Chapter 6

Conclusions and Future Work

6.1 Conclusions

Both research and personal objectives were outlined in section 1.2 to provide guidance for the project and provide a means to complete the project in the time frame given. This chapter discusses the goals completed and provides conclusions on the work carried out.

6.1.1 Goals Revisted

One of the primary goals of this project was to migrate the code for the current surveying tool to python3 and refactor it along the way to optimise it. The refactoring and migration process was carried out successfully, and there were significant improvements in the program by making use of new functionalities available in Python3. Since support for Python2 has depreciated, even though some may argue the benefits of Python2 over Python3 but since there is an industry-wide shift towards the adaptation of Python3, this would prove beneficial if other entities wish to use this program. In addition, the migration makes it more accessible and easy to run. While carrying out the refactoring process, the Python Enhancement Proposal 8 (PEP8) was followed to standardise the code to industry standards to increase understanding of the program. Following this convention allowed to maintain a single coding style throughout the program amongst many scripts, which could benefit other entities later if they wish to make changes to the program to fit their needs. All technologies used for this project, like Maxmind, ZMap and ZGrab, were upgraded to their latest versions.

The methodologies and the design of the program should allow other entities or institutions to

carry out scans for different populations. They can replicate the same work as carried out here with ease. The program was updated to scan populations using data from the Maxmind database, and it also has provisions to do so with the Censys databases. Although it was not possible to upgrade the program to work with the update of the Censys metadata due to Censys going commercial, attempts were made by contacting them to get some sample data to extend this work. However, unfortunately, Censys did not provide the data needed to upgrade this program.

Another goal of this project was to add port 853 (DNS over TLS) to the scans parameters. Code had to be written in Golang, and integration tests had to be run using the ZGrab2 integration tools available. However, it was unsuccessful due to a lack of programming experience in Golang and time constraints. Although a simple banner grab over port 853 using TLS was successfully added, it was not the most efficient way to go about it. The code for the same can be found in the appendix.

6.1.2 Final Remarks

Overall, all goals but adding port 853 were accomplished, and there is still widespread key reuse seen, as proven back in 2018 by Dr Farrell. However, key reuse between SSH and other protocols that use TLS was not seen as was the same case in 2018 [8].

6.2 Future Work

This section discusses some of the possible extensions of this work.

6.2.1 Scanning other Countries and IPv6 address Space

Due to the time constraints, only a couple of scans for Ireland were able to be carried out, and data analysis was only done on one of scans, but one could get a better understanding of some of the causes behind this key reuse by carrying out scans over a long period at regular intervals. While the accuracy of these scans is acceptable for this project, one could extend this work to distinguish between hosts that operate with more than one IPv4 address, i.e. multi-homed hosts. Currently, the program can not differentiate between multi-homed and single-homed hosts. Still, introducing some techniques to distinguish between the two would provide a more accurate picture of the key reuse scenario for a population.

Another possible extension of this work would be to scan the IPv6 addresses space.

6.2.2 Adding Additional Protocols

An interesting extension of this work would be to add additional protocols to scan for, like the MQ Telemetry Transport Protocol that is used by IoT devices and is adopted widely. MQTT has provisions for using TLS and since the number of IoT devices is growing exponentially, they have a reputation for being insecure. It would be interesting to see if there is key reuse across these protocols.

6.2.3 Database Managment

A place where this work could be extended is by improving data management. Since a large amount of data is captured using JSON and each JSON structure is highly sparse, one could look at integrating databases like Elasticsearch, which is an open-source NoSQL database that can be used to store unstructured data and query it with ease using SQL commands [7]. This could be highly beneficial for entities carrying out scans for a considerable period, gathering a lot of metadata.

6.2.4 ZGrab Data Transformation

One could also change the ZGrab2 output schemas [6] for better data structuring. Although, this could prove to be a bit cumbersome as there could be further changes to the ZGrab output in the future, and that would cause issues while developing a database management system and maintaining it.