**University of Essex – MSC Cyber Security**

**End of module – Reflection June 2021**

My experience of the Secure System Architecture module was one of particular interest because the module highlighted the importance of secure system development throughout the lifecycle management. The Open Group Architecture Framework (TOGAF) stood out to me, used to improve business efficiency and as of 2020 is implemented by “80% of Global 50 companies and 60% of Fortune 500 companies”. Currently on its 10th edition this showcases the constantly evolving nature of systems architecture (Soyana, Putera, 2019).

Our team project tasked us with designing and simulating Internet of Things (IoT) devices communicating through a central controller. As a group, we listed numerous IoT devices that could be used in our simulation. A vote decided that our ‘smart home’ would be a smart door lock, security camera and controller. Attack trees were developed to visualize potential vulnerabilities and mitigation strategies.

As a team we decided a ‘slack group’ to be the best form of communicating, sharing documents and discussing the various tasks required. This, paired with Google Docs enabled the sharing and editing of work needed for submission. Various meeting were held using Zoom. Appendix A and B below show how our group arranged the various tasks required. We established which section we would like to undertake; segments were allocated based on individual strengths. Appendix C and D show my contributions to unit three and six respectively, I also assisted with structure, spelling and grammar amendments.

I consider that I participated well in the discussions, used knowledge gained from established work experience, assessed the vulnerabilities, and supplied both meaningful comments and alternative suggestions. The module enhanced my awareness realizing securing systems and security lifecycle management on a global scale should be implemented more widely. This group work was overall beneficial as it enabled me to better understand others thought processes. I was also able to both comprehend and propose different outcomes, leading to a more in-depth assessment report.

One particular challenge we faced as a team was the geographical time difference between our physical locations. I am based in the Caribbean (GMT-5) and others across North America, Europe and Asia. This certainly was not easy, nor ideal and made group calls tricky at best. Another challenge was navigating the UOE web platform which can be difficult, especially when searching for academic reading material and papers pertaining specific subject matter. Another hurdle was a complete lack of communication and participation of one team member.

After some deliberation regarding which system and code should be used, our group settled on Message Queuing Telemetry Transport (MQTT) as the IoT messaging protocol and phython3 for the code as this best suited the project. MQTT, a lightweight protocol designed specifically for IoT devices is “ideal for connecting remote devices with a small code footprint and minimal network bandwidth” (Hunkeler et al, 2008) which was a deciding factor.

Overall, my main takeaways from this module was learning that discussing individual strengths, weaknesses, division of tasks and understanding architectural frameworks is the best approach for a successful group outcome. Strong communication skills and planning ultimately make the end goal more achievable. I look forward to the projects upcoming and gaining greater knowledge of the complexities surrounding the world of cyber security.

Appendix A

Graphical user interface, table, email

Description automatically generated

Appendix B

Text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Appendix C

Diagram

Description automatically generated  
Systems Architecture of the Smart Lock

Appendix D

Diagram

Description automatically generated

Initial Design

Diagram

Description automatically generated

Final Design

References:

U. Hunkeler, H. L. Truong and A. Stanford-Clark, "MQTT-S — A publish/subscribe protocol for Wireless Sensor Networks," 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08), 2008, pp. 791-798, doi: 10.1109/COMSWA.2008.4554519.

L Sofyana and A R Putera (2019), J. Phys.: Conf. Ser. **1375** 012056 DOI <https://doi.org/10.1088/1742-6596/1375/1/012056>