless this would cause hardship in which case you will need the module leader's permission to unmount the work
- Standard submission rules apply:
  - Late submissions attract ZERO marks for that section
  - Failure to submit on Blackboard may forfeit your opportunity to present or demonstrate your work
  - Failure to attend the presentation or demonstration on time may result in 0 marks for that component of assessed work

6. PART 1 of the Assessment: 80% weight (LO 1-3)

Scenario:

"Designing a Secure Online Banking Authentication System with Basic Fraud Detection"

As financial transactions become increasingly digital, banks must ensure secure systems exist to protect customer assets and maintain trust. In this assessment, you will analyse security risks in online banking, design a secure authentication system, and model basic fraud detection rules to create a prototype application that simulates user access to online banking facilities.

The final submission will include system modelling, a limited-scope prototype, and a presentation explaining design choices and risk mitigation strategies.

You are required to demonstrate business-critical system design principles while considering secure programming, validation, and professional standards.

The proposed system must include the following aspects relating appropriately to front-end and back-end functionality.

Assessment Tasks & Module Content Coverage

1. Problem Analysis

- Investigate key cybersecurity challenges in online banking
- Identify business risks of system failures and security breaches.
- Determine legal and ethical concerns, including financial compliance, data protection laws, and inclusive system design.

2. System Design

- Develop an authentication system architecture using secure architectural patterns (e.g., MVC for front-end, REST APIs for backend).
- Justify design choices in terms of business continuity, scalability, and security.
- Apply secure programming principles, including encryption, token-based authentication, and multi-factor authentication (MFA).
- Employ clean coding principles such as SOLID principles and software design patterns

3. System Modelling

- Create UML diagrams (e.g., use case, sequence, and entity-relationship diagrams) illustrating system behaviour.
- Define data models for storing user credentials, login attempts, fraud detection logs, and other relevant audit trails.
- Describe communication models (e.g. protocols), ensuring secure data transmission and API interactions.

4. Fraud Detection

- Propose basic fraud detection rules, such as:
  - Flagging multiple login attempts from different IP addresses in a short time.
  - Detecting transactions outside usual geolocations.
  - Any other relevant indicators of fraudulent activities.
- Use geospatial modelling to demonstrate how the system could track unusual banking activity.
- Implement a basic rule-based fraud detection system.

5. System Validation & Security Testing

- Perform conceptual validation of the security model (e.g., simulating cyberattacks, testing authentication failures).
- Outline how vulnerabilities could be identified and mitigated through testing.
- Conduct a peer review process, ensuring the system meets business-critical security standards.

6. Presentation & Demonstration

- Deliver a 15-minute presentation, explaining:
  - The identified business needs.
  - System design and security mechanisms.
  - Fraud detection models and geospatial risk mitigation.

    - Legal, ethical, and professional standards applied.
- Showcase a simple prototype demonstrating secure login and fraud detection logic.
- Justify how the system enhances business security and customer trust.

Assessment Deliverables

1. **System Analysis Report**
    - Risk analysis, system architecture, and fraud detection model.
    - Explanation of business-critical and safety-critical elements.
    - Compliance with legal and professional standards.
2. **System Modelling**
    - UML diagrams (use case, sequence, and ERD).
    - Data modelling and communication model diagrams.
3. **Prototype Implementation**
    - A working prototype demonstrating secure login with multi-factor authentication.
    - Basic rule-based fraud detection logic (conceptual validation acceptable**).**
4. **Presentation & Demonstration**
    - Clear articulation of system design, security considerations, and business impact.
    - Justification of security choices and fraud detection approach.

Marking Criteria for Part 1 Practical Artefact:

Component	Marks	Criteria
Problem Analysis	20%	Clarity and completeness of problem statement
		Depth of understanding of the business-critical problem
		Use of appropriate theory and practices
System Design and Modelling	25%	Quality and appropriateness of system design
		Accuracy and detail of models
		Consideration of scalability, reliability, and security
		Demonstration of innovation and problem-solving skills
System Implementation	30%	Functionality and performance of the prototype
		Thoroughness and accuracy of test cases
		Evidence that the prototype meets requirements
		Adherence to industry standards and best practices
Presentation	25%	Clarity and professionalism of presentation
		Depth of knowledge and research.

Component	Marks	Criteria
		Coherence and relevance to the report and prototype

7. Part 2: Presentation Assessment (20%) (LO-4)

Students will present for 15 minutes, demonstrating their understanding related to their practical artifact and the skills they have developed in its creation.

Tasks:

- Reflect critically on the skills developed during the project
- Outline the application of safety-critical and business-critical principles to the prototype system.
- Assess the system's performance in handling critical requirements using industry-standard techniques.
- Use visual aids such as slides, diagrams, and live demonstrations of the prototype to support the presentation.

Requirements:

- A 15-minute presentation, either live demonstrating the project outcomes.
- Presentation slides and any supporting materials.

Submission Requirements for Presentation Part 2:

- Upload your presentation to the blackboard via the link provided
- If you have a video demonstration, then upload the link and make sure to provide access for viewing.

Marking Criteria for Part 2 Presentation:

Component	Marks	Criteria
Clarity and Professionalism	20%	Clear and concise explanation.
		Professional delivery and presentation style.
		Use of presentational aids.
Technical Consideration	40%	Identification, exploration and assessment of critical system features.
Critical Reflection	40%	Insightful reflection on the skills developed during the project and the project outcomes.

Assessment Objectives

By the end of this assessment, you will be able to:

1. Analyse risks associated with online banking security and authentication.
2. Design a secure banking authentication system with multi-factor authentication (MFA).
3. Model the system using UML diagrams, system architectures, and data flows.
4. Implement a basic prototype demonstrating user authentication and fraud detection logic.
5. Apply professional and legal considerations, including ethical, privacy, and regulatory compliance (e.g., GDPR, PCI-DSS).
6. Validate security mechanisms conceptually and explain their impact on business continuity.

Good Luck!