CHI'22-Lesch-"It Basically Started Using Me:" An Observational Study of Password Manager Usage

概述：(S)目前很少研究揭示用户在实际中如何使用PM以及其中的原因.(T)本文旨在弥补这个gap,(A)通过对32名PM用户的调研,并采用grounded theory.(R)本文发现许多用户同时使用browser-based和第三方的PM;他们尽量避免使用PM生成的口令;难以使用PM的audit功能;用户很少使用移动端的PM,作者给出了背后的具体原因,并且对其它的发现做了介绍.

优点：①通过observational interview揭示了许多用户使用PM的背后的原因

②对文献的引证较好.

问题：①Observational Interview不应过多在过程中干扰用户,否则会造成用户答案误差变大

②对于多PM的使用,应当无法避免此类使用场景,可以设置二者的使用优先级

③本文研究多数为确认前人的研究成果,应给出具体的对比来突出本文的贡献.

1. The effectiveness of PMs is limited if users fail to fully leverage the manager's rich feature set or use the manager in unexpected ways.

找出用户未使用或误用的PM功能.

2. 关键结果(32名PM用户)

1> 66%(21/32)的参与者同时使用多个PM, 41%(13/32)使用browser-based和external PM组合.

▲但对browser-based PM的采用可能是预料之外的,点击出现的弹窗后便采用了.

另外,部分用户使用的原因为使用1个作为另一个的备份,担心一个失效后无法访问自己的帐户.

2> 参与者需要在没安装PM的设备上输入自己的口令,因此会避免使用PM生成的随机口令. ☆(全面的设备无法建立)

3> 参与者很少使用口令审计的功能,虽然很感兴趣,但是认为警告的数目过多,以至于用户不知道哪个最重要.(对Usability的研究很少).

▲很喜欢Chrome的凭证泄漏警告,自动给出提示,且告知了用户需采取的措施.

4> 移动端PM的使用很少,造成的原因:

①autofill和autosave功能的不一致 ②桌面端和移动端同步的不一致.

③在移动端应用和网站的登录会话持续时间较长. ④对SSO更偏爱.

▲即使使用PM,也很少使用它的autofill和autosave功能

5> PM的采用的主要来源为:

①工作需要 ②简化凭证输入的过程. ③改善口令的质量.

▲对于选取的PM,用户依赖于朋友,同事或可信的来源

81%(26/32)不会推荐给除家人以外的人(即使推荐成功率也很低).

对2>的解释：担心在PM不可用时难以输入复杂的口令,特别是在不方便输入的物联网设备中.

另外担心自己无法记忆生成的口令.

3. 研究方法(询问过程)

①PM的一般使用方法. ②使用临时帐户登录两个不同安全级别的帐户(是否使用不同的口令策略)

③登回两个帐户(是否使用自动填充),并更新口令 ④口令创建、存储和autolock功能,是否可以填充口令到桌面App上

⑤是否共享口令,是否注意到PM的这个特征.

▲采用4阶段的grounded-theory

①open coding：3位研究人员细致研究,分类.

②axial coding：使用constant comparative method将code分组成多个concept

③selective coding：将不同的concept进一步分成不同种类.

④theory generation：将不同类和联系构成map,用于生成人们如何使用PM的theory

4. 局限性

1> 由于COVID-19,只能找MTurk的参与者且只能线上访谈.

2> 样本均为美国人,且MTurk的样本倾向于年轻化,接受过更好的教育且更懂技术,对隐私的为关注

3> 选用的用户均为PM用户,且多为LastPass和Chrome的用户.

4> 由于调研的性质,以及调研者需持续观察,可能会影响用户的行为.

5> 由于使用假帐户无法捕获用户对日常自己帐户的态度.

6> 对一些未知的功能的介绍可能会改变参与者的态度.

5. 结果的补充内容

1> Adoption of Multiple Managers.

19%(6/32)在桌面和移动端使用不同的PM.

不使用多个PM的原因(9%, 3/32):存储口令在多个地方不安全;

▲Browser and External Managers

①担心存储在External PM的口令会丢失,使用Browser作备份

②由于习惯性地点击浏览器的弹窗而使用了浏览器的PM.

③希望一个不可autofill时,另一个可以补上, 13%(4/32)发现两个PM均添加了值, 19%(6/32)发现多个PM会互相干扰.

▲Other Patterns. 19%在phone和desktop设备上使用不同的PM.

2> Password Entry and Reuse. 25%(8/32)重用口令

跨设备的输入(特别是在一些无法安装PM的情况下)无法满足,导致用户不愿使用生成的口令

①在无PM的autofill的功能的情况下难以输入生成的口令.

②担心无PM的情况下无法访问自己的帐户.

▲但对于不担心cross-entry的用户则认为PM很易用

▲即使参与者记忆了口令,他们仍喜欢PM的autofill的功能

▲发现用户会选择临时数据(如眼前的事物)作为口令并存储在PM中.

3> Overwhelming Credential Audits

用户通常会避免heath check,因为会面对许多问题和错误.

但参与者喜欢Chrome提供的帐户泄漏提示,可以及时发现问题并进行修正.

而credential audit services与Chrome自动化的提示不同

①需用户手动开启audit过程. ②同时audit用户的所有凭证.

③可以找出所有的问题但不提供严重程度以及解决方法.

▲用户会更改口令的情况：
①对口令泄漏的响应 ②周期性地更改重要的口令 ③由网站强制要求

4) Limited Mobile Usage
参与者很少使用移动应用PM，即便安装了也很少使用原因包括：
①功能（特别是autofill和autosave）有时无法使用。
②移动端和桌面端的口令同步存在问题，在另一个平台上无法访问，导致用户使用易记的口令，除非在使用桌面端存储时会使用强口令。
③参与者很少在移动端进行身份认证，而且许多移动端帐户在登录后会有较长的在线时间
有用户把移动端PM当作可以查阅的口令库，不使用其它的功能（但复制粘贴有安全隐患）

6. 其它发现
1) Adopting a manager.
3点原因：①工作需要PM. ②可以便生活更容易 ③可以增加在线帐户的安全性。
促进采用的因素中25%(8/32)为外部推荐（朋友或其它可信的在线资源）。

2) Prompting a manager to others.
推荐难以成功的原因是参与者无法帮助别人建立正确的mental model，无法给出PM可以提供的便利性和可用性。
▲但是可以为家庭成员或亲密的朋友推荐成功。便利性是最关键的因素，另外可以为家人提供更高度的信任级别，也愿花时间建立正确的mental model

3) Password Sharing.
许多参与者没有意识到该功能的存在，9%(3/32)的参与者认为该功能在工作中很有用。
但许多用户由于共享失败或不知道对方是否有PM而采用发送信息或由附件的方式共享。

4) Inconsistent Autofill and Autosave.
一半的访谈中，PM没有正确识别登录表单，也无法存储新的或更新的凭证。
例如在两页的登录表单中，但参与者认为这不算作一个严重的问题。
为了解决这个不一致性，用户会选择在其它位置保存口令。（即产生一系列不安全行为）

5) Attitudes Towards Autolock.
13%(4/32)的用户认为external PM的autolock功能十分让人厌烦。
认为这项功能不会增加安全性反而会增加不便。

6) Ubiquitous Default Settings.
用户很少更改设置，故才用有安全的默认设置十分重要，因此PM应提供更恰当的默认设置

7) Desire for Single-Sign-On.
用户希望可以尽量减少帐户数目（即使有PM负责管理），也可以在PM存储更少的口令（用户希望可以记住存储在PM的口令）

8) Impacts from COVID-19
9%(3/32)的参与者提到COVID-19影响了PM的使用
9%(3/32)的参与者称居家时使用PC也减少了对Mobile PM的使用。
一位参与者认为口令共享在COVID-19期间很有用。

7. 改善PM的可用性
1) Multiple Manager Usage
▲built-in PM需改善安全性与external PM一致，或者在external PM安装时自动失效
▲改进autosave的一致性以及credential同步等问题，避免用户使用另外的PM
▲提供数字或物理的数据备份

2) Generate Usable Passwords
当PM不可用特别是移动设备时，使用户更容易输入凭证

3) Seamless and Targeted Credential Audit
①audit应自动执行并主动给用户提示
②提示信息应尽可能短且可执行

4) Limited Usage of Advanced Features.
PM应主动让用户得知PM新的功能

▲单纯的访谈不如observational interview观察到的信息多