Are Users More Willing to Use Formally Verified Password Managers?

Carolina Carreira
Carnegie Mellon University, IST and INESC-ID

CMU PORTUGAL SUMMIT 2022
NEW FRONTIERS IN TECH

1. Introduction

Although formal verification has been increasingly used to prove the security of many applications, the views of non-technical users' on this topic are largely unknown. To address this problem, we conducted two user studies, focusing on Password Managers (PMs).

> **A formally verified PM is one that:**
> is mathematically correct, that is, its features are as trustworthy as a mathematical proof.

2. Methods

To understand users' views on formal verification we designed and implemented **two studies**.

Figure 1. Formal Verification icon used in the first study to represent formal verification in the PM's interface

First study (pilot)	
Goal	Gather insights on general themes on this topic
Sample	15 participants
Method	Interviews

Second study	
Goal	Test the findings of the first study and answer the RQs.
Sample	200 participants
Method	Surveys

3. Research Questions

RQ1. How does formal verification impact users' willingness to use PMs?

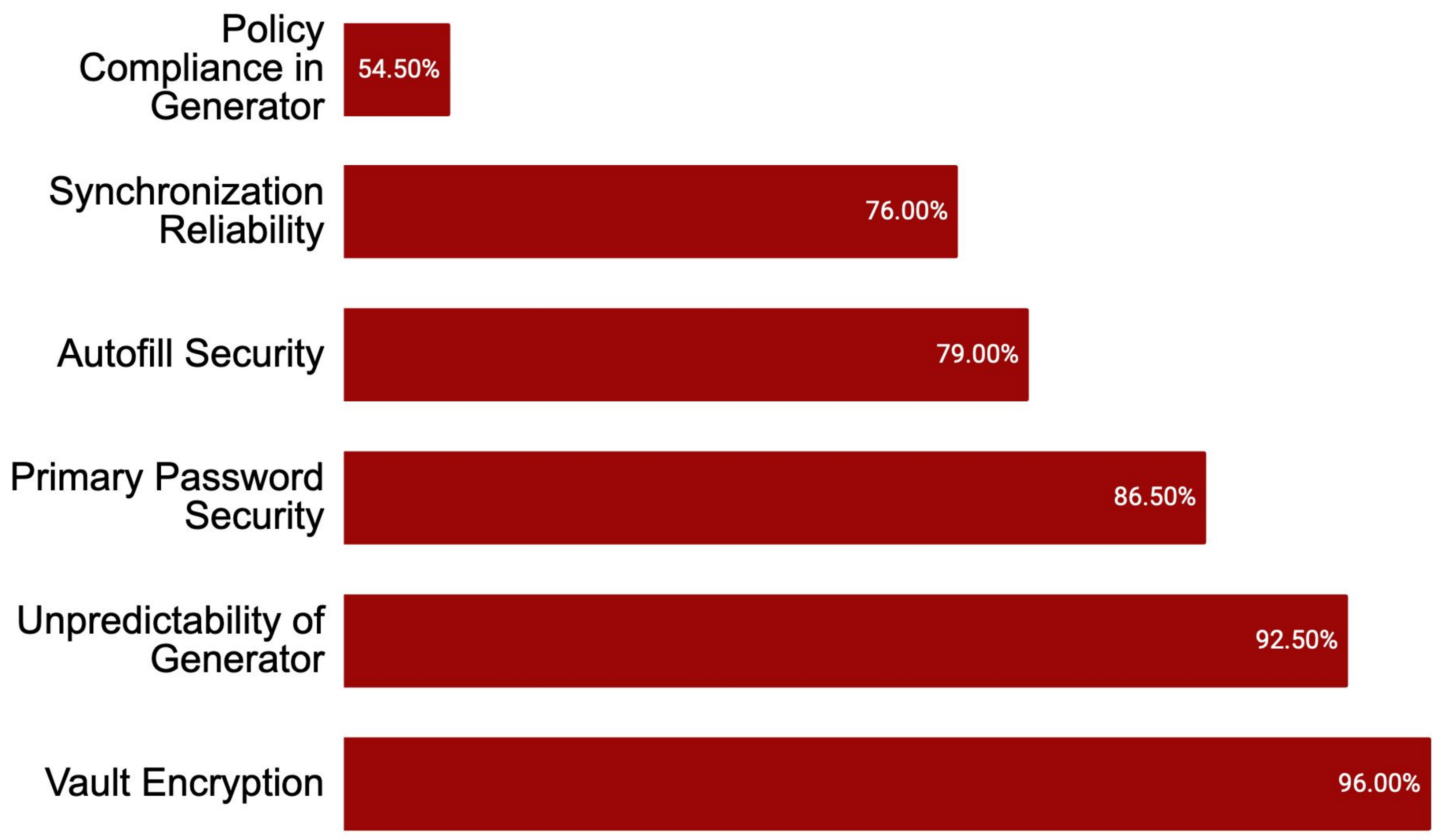
The results from the **first study** and **second study** seem to suggest:

- Users associated formal verification with security;
- Users **may be more willing to use a formally verified PM.**

RQ2. What features would users like to see formally verified in a PM?

In the **second study** we asked participants about potential formally verified features of a PM. Each feature corresponded to one or more scenarios (see Fig. 2).

Figure 2. Percentage of participants that agreed or strongly agreed the respective scenario would make them stop using a PM.



4. Future Work

- ⟹ Prioritize the verification of the features in Fig. 2;
- ⟹ Study the impact of formal verification in other domains;
- ⟹ Understand the most effective way to communicate about formal verification.

5. Conclusion

Our results help identify what features should be a priority for formal methods researchers and practitioners interested in formally verifying PMs.

Moreover, our work has shed a light on a previously uncharted area of research --- formal verification allied with usable security.

This work was partially funded by Fundação para a Ciência e a Tecnologia (FCT) and CMU Portugal Program, in the context of the PassCert project (CMU/TIC/0006/2019) and the GOLEM project (ANI 045917).

Carnegie Mellon Portugal
fct Fundação para a Ciência e a Tecnologia
inesc id lisboa
PassCert
TÉCNICO LISBOA