IT Pro'16 - Arias - Comparing Password Management Software: Toward Usable and Secure Enterprise Authentication.

本论述：(S) PM被广泛推荐使用，但安全性和可用性可能存在问题；(T) 本文基于专家知识和通过用户调研的实证分析，评估PM的安全性和可用性。(A) 评估3种主流的PM(免费)。可用性通过用户调研采用06年的5个task及5E评价指标，安全性研究集中于master key，凭证以及通信的安全性。(R) 可用性得分4.07~5.07(of 6)，安全性得分1.13~1.80(of 2)，Dashlane最好，keePass最差。支持expire机制，最后为企业中的PM提供3未来的研究方向。

优点：① 可用性和安全性的定量分析较好。
② 第一段中许多表达可以学习，例：stories of such breaches have been front page stories…
③ 对企业环境中PM的应用提出了许多见解

问题：① 未给出14位参与者的身份信息，实际上无法判断选择样本是否合理。
② 本文建议定期更新口令，但有研究(ISSA'17 Renaud)讨论是否应要求口令过期策略，认为应不R从安全性分析，也应从用户体验考虑这一点要求
③ 安全性指标为启发式，应说明合理性或使用更权威客观的指标。

▲用户不安全的口令行为除了给个人带来危害，且严重威胁企业的安全：
A breach on an employee password could leak highly sensitive data and cause significant business and reputation damage.
• 研究表明越严格的policy将越可能导致用户采用不安全的实践(对抗带来的mental model)

▲在企业中，PM除了发挥自身的作用之外，还可以带来economic benefits：
① reduces the cost of helpdesk calls related to password issues
② minimizes the time employees dedicate to tasks that are not related to their work(如login)

▲研究3种流行的免费的PM应用：Dashlane, keePass, 1Password, LastPass

▲Usability Analysis.
1>评估指标为5E，可用的软件应满足如下要求：
① Efficient：用户正确完成任务时的速度如何
② Effective：用户是否完整且正确地实现了特定的目标，取决于用户目标是否完成以及是否正确
③ Engaging：接口应使用户pleasant且satisfied，应特别考虑PM的可视化设计
④ Easy to learn：用户不需要特别费力就可以使用
⑤ Error tolerant：应减少与用户之间的交互错误，且可以帮助用户从错误中恢复。

2>采用06年Chiasson研究的5个任务：① initialization ② login ③ remote login(可移植性和同步性)
④ password change(使用PM更改口令) ⑤ login with changed password.

3>采用seven-dimension的Likert scale，代表分数(由高到低)：6~0，定量研究PM。
共有14位用户参与，通过在线问卷工具完成

4>结果
① 4个PM在efficiency, effectiveness和error tolerance上评分较高，多数接近5分(满分6分)
② engaging和easy-to-learn则存在不同，最高点和最低点之间相差多于2分，keePass在这两类最差
③ 所有PM的平均得分均高于3分；Dashlane最好。
④ 表明从可用性角度用户接受PM，但企业应注重engaging, easy-to-learn，且应该使转变更平滑

▲Security Analysis.(基于启发式分析，并按照是否满足NIST等权威机构的guideline评价)
1>评价指标(PM架构以及通用安全性)：
→ Security of the master key (SM)
① minimum mandatory length：强制的最小口令长度。(R有Dashlane有)
② user must apply policy for strong master key 采用严格的policy(R有Dashlane有)
③ master key securely stored：安全存储，均提供
→ Security of the credentials database (SDDBB)
① algorithm used for database encryption. 除keePass(还有Twofish)，均有AES-256
② the PM gives feedback on the security level of the stored passwords
给出存储口令安全级别的反馈(均提供)
③ automatic generation of strong passwords on the users' behalf：自动生成(均提供)
④ multifactor authentication：均提供，1Password R在macOS和iOS提供
⑤ can schedule password validity periods and generate new passwords upon expiration.
设置口令周期并在过期时生成新口令，仅Dashlane和LastPass提供
→ Security of communications (SC).
① security of the communication algorithm between the PM and external servers
仅Dashlane和LastPass使用HTTPS(它们]提供云存储)，且提供PFS特性
② Security of the communication algorithm between the PM and the browser plugin.
仅Dashlane提供，使用AES-256.

2>定量分析(1提供，0不提供)
▲ masterkey不存储在本地或远端，采用基于password的KDF函数生成(可能执行多次)。
分析中未考虑通信的安全性，比较PM的核心功能
▲ 最安全的为Dashlane，1.8分(满分为2)。
所有的PM的安全性尚可，最低分为1.5分(1Password)

▲有关于企业中PM的未来研究方向：
① 自动化集成并执行企业的安全策略。
② 在企业内部环境中将PM与SSO组合使用
③ 通过引入implicit authentication-替代master key改善可用性。

▲其它认证方式：
① SSO：认证一次可访问许多站点，但需提前建立信任
② Pico：smart client authentication：使用设备存secret进行登录，需server更改。
③ implicit authentication：检测用户行为模式进行会话管理，无法避免多口令登录。