Unit 5 Reflection

In this unit, it was interesting to consider the algorithms used in cellular networks, specifically the A5 algorithm used to encrypt cellular data over radio links between base stations and serving stations. This was a topic I never considered previously but found rather interesting to learn about. Especially considering that there are various levels of encryption such as A5/0 that has no encryption, and A5/1 and A5/2 that use a key length of 56 bits due to a compromise required by the British to intercept calls. The unit's reading material referenced by Jøsang et al. (2015) was an interesting read because I never considered the workings of 3G networks and related security architecture in 4G Long Term Evolution (LTE) networks.

Also, part of this unit's reading material involved learning about the evolution of wireless network security which led to further research about Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). What I take away from the material is that using WEP with weak password policies, does not guarantee network protection WEP-protected networks' 64-bit or 128-bit are easily deciphered. The recommendation is to utilise WPA2 (second version of the WPA standard) that uses Temporal Key Integrity Protocol (TKIP) encryption that makes it harder to decipher the network key. WPA2 also uses Advanced Encryption Standard (AES) cipher. There are several techniques one can leverage to protect their networks, one is using the latest iteration of WPA (WPA3, release in June 2018), and another important aspect that stood out so far, is to replace the router's default password.

I considered this unit's reference reading, the book "TCP/IP Tutorial and Technical Overview" by Parziale et al. (2006), valuable as contribution to this unit because the required chapters (one to five) added to my existing understanding of TCP/IP and the content learned from previous units. The book considered the concept of bridges, routers and gateways that support network communications. I found interesting the process to develop TCP/IP standards, where specifications are submitted to the Internet Engineering Steering Group (IESG). When approved, they issue a Request for Comments (RFC), which are assigned one of six states assigned by the Internet Architecture Board (IAB). Continuing through the reading material, I found it interesting that certain IP addresses are classed as reserved such as 224.0.0.0/4 (multicast) or 192.168.0.0 through 192.168.255.0 for contiguous Class C networks. Also dealt with was the concepts of IP subnetting, IP address classes, the IP routing algorithm; I gained a deeper understanding of unicast, multicast, broadcast and anycast.

During this week, the team collaborated to prepare the team design document. We discussed format, content and performed several reviews on the document generated to date. I focused

on the risks and recommendations and ensured that all entries listed matched closely with content from the previous section. Developing this section was engaging and I was pleased that the content learned from previous modules was tremendously relevant to the risks and recommendations uncovered—the content learned is slotting into place very well. The team spent a few days communicating to review the document, ensure consistent format and supporting other members with any additional information where relevant.