Password Managers: Security Solutions and Vulnerabilities in Modern Authentication

Sam Wang
Team Member

Nicole Kuo
Team Member

Caleb Su
Team Member

Yi Yu
Team Member

Parkash Singh
Team Member

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—password managers, cybersecurity, authentication, encryption, LastPass breach**

I. Introduction

A. The Password Problem

B. Motivation and Significance

II. Technical Background

A. Encryption Methods

B. Master Password Protocols

C. Architecture: Local vs Cloud-Based Solutions

III. Comparative Analysis

A. LastPass

B. 1Password

C. Bitwarden

D. Dashlane

E. Feature and Security Comparison

IV. Security Vulnerabilities & Case Studies

A. LastPass 2022 Breach (Primary Case Study)

B. Other Notable Vulnerabilities

C. Common Vulnerability Patterns

V. Conclusion and Discussion

A. Best Practices and Recommendations

B. Future of Password Management

C. Role in Broader Cybersecurity Landscape

Acknowledgment

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks …”. Instead, try “R. B. G. thanks…”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.