**ePortfolio:** <https://alesteka.github.io/essexPublic/>

**REFLECTIVE PIECE OF WORK**

Throughout the module, I acquired a lot of knowledge about secure design concepts. The module provided me with the knowledge that previously I hadn't put attention to and I found out that security does matter in any system that we can think of. I was particularly excited about the final project, as at first I tought that this would be an impossible assignment to do. However, with a great amount of dedication, our team learned a lot and managed to submit a working project that took into account most common security vulnerabilities, together with contemporary design and architectural principles.

At the beginning of the module, we were introduced to different software development approaches, particularly to Agile and Waterfall, as they are two of the most common at the present. Understanding these approaches allowed us to get organized for our team assignment and to communicate ideas easily within the team. In addition, we were introduced to UML diagrams that took part in the first collaborative discussion, together with the focus on OWASP security risks.

For the first collaborative discussion, there were a lot of interesting discussions, covering all aspects of common contemporary security risks. My focus was on Software and Data Integrity Failures, as we can easily get lured into downloading third-party content, whether it is a programming package or just a movie from an untrusted source. The opinion from Michael gave me an additional component to think about, which is raising awareness among people, since we are often the weakest link in a system. The first collaborative discussion was also interesting because of the new security terms that I encountered and the content of how the attacks work within the systems. To understand this, we have to know the core functionalities of the systems and overall web communication.

Additionally to the discussion, we were encouraged to write a blog post on how the people within an organization could be managed to mitigate potential security risks. The content acquired throughout the first half of the module helped us to successfully submit our first part of the team assignment. This assignment was special in the meaning of the team collaboration, as not everyone had the same amount of expertise and especially the same vision. From that perspective I would say, that the key was in communication and recurring meetings rather than the technical aspects of the assignment itself. However, we have managed to collaborate well, trying to make the most of our individual skills. The real value there was brainstorming the ideas, of how to make the system meaningful, while considering all security vulnerabilities. To facilitate the ideas, UML diagrams were the main part of the project, as well as the tools and techniques used.

With the help of the session lectures and lecturecasts, the module was well-guided, covering basic topics to more advanced ones. Therefore, after the design proposal we were introduced to operating systems from the perspective of security vulnarabilities and cryptography, which was also the topic for the second discussion, where we read about TrueCrypt. This case study provided insight into an interesting topic about outdated software that is no longer supported. However, more than the topic itself, I found the technical description of vulnerabilities more interesting, as the article demonstrated, how the breaches overpass the system. Hence I really enjoyed reading, as I learned more about core system vulnarabilities (understanding various overflow errors, Kernel weaknesses, bootloader problems).

If I were to compare the design proposal with the final project, I could say that we managed to achieve amazing coding output. However, some minor goals received less attention, such as system requirements. In that particular example, we had the entire project situated in a cloud environment, so that the RAM, CPU and disk size were not an issue (as the cloud is likely to scale up in the case of heavy traffic). Beside that, we were not completely certain with some functionalities of user roles (employee/admin). However, during the development, we managed to make some adjustments, to ensure that the operations would have meaning. Nevertheless, I would say that the main goal had been accomplished, that was to deliver functional app with as much of security considerations as possible. What I would also like to highlight is the motivated team that I worked with. Members were always ready to jump in and talk in the case of any misunderstandings. In addition to that, we often scheduled additional meetings, just to review the work that had been done and what else would have yet to be finished. This allowed us to follow the plan without pressure.

Entire module experience brought me the knowledge that I had been missing, and I'am certain it will benefit me in the future. That is because side activities, such as using Codio allowed me to understand concepts through the practical examples. One of these were using the API-s which are nevertheless present in almost all main systems.

Overall, I can say that the entire process went well and the learning was pleasant, despite not being able to attend the sessions, due to job obligations. Nevertheless, this wasn't an issue, as all recordings were well placed, following the content of the subject. On the other hand, team meetings took place mostly at the weekends, when we all had time to meet. I would say that we spent more time than expected, however this is understandable as the project itself wasn't that simple.