USENIX Sec'22-Mayer-Why Users (Don't) Use Password Managers at a Large Educational Institution

概述：(S)口令管理器(PM)可以有效改善口令管理的问题，但用户由于安全性和可用性等原因不使用PM. (T)本文评估了当前PM的使用情况和影响使用率的因素. (A)为大学中不同背景的人员发放问卷，内容包括是否了解PM，是否使用PM，使用或不使用的原因等. (R)作者进一步使用logistic regression对数据进行分析，分析哪些因素对采用率影响最大，对于不同类型的PM，最大的影响因素不同，另外组织机构和人为的支持和宣传也有助于提供采用率，作者最后为组织机构和PM开发人员提供了建议.

优点：①详细描述了研究方法和方法的局限性，也给出了详尽的问卷内容。②定量分析了解认了前人的结果，也给出了一些与前人结果不同的结论

问题：①统计学的术语和缩写在正文和表格中未给出明确的解释，降低可读性；②5.3节对PM开发者建议改进UI设计，这一建议无法从前文的分析中得出；③部分现象未给出明确原因，例如当PM机构免费提供时，为何部分PM用户不愿使用PM，作者应简要讨论.

---

1. 用户不使用PM的可能原因

①增加管理需求 ②带来了其它可能发生的问题(complication) ③担心无法访问自己的口令 ④认为当前的口令生成习惯是可行的 ⑤认为PM没有改善当前的口令生成习惯.

2. 研究方法

1) Research Questions

① Awareness：探索参与者是否了解PM及其三种类型.

② Password Strategies in General：探索参与者创建、查找和重用口令的方式，探讨PM对口令管理的影响

③ Institutional Account Management：探索参与者如何管理大学帐户(可用于登录PM的mpw).

④ Motivations & Barriers：探索总结采用PM的动机和障碍

2) Research Structure.

① Informed Consent：告知参与者研究的目的、结构、长度及抽奖环节.

② Affiliation with the George Washington University：确认参与者在大学中的角色

③ General password management：询问用户如何管理不同帐户的口令，此外在给定的列表中选择特定的技术(及组合)，最后询问用户是否重用口令.

④ Password synchronization methods：询问参与者如何在多个设备中共享或同步口令值.

⑤ University account password management：询问参与者对学校帐号的管理方法，是否与其它帐号相同

⑥ Introduction to PMs：向用户介绍PM，并通过Likert-scale询问用户有关PM的8个问题

⑦ PM user questions：询问用户如何得知PM，使用的PM和使用原因以及是否满意

⑧ Non-PM user questions：询问用户不使用PM的原因，是否使用一段时间后停止；是否会再次使用PM

⑨ IT skills：询问参与者的IT背景和对计算机的熟悉程度(包括web和security)

⑩ Demographics：参与者提供个人的背景信息 ⑪ Raffle：询问用户是否想参与抽奖

3) Data Analysis.

▲采用logistic ordinal regression分析影响PM认知和使用的因素，其中上述的8个Likert响应映射为agree & disagree，参与者角色记为student和non-student，web-skill和security attitude为平均响应，参与者身份信息为控制变量.

▲使用statistical tests测量Likert-scale和closed-response questions，使用基于inductive coding的open-coding分析open-ended responses

4) Recruitment and Demographics：给2000人发送电邮，27人响应；参与者身份信息多样

5) Limitations:

①很难保证参与者遵循了指示 → 让用户在不同页面花费一定时间并且浏览开放式响应确保数据

②研究在一个大学中进行无法覆盖所有可能现象，且部分信息存在缺失 → 由专业组织调研保证信息多样性

③各研究可能有一定的social desirability bias，参与者可能修改响应使其在安全性研究中看起来更好

④研究可能有一定的response bias，了解PM的人可能更愿意去参与，导致结果存在一定bias

6) Ethical Considerations. 研究经过了IRB的批准，参与者了解研究的目的、结构和风险，研究不会收集任何隐私数据

---

3. 结果(关键的结果信息)

1) Awareness

①询问参与者是否了解PM以及了解方式：Word-of-mouth是最多次数的方式，占所有参与者的28%

②运用logistic regression统计影响对PM了解的因素，发现web skill影响最大，但security attitude没有明显的关系

③调研中两次询问参与者对PM 3种类型的了解. 客服人员对PM的类型有误解(但对第三方PM的理解最好)

2) General Password Strategies.

①口令管理策略：70%用户记忆口令，60%使用浏览器自带的PM，10%的用户选择登录和重置口令组合多种策略的原因：使用频率不同，一些口令存储在PM或写在纸上；冗余存储防止忘记；用于区分不同场景的帐户；在不同的策略之间切换.

②77%的参与者使用PM，74%的参与者对PM的使用是满意的(不同程度的)

③同步口令：PM用户通常通过PM同步口令，非PM用户可能使用额外的工具

④口令重用与口令生成器：77%的参与者重用口令，第三方PM用户的重用率较低，每次登录即重置的用户最可能重用口令；67%的用户不使用PM生成口令. 使用logistic regression得出security attitude和perceived security of PMs对口令生成器使用的影响最大.

3) Strategies for the George Washington University Passwords

①大多数参与者的大学口令至少与其它帐户一样强，最多的原因为该帐户很重要

②创建该口令的策略大多数为重用(例如变形)，也有包含特殊字符和个人信息，采用这些策略的原因最主要的为可记忆，也有安全性

4) Motivations & Barriers

①综合来看，ease of use和transparency较明显地增加了PM的采用率；对于基于浏览器的PM

security attitude和 ease of use影响最大；对于基于OS的PM，ease of use为主要影响因素，对于第三方PM，security attitude，perceived security of PMs和 perceived transparency of PMs影响最大。参与者的身份与不采用的比率有关.

②使用PM的参与者的最主要原因为 ease of use，memorability，部分参与者由于安全存储和口令的唯一性使用PM。PM用户最喜欢的部分为 autofill，其次为 memorability.

不使用PM的原因多数为安全性的考虑，但部分可能再次使用(convenience&security)

▲另外，调查研表明若PM由组织免费提供，非PM用户一部分会愿意使用PM.

③不采用PM的主要原因为安全性担忧，另外有参与者认为不需要PM。最不喜欢的部分为安全性担忧，在不兼容的网站或设备中仍需要手动输入口令(或PM不可用时)

4. 建议

1)对组织机构的建议

①机构的推荐可促进PM的使用，且可以减轻 trust带来的问题

②利用口头宣传也可提高PM的使用率，可减轻对PM的担忧和误解.

③机构可以给PM投资，使员工免费使用PM，也可提高使用率.

④促使基于浏览器的PM的用户转向第三方PM

⑤为已知兼容性问题提出建议

2)对PM开发者的建议(特别需要改善基于浏览器的PM)

①进一步改进基于浏览器的PM的UI设计，使PM的功能更明显.

②由于许多用户会忽略浏览器PM的口令重用警告，需要改善对应的对话框设计使其更明显