Analysis on the Security and Use of Password Managers

Carlos Luevanos[1], John Elizarraras[2], Khai Hirschi[3] and Dr. Jyh-Haw Yeh (Mentor)[4]

[1]Willamette University
[2]North Star Charter School
[3]Capital High School
[4]Boise State University

Abstract Cybersecurity has become one of the largest growing fields in computer science and the technology industry. According to CNBC, the global economy lost over 450 billion dollars due to faulty security. Oftentimes, the pitfall in such financial loss is due to the security of passwords. Companies and regular people alike do not do enough to enforce strict password guidelines like the NIST (National Institute of Standard Technology) recommends; so when big security breaches happen, thousands to millions of passwords can be exposed and stored into files, meaning people are susceptible to brute-force attacks In this paper we will be going over three open-source password managers, each chosen for their own uniqueness. Our results will conclude on the overall security of each password manager using a list of established attacks and development of new potential attacks on such software. Additionally, we will show the results of a survey to give us a closer look as to why such software is not so popular; and we will compare our research with the limited research already conducted on password managers in the literature; and finally we will provide some general guidelines of how to develop a better and more secure password manager.

This research was supported by Boise State University and funded by the National Science Foundation under the grant CNS 1461133 and the NASA Idaho Space Grant Consortium Summer STEM Experiences for High School Students Grant.