INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

Decentralized Authentication Without Passwords

A dissertation by

Mr. Pin Chamath Avishka de Silva

Supervised by

Dr. Nimalaprakasan Skandhakumar

Submitted in partial fulfilment of the requirements for the MSc in Cyber Security and Forensics degree at the University of Westminster.

May 2022

Abstract

Passwords have been used since early digital systems. The security on authentication provided by it was sufficient at the time, especially with the computing power that existed. However, with the availability of extremely powerful processing power in the modern age, as well as the utilization of ingenious techniques by hackers, passwords rapidly could be seen as insecure. The acceptance of these vulnerabilities caused alarm in the digital world, which led to louder and louder cries to strengthen passwords. Multi-Factor Authentication, Stronger/Complex Passwords etc. were results of this. They did provide a dampening relief from an otherwise collapsing technology and did help buy more time to find a better alternative. But this quest has been painfully slow; solutions either had issues passwords did not have at all, were too complicated or expensive, extremely difficult to use or reduced efficiency. A clear understanding of what is required and expected from a secure authentication mechanism is needed, not only in technical terms but also with due attention to what users prefer or expect.

A broad analysis of the available options to replace passwords made it evident that Public Key Cryptography has the potential to cater the needs and is becoming the popular trend. Existing implementations however, seemed to have unclear, non-standard approaches, which could have contributed to resistance or slow progress. Utilizing existing tools and techniques could catalyse progress and acceptance when attempting to propose a solution. Such a framework has been developed in this research by trying to give focus on all aspects of a secure authentication mechanism, to produce a Decentralized Authentication without Passwords.

In the proposed framework, the unified approach to address every aspect of authentication can help minimize resistance to be adopted and speed up the milestone of making passwords a thing of the past. Due attention to ensure security, compatibility as well as user-friendliness have been made especially for this end.

Keywords: Secure Authentication, Password-less, Public Key Cryptography, Hardware Security Module