ACSAC'21 - Simmons - Systematization of Password Manager Use Cases and Design Paradigms

概述：(S)之前关于口令管理器的可用性(usability)只包含了部分使用情景，更多的研究集中于口令管理，很少涉及PWM的设计(design paradigms)，这个gap导致不同设计的优势和劣势不清楚。(T)为了弥补这个gap进而改善PWM的设计。(A)本文将口令管理的用例和设计范式系统化，主要通过回顾口令管理文档，调研了12个桌面PWM和12个移动PWM以及回顾相关文献，发现了7个用例，涉及了7个设计范式，另外使用了cognitive walkthroughs研究了PWM中的可用性挑战。(R)本文给出的设计范式有助于改善PWM的设计，同时也出了一些关键的研究问题。

优点：①指出之前有关PWM可用性的研究不够全面
②通过调研，给出了PWM的7个用例，涉及7个设计范式
③使用认知走查法揭示了许多PWM可用性的问题和研究挑战

问题：①认知走查法本身具有一定的局限性，无法代表真实用户；若有更多人员进行测试结果更全面
②作者最终未给出各个设计范式优势和劣势的总结，应进行一个说明，特别本文提出的设计范式与已应用的设计范式的比较。
③作者应在实验介绍部分给出更多解释，如为什么只对8个流行桌面PWM进行认知走查法，为什么采用附录A的测试流程等。
④引用不够全面具体，第3节应提供更有说服力且准确的引用。

1. PWM要解决的问题
1> generate strong passwords (avoid weak passwords)
2> store those passwords (encourage unique passwords at every website)
3> fill those passwords (ensure passwords are only sent to the correct website)

2. ~~用户用例~~ 使用用例
1>研究用例分类的数据来源：①PWM的文档 ②查看最流行、下载量多的桌面和移动PWM.
③相关的研究文献

2> Essential Use Cases (10) 除Edge不支持password生成外，其余用例，所有PWM均支持
①Setup manager：首次使用时安装、配置PWM(多数包括设置用于同步的在线帐户)
②Register credential：注册新的凭证和域名或将凭证与多个域链接起来(共用后台认证系统)
③Update credential：帐户恢复或口令重置时更新凭证.
④Remove credential：移除或清空PWM中的凭证(凭证过期或移植到另一PWM时)
⑤Autofill credential：自动输入、填充凭证.
⑥Manually enter credential：在无PWM的情况下，允许手动输入凭证(或autofill失效时).
⑦Generate password：帮助用户生成strong and unique的凭证或根据用户需要生成
⑧Sync credentials：允许用户在多个设备之间同步凭证.
⑨Lock manager ⑩Unlock manager：锁定和解锁PWM.

3> Recommended Use Cases. 大多数PWM均支持的用例
①Audit credentials：帮助用户识别重用的、弱的口令，以及在泄漏集中的口令
②Modify settings：修改PWM的默认设置.
③Recover access：在用户无法访问帐户时提供恢复访问的服务(此时，PWM的安全性与恢复机制的安全性相同)

4> Extended Use Cases 并未广泛使用的用例
①Migrate manager：在不同PWM之间转换，并安全停止原有的PWM.
②Share credentials：与其它人共享凭证，包括更新、删除及共享使用的凭证
③Manage identities：允许凭证在不同实体之间分隔，后续包括添加、移除实体，实体转换等
④Store sensitive data：存储凭证之外的结构化或非结构化的隐私数据

3. 设计范式(design paradigms)
比较设计范式有助于识别不同范式的优势和劣势，有助于设计和实现PWM.
本文从high-level的角度，分析了12个桌面PWM和12个移动PWM，并结合之前的研究分析得到设计范式
→可标识哪些设计范式使用广泛，哪些支持较少以及哪些通常一起出现.
▲本文共标识出7个设计范式，其中6个在实际PWM中应用，3个在文献中，另有9个是本文提出的
包括：①Auto-detect removal ②Download the PCP ③Partially automated sync
④Identify unused passwords ⑤Prioritize audit recommendations ⑥Audit settings
⑦Disable the prior manager ⑧Share credentials with non-users ⑨Protect an identity with a PIN

4. Cognitive walkthroughs (认知走查法) 评估了8个流行的桌面PWM，包括7个任务(附录)
1>采用认知走查法的原因：①在找到low-hanging可用性问题方面高效.
②允许探索更大的用例和工具的集合
任务结束后描述观察到的情景及产生的困惑，后期会定期被提问
2> 观察
①在未安装PWM的设备上手动输入口令是比较困难的
②一些PWM的设置过程是比较繁琐的
③将多个共用一个认证系统的PWM链接到一个凭证上是较困难的
④许多PWM的UI的接口难以理解，容易出错
⑤基于OS的PWM(如keychain)的内部逻辑难以理解，且即使从Safari登出，也可看到注册信息(虽然在无account password时不会泄漏口令，但也泄漏了其它信息)
⑥基于Browser的PWM功能最受限，且即使云端登出，本地仍存有此信息容易暴露(需更多研究)