SecureComm'20 - Stobert - ByPass: Reconsidering the Usability of Password Managers

大概述：(S) PM由于糟糕的可用性，移植帐户比较困难以及用户普遍认为PM没价值等原因而采用率较低。(T)作者首先剖析了PM采用率低的一个原因：用户需参与众多的口令管理任务，并提出Bypass使用户的交互任务最小。(A)作者为网站提供了API接口，进而使Bypass PM可以直接与网站交互 (R)经过两个阶段对参与者通过问卷调研和可用性分析，表明Bypass具有较高的可用性，帮助用户更好、更安全地管理帐户。

优点：①提出了PM的新的设计，处于网站与用户之间，减少用户与PM的交互，由PM与网站交互。

②给出了可用性分析实验，结果看起来具有说服力（指出用户对共享口令等重控制的担忧）

问题：①方案必须让网站更改，集成PM提供的API，较难实现（是否比SSO更好也未知）

②未给出可用性研究的可能问题及局限性

③本文提出的方案与SSO场景类似，但实际为一种Pseudo-SSO，首先用户通过TWT向PM认证，TWT通过什么渠道获取没有说明，若声明实体分发TWT，本文方案难过于庞大。另外用户、PM与网站之间的信任应如何建立，若恶意网站诱导用户存储其他网站口令，则可能造成泄漏

▲ ByPass的主要目标：提供更可用的PM使用户口令行为更安全，且使各项任务更加容易

1、设计思路 减少点击和操作的次数，不需要用户过多地参与

1> PM的可用性问题的主要原因是PM作为用户与网站的中间实体，只与用户交互，导致许多用户参与才产生的问题（如错误字段，粘贴板的泄漏）

2> user ⟷ ByPass (PM) ⟷ (API) Website.

① PM为网站提供API，可以直接将凭证发送给网站

② 采用nudge让用户采用安全的选项（比如默认提供随机口令，用户若想选择需多步骤）

③ 需要网站必须实现API才可完成实现（新的设计思路）.

④ PM处于两者之间，并与两者交互，可以提供更多的功能（如自动化口令更改）.

3> ByPass提供的功能

① Adding Accounts：PM与网站交互，用户将域名发送给ByPass，ByPass请求网站得到表单，网站同时发送口令策略给PM，PM可以为用户生成符合策略的口令。ByPass也可以存储现存帐户（像传统的PM一样）.

② Account Login：用户可以直接在ByPass着页点击Login按钮，ByPass发送用户名和凭证给网站，不需要用户与网站直接交互.

③ Password Changes：在更改帐户的页面中，可以查看口令，更改口令，也可以设置自动更新定时器.

④ Account Deletion：可以通过更改帐户页面直接删除帐户.

4> 实现细节.

Browser Extension

JS + Indexed DB. ⟷ (JSON) [API] ⟷ Server: Web Application + MySQL DB.

使用JWT进行认证；使用离线数据库存储口令.

2、安全性分析.

① 离线字典攻击：使用PBKDF2生成的口令使用AES-256加密数据库.

② 在PM和网站之间的通信，采用TLS通信.

③ 避免了Autofill相关的安全问题，也没有与复制到粘贴板相关的一系列问题.

④ 防止在用户界面的暴力攻击：可以在多次尝试master password后增加时延.

3、可用性评估.

1> 初始版本的评估：采用认知走查法，找到用户存在的问题，例如对用户界面的困惑和较弱的mental model，采用一定的方案进行改进.

2> In-lab User Study

①测试：用户如何学习使用ByPass，对于这些功能的响应，评估如何使用API帮助用处理网站的相关工作？（未提供与其它方案的对比，原因是认为与其它方案的设计思路不同）

▲参与者信息：20名参与者，12位女性，15位有过PM经历，3位称PM是存储口令的主要方式.

4、结果.

1> 指标：efficiency：每个任务所用时间

effectiveness：记录研究中发生错误的次数和类型

satisfaction：采用Likert scale问题.

包括参与者的完成情况，评论，问题和建议.

2> ▲ 95%的用户使用ByPass生成的口令，意味着本文给出的nudge成功了.

3> 出现的错误：多数参与者没有出现错误，最大数目是4，关注类别和出现频率

▲ 注册过程中出现错误最多，两次输入的口令不匹配，选择足够强的mpw较困难等

但多数错误不是由ByPass引起的

4> 对可用性的感知 Usability Perceptions.

① 认为ease-of-use的部分：口令更改和网站登录过程，创建帐户，添加现存帐户.

移植第三方帐户到ByPass也较容易，

② · ByPass评价中等偏上的特征：感知的安全性，选择主口令的过程，

专家参与者认为若ByPass的结构更明显，将更受信任

▲ 参与者最不喜欢的是：不知道真实口令，对口令生成和自动更改评价不同.

31%用户希望使用自己的口令