Module SSA+PCOM7E has provided more opportunity for reflection than any of the previous, particularly with group dynamics. The module itself had two main deliverables, an application threat assessment illustrated and quantified via attack defense (AD) trees (Bagnato, et al., 2012) and a working model of an Internet of things (IOT) application utilizing microservice architecture. The technical elements of the project are important and represented a significant challenge, but the change in group dynamics between the two deliverable phases is the primary focus of this reflection.

“Performing threat modeling on cyber-physical systems with a variety of stakeholders can help catch threats across a wide spectrum of threat types” (Shevchenko, et al., 2018). To facilitate discussion, I created a preliminary design of an IOT system in advance of our first group meeting intentionally to initiate design consensus dialog and meaningful vulnerability considerations (Leece & Johnson, 2021).

During the preliminary meeting some group members indicated limited programing confidence therefore a division of work was agreed upon, I would support AD tree and vulnerability assessment work others had committed to, focusing on deploying project infrastructure and beginning development. Despite alignment with university group project guidance (Swain, 2019); I.E, clear goals and contributor assignments, the group struggled designing AD trees, identifying design specific vulnerabilities and risks resulting in draft content incongruent with assignment requirements. I rewrote the entire assignment overnight, including others’ content where possible. All other members agreed the report aligned closely with the requirements while one member was openly confrontational despite limited contribution during the previous two weeks. Despite my personal feelings of anger and frustration, I responded that the group was an open forum, but the timing of the objections did not allow for changes.

Initially members agreed to self-organization and personal accountability, despite not being officially appointed leader I feel my response and open decision to proceed with the majority opinion changed group dynamics for the rest of the project. Reviewing the Swain article, I feel I was both the primary leader as well as ideas person and the assertive stand on submitting the initial assignment as it was and reiterated invitation to contribute led to the dissenting member becoming an active participant in the development process, often working late in the evening and openly collaborating. Two other members who had been supportive, but somewhat passive, took proactive measures to complete the written work, ensuring a strong deliverable despite their own personal work pressures.

The assignment requirement to demonstrate a distributed services application, including network communication between independent services (University of Essex, 2021) was particularly challenging. Although familiar with network socket programming, container-based services presented significant personal learning curve, requiring much self study (Gahdhi, 2019). Like a real-world software development project, multiple members must contribute to a project’s success.

Figure 1 captures the last bit of group interaction after a lengthy online meeting finalizing the team’s submission. The good will and mutual respect was evident and a marked turn from just three weeks earlier.

Text

Description automatically generated

Figure Team 3 Collaboration

# References

Bagnato, A., Kordy, B., Meland, P. H. & Schweitzer, P. (2012) Attribute Decoration of Attack-Defense Trees. *International Journal of Secure Software Engineering,* 3(2): 1-35.

Gahdhi, R. (2019) *Learning Path: Creating Docker Imagers and Dockerfiles.*    
Available from: https://learning.oreilly.com/learning-paths/learning-path-creating/9781098115180/  
[Accessed 27 November 2021].

Leece, D. & Johnson, s. (2021) *Design Secification: IOT Climate Control Solution.*    
Available from: https://github.com/t3ssa1121/climatecontrol/blob/gh-pages/Climate\_Control\_Specification-final\_draft.pdf  
[Accessed 19 December 2021].

Shevchenko, N. et al. (2018) *THREAT MODELING: A SUMMARY OF AVAILABLE,* s.l.: Carnegie Mellon University.

Swain, R. (2019) *3 tips for successful group work.*    
Available from: https://www.prospects.ac.uk/applying-for-university/university-life/3-tips-for-successful-group-work  
[Accessed 19 December 2021].

University of Essex. (2021) Development Team Project: Code Development. Available from: https://www.my-course.co.uk/mod/assign/view.php?id=571577  
[Accessed 19 December 2021].