Abstract

Internet Scanning is used for a variety of purposes. While some may use it to detect and investigate flaws and vulnerabilities in a network, others may exploit them. This project aims to migrate, refactor, optimise the existing program, and survey long term cryptographic keys for web, mail and SSH protocols in the IPv4 address space. The target population for these scans are hosts that accept connections on TCP port 25, i.e. hosts that offer mail services. The hosts identified as port 25 listeners are further scanned to get their SSH and TLS session data to check for key reuse for Secure Shell Protocol and Transport Layer Security protocols. Finally, the project investigates some of the causes behind this key reuse and builds directly from Dr Farrell's research in this domain.

Mismanaged key reuse can create vulnerabilities in a network that can go undetected and leave entities open to attacks such as the man-in-the-middle. The program to survey these keys was last run in 2018, and the project explores how key reuse has evolved since then. Internet-wide scanning is a well-researched domain, but this project performs local region scans with only port 25 listeners, hoping that small scale scans could identify vulnerabilities better than internet-scale deployments. The project also entailed code migration, refactoring and optimisation to decrease the run time and memory consumption by identifying bottlenecks in the program and exploring alternate solutions with new developments in the technology landscape since 2018.