Security and Privacy (ELEC0138) Project Assignment

2024/2025

Assignment Issued: February 2025

Guidelines:

All assignment deliverables to be handed in by: **25th of April 2025 4pm** (optional half-page work-plan to be submitted by March 19th 2025 11:59pm for feedback, this piece is not part of the final marks)

Penalties will be applied for late submissions in accordance with the guidelines:

https://wwws.ee.ucl.ac.uk/masters/masters-docs/regulations/late-coursework-penalties

Security and Privacy (ELEC0138) 2024/2025

1. Description:

In this assignment, you will prepare a report titled: "Resilient Security: Threat Modeling and Defensive Strategies for X" This report will be presented to the Chief Security Officer (CSO) of your chosen organization. You will analyze and address security and privacy challenges within a chosen real-world digital environment, highlighting vulnerabilities, simulating realistic attack scenarios, and designing effective defense mechanisms.

The assignment is divided into two interrelated coursework components:

Coursework 1: Threat Modeling & Attack Simulation

Select a real-world digital environment (e.g., smart city, connected healthcare, corporate IT infrastructure, industrial IoT, digital banking, etc.) and conduct a thorough security and privacy assessment.

You should:

1. Define the Scope & Identify Critical Assets
   - Clearly define the environment/system being analyzed.
   - Identify and categorize critical assets (e.g., sensitive data, applications, infrastructure, user access points).

2. Develop a Threat Model
   - Identify at least two major security/privacy threats to your system.
   - Consider threats arising from cyberattacks, insider threats, regulatory non-compliance, or emerging risks (AI, quantum computing, etc.).

3. Impact Analysis & Risk Prioritization
   - Evaluate the likelihood and impact of each threat, considering business, financial, and reputational risks.
   - Use a risk matrix or threat taxonomy to justify your prioritization.

4. Simulate Attacks (Code-based or Tool-based Demonstration)
   - Develop and describe realistic attack scenarios that exploit identified vulnerabilities.
   - Utilize ethical hacking tools, exploit frameworks, or custom scripts to demonstrate potential system compromises.
   - Provide an attack chain analysis, showing how adversaries might infiltrate or manipulate the system.

Coursework 2: Security & Privacy Defense Strategy

Using your threat model from Coursework 1, design and propose a security and privacy defense system to mitigate the identified threats effectively.

1. Design a Resilient Security & Privacy Solution
    - Propose a multi-layered defense approach, incorporating:
        - Access controls & authentication (e.g., Zero Trust Architecture, MFA, behavioral biometrics)
        - Data security & encryption mechanisms (e.g., homomorphic encryption, differential privacy)
        - Network protection & monitoring (e.g., AI-driven IDS/IPS, honeypots, deception technology)
        - Resilience against emerging threats (e.g., adversarial AI, quantum-safe cryptography)

2. Prototype Demonstration
    - Implement a proof-of-concept security feature (e.g., encryption demo, intrusion detection prototype, secure authentication mechanism).
    - Provide code snippets and screenshots.

3. Regulatory Compliance & Ethical Considerations
    - Map your solution against relevant security and privacy regulations (GDPR, CRA, PSTI etc.)
    - Address potential ethical dilemmas, such as surveillance risks, user consent, and AI-driven security concerns.

4. Scalability, Innovation & Enterprise Considerations
    - Discuss how your solution could scale for enterprise-wide adoption.
    - Highlight innovation opportunities, including how your design can differentiate from traditional security methods.
    - Evaluate its long-term viability, cost implications, and future-proofing strategies.

You will work with others on complementing the app/platform, but each individual must submit their own assignment independently, clearly specifying their own contribution and the way it complements that of others'.

2. Submission:

- Submissions: 1 report to be submitted per student, combined PDF of up to 10 pages, one for coursework 1 and one for coursework 2 (up to 5 pages each), using the template on Moodle (ELEC0138Coursework_SN).

- Presentation: up to 5 minutes, demo (hardware/software/app), to be put up on YouTube (or any other publicly available link) and URL link provided in the report.

- Code & Data: link to accessible code (ideally Github, or publicly accessible Dropbox folder), link to data repository.

- The report, presentation, code & data should be identical for each group. However, each student is required to submit the report outlining their individual contribution, with a maximum limit of 200 words (see template).

3. Assessment:

Your project will be assessed on the basis of the following:

- 60% on the quality of your proposed model and code. How you design the threats, how you design the security/privacy application
- 10% on your chosen data sources and how they were pre-processed
- 10% on innovation, creativity etc. and regulation/ethical considerations
- 20% on presentation of your report/video

Moreover, Individual Peer Assessed Contribution (IPAC) will be used as a factor in determining your final grade for the project, as follows:

- group mark * IPAC

Appendix: Guidance questions
For the various section of the report, think about the following questions:
• Executive summary:
o Have you outlined the background to the problem?
o Have you clarified the purpose of the report?
o Have you provided brief details of the approach you followed?
o Have you summarised the important results and findings?
o Have you stated the major conclusion from your work?

• Design and implementation:
o Have you identified the problem you are addressing?
o Have you provided an overview of how you are addressing this problem?
o Have you provided detailed steps of what you did in a logical order?
o Have you described the methods you used to solve the problem and their purpose?

o Have you identified the parameters for designing your system?
o Have you identified the metrics for evaluating the performance of your system?
o Have you used illustrations to give the reader a visual interpretation of your system?

• Results:
o Every result included must have a method set out in the design methodology.
o Likewise, every method should have some results.
o Have you used figures and tables to illustrate your points?
o Have you critically evaluated the quality and reliability of your results?
o Are your observations supported by evidence?
o Is the analysis and discussion relevant to the project and its context?
o Have you explained how well (or not) you have met the project’s objectives?

• Trade-offs:
o Have you considered and quantified the cost (you will incur) versus the gain (you will obtain) when you modify different parameters in your system? For example:
▪ Local vs. Cloud processing.
▪ Range vs. Power consumption (battery life).
▪ Throughput vs. Power consumption.
▪ Latency / Delay vs. Accuracy.
▪ Performance vs. Security.
▪ Generic vs. Bespoke hardware.
▪ Price vs. Functionality.
▪ Price vs. Usability.
▪ Price vs. Robustness / Reliability.
▪ Functionality vs. Usability.
▪ Functionality vs. Rapid development (time to market).
▪ Functionality vs. Backward compatibility.
▪ Flexibility vs. Accuracy vs. Interpretability.

END OF ASSIGNMENT

February 2025