Chapter 1

Introduction

This chapter introduces the reader to the motivation behind this project and provides a brief outline of the research and personal objectives to be accomplished. It also gives an overview of the structure of this report.

1.1 Motivation

Since the inception of the Internet, it has been in a constant state of evolution. While it provides users easy access to information and services, it also includes several risks. The rapid development of the Internet has revolutionised how humans communicate with each other and has become a natural extension of our lives. However, this rapid evolution leaves an opening for people to exploit the weakness in the infrastructure for their gain. Data from Internet-Wide Scans can be used to identify devices and services exposed to the Internet. In addition, the data can be analysed to determine devices or services prone to vulnerabilities or weaknesses. The risks associated with those vulnerabilities and flaws cannot be underestimated as they can lead to severe ramifications not just for the entity involved, but also for the users that use that service.

In 2014, the Yahoo Data Breach, which is known to be one of the most significant data breaches, occurred. Due to improper input validation systems in place by Yahoo, the attackers were able to take any identity of their choice on the network. They did this by exploiting a weakness in the user creation and identification process [33].

The project implements an Internet-Wide Surveying tool for Ireland, but can be used for any country to check for long-term key reuse and builds on existing research as outlined in Chapter 3.

1.2 Objectives

This section sets out the research questions and objectives for this dissertation. It also outlines the personal goals set out.

- Recreate Dr Farrell's existing research in 2018 on surveying cryptographic keys.
- Migrate the current program to Python3 from Python2.
- Refactor code to increase readability and decrease complexity.
- Understand the development in key reuse as compared to previous scans.
- Research existing tools and APIs for accurate geolocation IP data to carry out the scanning process.
- Refactor existing code for the program to work with the latest tools and APIs.
- Add DNS over TLS (port 853) in the scanning process.

1.2.1 Personal Objectives

- Develop knowledge on the Public Key Infrastructure (PKI) and how it is deployed to manage internet security for different protocols.
- Develop knowledge of internet protocols like SSH, TLS, SMTP, IMAP, SSH and more to understand the implications of key reuse.
- Familiarise with internet scanning and surveying tools like ZMap and ZGrab to get data needed for analysis.
- Learn to code with industry-standard Python practices and use memory-efficient methods for data storage, retrieval, and access.
- Ability to multitask and efficiently manage time to complete the research, coursework, and other personal work like a job search.

1.3 Thesis Overview

A brief outline of each chapter of this thesis is presented below:

- **Chapter 2: Background -** This chapter presents a detailed theoretical background of the research project.
- **Chapter 3: Related Work -** This chapter provides a summary of existing and relevant scientific literature for this project.
- **Chapter 4: Methodology -** This chapter describes the methods used for the investigation of the problem and the technologies used.
- **Chapter 5: Results -** The chapter presents the results obtained after the network scan.
- **Chapter 6: Conclusions and Future Work -** This chapter concludes the project with a summary of the research done and its validity, along with possible research that can be carried out on top of this.
- **Bibliography and Appendix -** These sections comprise a list of all the papers, articles, and books referred to while writing this thesis, and the appendix contains some supplementary information.