Security and Privacy (ELEC0138) Project Assignment

2023/2024

Assignment Issued: January 2024

Guidelines:

All assignment deliverables to be handed in by: **19th of April 2024 4pm** (optional half-page work-plan to be submitted by March 13th 2024 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) 2023/2024

1. Description:

In this assignment you will write a report entitled: "Securing X: Designing a Comprehensive Security (or Privacy or Both) System" to be presented to your Chief Security Officer (CSO) at your company.

Coursework 1: Defining a threat model and a security (or privacy or both) attack

Consider a user-centred environment (smart home, smart city, smart hospital, company, etc.), then define a threat model with at least 2 security (or privacy or both) threats and for each of them define and design the attacks. You should understand and identify the specific security (privacy or both) risks and vulnerabilities of the system, and prioritize the implementation of measures to mitigate these risks.

You should:

1. Identify assets: Identify the assets of the system, including data, applications, and infrastructure.
2. Identify threats: Identify the potential security (or privacy or both) threats to each asset, including internal and external threats.
3. Assess impact: Evaluate the potential impact of each threat, including the potential damage to the assets and the cost of remediation.
4. Prioritize threats: Prioritize the threats based on their impact and likelihood of occurrence and focus on mitigating the highest-priority threats.
5. Design the security (or privacy or both) threats by implementing code-based attacks and utilizing existing tools. You will have to be as exhaustive as you can covering as many attacks as possible.

Coursework 2: Security/Privacy mitigations

Consider the above threat model and threats, and within the context of the course:

1. Design an app/system for security (or privacy or both) defence (including access control, encryption, firewalls, intrusion detection and prevention,..).
2. Present and discuss opportunities innovation, creativity, enterprise, scalability & complexity analysis within your system.
3. Explain regulation and ethical considerations. You will have to explain how you will adhere to the several privacy/security regulations, GDPR in Europe and equivalent in other continents and explain what ethical issues may be raised by your prototype.

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