SOUPS'19-Pearman-Why people (don't) use password managers effectively

概述：(S)专家推荐用户使用口令管理器(PM)存储并管理口令，但当前的采用率不高，许多用户不知道PM是什么，怎么用，是否可信；(T)本文旨在研究用户为何(不)使用口令管理器，(A)对30位用户进行了半结构化访谈，包含9位未使用过PM，12位使用built-in PM和9位使用独立安装的PM，询问他们使用或不使用(某种PM)的原因，以及对现有管理方式的不满，(R)给出用户(不)使用PM的可能影响因素，结合前人的研究，给出更深入的讨论和可实行的建议

优点：①调研过程的描述和方法结果的分析比较详细，且较清晰

②通过半结构化的访谈探究了用户使用或不使用PM的原因.

③作者给出了方法的局限性和本文的未来工作

问题：①由于人数较少无法反映普遍的现象，且参与者的身份特征有一定的bias

②对于存在的问题，没有全部给出改进建议，如生成口令不符合网站需求

③没有讨论内置PM用户不采用独立安装PM的原因

---

1. 研究方法

1>采用purposive sampling确保参与者使用了不同类型的口令管理策略.

2>首先采用short screening survey确定参与者的合规性，帐户数目，采用的设备及OS，采用的口令管理策略，是否经历过数据泄漏以及基本信息

3>在填写知情书后进行访谈，记录成interview transcripts后采用inductive coding进行分析，通过计算Cohen's kappa为0.84表明两个coder的意见一致

4>局限性

①本文是定性分析且采用的是purposive sample，选取访谈的人群存在一定倾向

②由于screening survey和purposive sampling，参与者可能已知研究的是安全课题，可能导致priming和Hawthorne effect.

③用户可能不报告个人的口令习惯

---

2. 结果

1>口令管理方法：(USENIX'22)

①不使用特定工具的方法：记心口令，写在纸上，写在邮件中，列在文件或记事本中，重置口令

②Built-In PMs：使用浏览器或OS的标准PM，且若浏览器和OS来自一个公司，则可以集成起来进而同步口令.

③Separately Installed PMs：需用户额外安装PM.

④其它方法：使用混合的或自定义的方式存储口令.

2>当前口令习惯.

①帐户数目：独立安装PM帐户最多(通常>100)，内置PM和非PM用户的帐户通常少于50

②口令重用：非PM用户和内置PM用户口令重用较严重，而独立安装PM多采用随机生成的口令

③是否使用口令生成功能：内置PM(→采用不同策略生成)和独立安装的PM均提供了，但内置PM用户使用特性相对少

④对主口令的处理：部分采用随机生成的口令，存在直接重用的情况

3>不使用PM的参与者的经历

①(略)对当前的管理方法满意

②对当前管理方法的不满：难以记忆；难以组织；当记录的文件不在手头时会造成访问问题；具有潜在的风险.

4>阻止参与者使用PM的因素：①未意识到PM的存在(↑不知道/在清单保存口令) ②认为不需要保护 ③担心单点故障 ④过去有使用PM的糟糕经历

5>使用内置PM的用户的经历

①喜欢的特征：autofill，同步功能(此外，这组用户中一半人提到喜欢重用口令)

②不喜欢的特征：担心另人可以访问到其中的口令；在另一台未安装浏览器的设备难以访问帐号更改口令之后，工具不更新其中的口令.

③采用内置PM的主要因素：有提示；方便；有助于减轻记忆负担(无人提及安全性和可以产生唯一随机的口令).

④影响有效使用内置PM的障碍：不正确的风险评估，低估了自身所处的风险，认为自己的帐号没有那么重要；对PM缺少足够的认知和了解，对不熟悉的软件产品担心

6>独立安装的PM的用户的经历

①喜欢的特征：可以存储口令及其他的数据；可以生成随机、唯一的口令；可以在设备之间同步，可移植性；可自动填充口令并通过检测避免钓鱼攻击

②不喜欢的特征：部分PM无法正确存储用户名和口令，甚至只填充了口令就尝试提交；在浏览器中的插件可能与浏览器内置PM冲突；在不兼容PM的设备中输入随机生成的长口令时存在困难；生成的口令不符合网站的需求；部分PM必须手动同步，无云存储，用户会担心mpw丢失.

③采用的动机：使用唯一随机口令时缓解记忆负担；增加安全性；避免手动输入；认为PM提供了加密

---

3. 建议

1>非PM用户：采用推力，教育或浏览器提示使用户更显著注意到PM的功能

2>内置PM用户：改善UI设计，改善口令生成工具让用户可以方便安全地产生随机口令

3>独立安装PM的用户：提供改善口令强度的方法；提供免费的或试用的版本