2. Related Work and Background

In this section, we briefly review the related password and password man-

ager research, and provide the background information on the BPMs of the

five most popular browsers.

2.1. Related Work

Morris and Thompson pointed out long ago in 1979 that weak passwords

suffer from brute-force and dictionary attacks [7]. Later, Feldmeier and Karn

further emphasized that increasing password entropy is critical to improving

password security [5**]. However, strong passwords that are sufficiently long,**

**random, and hard to crack by attackers are often difficult to remember by**

**users due to human memory limitations. Adams and Sasse discussed pass-**

**word memorability and other usability issues and emphasized the importance**

**of user-centered design in security mechanisms [4].** *Yan et al. [8] analyzed*

*that strong password requirements often run contrary to the properties of*

*human memory, and highlighted the challenges in choosing passwords that*

*are both strong and mnemonic****.* Recently, Florˆencio and Herley performed a**

**large-scale study of Web password habits and demonstrated the severity of the security problems such as sharing passwords across websites and using**

**weak passwords [12].** A large-scale user study recently performed by Koman-

duri et al. demonstrated that many Web users write down or otherwise store

their passwords, and especially those higher-entropy passwords [6].

To help Web users better manage their online accounts and enhance their

password security, researchers and vendors have provided a number of solu-

tions such as password managers [21, 22, 23], Web Single Sign-On (SSO)

systems [24, 25, 26, 27], graphical passwords [28, 29, 30], and password hash-

ing systems [31, 32, 33]. As analyzed in Section 1, **password managers espe-**

**cially BPMs have the great potential to well address the challenges of using**

**many strong passwords and protecting against phishing attacks. The inse-**

**curity of third-party commercial password managers such as LastPass [34]**

**and RoboForm [23] are analyzed by Zhao et al. in [35].** *Web Wallet [21]*

*is an anti-phishing solution and is also a password manager that can help*

*users fill login forms using stored information; however, as pointed out by*

*the authors, users have a strong tendency to use traditional Web forms for*

*typing sensitive information instead of using a special browser sidebar user*

*interface. In addition, Web Wallet is not cloud-based. In terms of Web SSO*

*systems, their security vulnerabilities such as insecure HTTP referrals and*

*implementations are analyzed in [24, 36, 37], their business model limitations*

*such as insufficient adoption incentives are analyzed by Sun et al.* in [25], and

their vulnerabilities to phishing attacks against the identity provider (such

as Google and Facebook) accounts are highlighted by Yue in [38]. Security

limitations of graphical passwords are analyzed in [28, 29, 30]. Security and

usability limitations of password hashing systems are analyzed in [39, 31].

We do not advocate against any of these other approaches. We simply focus

on the BPM security in this paper.

2.2. Password