Secure Software Development – Introductory session and group allocation for Team Project

Outline:

- Online session rules
- Learning Outcomes
- Introductions
- Seminar 1 Questions Q&A

Online session rules:

- Microphone muted when not talking.
- Not over talking each other.
- Everyone is encouraged to contribute and should be treated with respect.
- Asking questions are wanted and could benefit for everybody.

Module learning outcomes:

- Understanding of the principles of information security management.
- Understanding of secure programming and development techniques.
- Opportunity to reflect on and evaluate their personal development.
- Ability to present critical arguments for specific actions or outcomes to a diverse audience.

Assessment:

- You are required to develop an application for an organisation with domain-specific requirements. A domain refers to a group of users with similar application and hardware requirements. A domain may be characterised by having:
- → periodic pressure on resources (CPU, storage, or the network)
- → interactive response requirements between request and reply
- → substantial data download requirements
- Such requirements place specific demands on a system's operations, and this influences the way that it should be operated and managed.
- Domains which you should consider for the purpose of this assignment include:
- → The International Space Station (NASA, 2007)
- → The Dutch Police Internet Forensics (Government of the Netherlands, n.d.)
- The Hadron Collider (The Computer Security Team, 2020)

- You can read more about the computer requirements of these systems using the references given. You should choose a single domain to focus your development on, and your system

should be tailored to the requirements of this domain. In all domains, a user will need to be able to upload, download and share data.

- The agreed criteria for successful development are:

- → The solution should ensure that all privacy and security regulations are met, including those specified by the GDPR.

- Mechanisms should be deployed to minimise the attack surface of the solution.

- The organisation would like to see a monolithic version of the application because they have concerns about security, scalability and supportability and they may wish to extend use to partner organisations on a worldwide basis.

Part 1: Design Proposal Report

- Your team is expected to prepare and deliver a design proposal report of your intended development work for the organisation.
- Your report should detail the design decisions and approaches that you have adopted to create your secure software solution. It should outline business and technical challenges you have identified/ ecpect to encounter, and then highlight (briefly) what paradigms, patterns, theories and practices you intend to utilise on this project. Build up a rationale where appropriate supported by literature.
- Sate any requirements you have gathered, and any assumptions you are making in relation to the design of the system as a consequence of your investigation. You should also satate any tools and models that you will use in your solution.

Checklist for the assignment:

- High level system design (preferably in diagrammatic form e.g., UML) that provides an overview of the solution you propose.

- List of technical challenges to be addressed (inc. Infrastructure)

- List of patterns and approaches to address the challenges, supported by references where appropriate (e.g., three tier architecture, client-server architecture, ect.)

- List of system requirements (based on domain)

- List of assumptions (with brief justification)

- List of tools and libraries (e.g., syntax checkers, editors, compilers, libraries that provide additional functionality such as Regex paresers, Cryptographic routines, ect.)

- ➔ The design should be organised with tables, diagrams and graphs instead of written text.
- ➔ Use of the appendix is a possibility to add more information in the assessment.
- ➔ It is asked to explain a general overview of the needed infrastructure.
- ➔ An aspect of the design report is to make assumptions about what is needed and to reflect it with the real results implemented in the final document.

- You should get your design outline reviewed and approved by your tutor before you submit you design or start to code.
- Assessment – group assessment teams of 4-5 people
- Design/Report (week3)
- Working & Tested Application (week 6)
- Individual Reflection (week 6)
- Formative feedback on discussion forum
- E-Portfolio is not required for this module
- Office Hours: Tuesday 12:00-13:00 / Friday 18:00 – 19:00

Next Week:

Prepare DRAFT outline of design (in UML)

Present and review design in Seminar

If you can't make the seminar, please contact me to make an alternative appointment (ideally in office hours slot)

Also the Seminar Preparation and reading around UML