Unit 4 Reflection

In this unit, we focused on using basic tools to investigate networks especially when attempting to perform troubleshooting.

I read the requisite chapter 8 and 12 form the book by Schneier (2015) concerning computer security and network defences. In the book reference is made to the cyber security triad of confidentiality, integrity, and availability (CIA) where the majority focus of computer security is around confidentiality which, according to Schneier, is because the military funded much of the early research into computer security. I learned that access control is fundamental to CIA and that there are two aspects to access control: who can do what, and what can be done. One constituent part of access control is an *access control list* (ACL) which I can relate to as often I have had to set permissions for folders within Microsoft Windows. Following on from ACLs, it was enriching to read about the Bell-LaPadula concept of mandatory/multi-level security policies and discretionary access controls tough most users are familiar with the Role Based Access Controls (RBAC) setup today.

I gained greater insight details about IPv4 and IPv6. IPv6 accommodates for the growth of the internet—Internet of Things. I was interested to learn that IPv6 does not fragment packets or require Network Address Translation (NAT) and has IP security built in, making it a suitable protocol for future growth. The downside to IPv6 addresses is the address notation that consists of 8 groups of 4 characters each separated by a colon (“:”). I thoroughly enjoyed reading about the avian transmission of IP data and considered this similar to Windows Communication Framework (WCF) that supports messaging over every type of medium (https://docs.microsoft.com/en-us/dotnet/framework/wcf/architecture) using either unique protocols or transports. WCF could be leveraged to implement a Pigeon Messaging channel. Indeed, Cher Ami—the last war pigeon—saved the lives of 194 war survivors (NMMC, ND).

I enjoyed spending time researching about the history of the Internet’s OSI and TCP/IP models for this unit’s seminar. It was enlightening to delve deeper into why the OSI model is not as widely used as the TCP/IP stack. One big takeaway from the research about OSI’s failure is that OSI had IBM’s business interests in mind in trying to guide the development of the internet. Another takeaway is that ISO organisation was bureaucratic while IETF’s development of TCP/IP was more agile (in software development terms) and importantly, free to implement. A third takeway was that TCP/IP was developed as a working prototype ahead of OSI’s *theoretical* models, and I consider that *practical implementations* beat *theoretical implementations* every time. I take this research onboard as I believe it has valid real-world applications. Also, I consider that hiding the ability to implement technology behind licensing

costs strongly hampers any collectives' ability to design flexible solutions that meet requirements of *stakeholders*. Considering other aspects of the OSI model, I think it was designed to be flexible and extensible, evidenced by the seven layers within to the model. The concept of layers is seen even in today's software development, since developers typically think of systems in terms of "database", "application" or "business"—each considered a unique and separate layer.

I continued to contribute toward the collaborative discussion, looking to stimulate further discussions around the tools we used for network troubleshooting. I found the discussion topic rather difficult to raise specific questions because all students performed the same task with the same tools.

References

NMMC, (ND). National Museum of the Marine Corps: War Communication during WWI. Available from http://www.usmcmuseum.com/uploads/6/0/3/6/60364049/nmmc_wwi_military_communication_resource_packet.pdf. [Accessed 6 Jan 2021]

Schneier, B. (2015). Secrets and lies: digital security in a networked world. Indiana, USA: John Wiley & Sons.