S&P'21 - Huaman - They Would do Better if They Worked Together: The Case of Interaction Problems Between Password Managers and Websites

总结：密码管理器(PWM)是一种安全生成、存储凭证并帮助用户登录的工具，过去的许多研究表明PWM面临许多安全性和可用性的挑战，PWM与网站之间的交互仍然存在较大的问题。
(1)本文首次定量分析了PWM和网站之间的交互问题，并分析了各个PWM如何受到这些影响。
(A)首先根据下载量及是否开源等属性选择了研究的PWM，接下来搜集了许多用户评论和Github issues的信息，将得到的问题分类并实现了对应的MWE，进而测试选择的PWM是否存在类似的问题。(R)分析所得到的PWM和网站存在的问题，并给出了建议。

优点：① 首次系统分析了PWM与网站之间的交互问题(来源于真实用户评论)
② 对PWM的概念介绍(第3节)和相关工作(第2节)介绍均较好，很详细
③ 本文的实验设计、实现描述详实，且提到自己实验方法的局限性

问题：① 本文的关注内容存在局限性，可引入其它开源网站的话题；另外，可以从移动端的PWM展开研究。
② 本文可添加两个内容：首先是PWM与网站之间的通信框架的整体描述，易于理解本文研究所处的范围；其次是，应介绍什么样的交互是好的或推荐的而不是只介绍交互问题
③ 对于表III的各个描述，应给出更清晰的描述，当前部分存在模糊情况。

一些问题可通过标准和最佳实践解决，而另有一些当前难以解决。

1、本文解决的3个研究问题：(3研究专注于桌面PWM及浏览器扩展)
1) RQ1：对于PWM，网络中的哪些交互模式有问题。
2) RQ2：PWM的浏览器扩展如何处理这些交互？
3) RQ3：可以如何改善PWM和网站之间的交互？

2、PWM可以通过生成、存储和自动填充安全口令来改善在线帐户安全性，用户可以不记忆口令，而且可以节约填充口令的时间
PWM需与网站交互，在认证过程中，通常提供以下的特征
1) Service Detection. PWM确定服务，进而确定要使用的认证数据(例如URL)
2) Credential Storage and autosave 核心功能，存储凭证(可以自动存储和更新)
3) Providing Credentials and autofill 主要功能，在访问服务时提供凭证(及自动填充相关值)
4) Automatic Login or autologin：较罕见，填充后自动登录。
5) Secure Credential Generation：在注册或更改口令阶段生成更安全的口令

3、用户投诉评估。
1) 选择PWM：Chrome Webstore中下载量超过1w的浏览器扩展PWM(部分为开源)。
2) 不同的用户评论的来源：
① 不同扩展的user reviews和support requests

3) 问题分类
使用iterative exploratory coding approach进行反馈分析。
去除无关的评论，评估不同条目的类别，进一步去除描述不够细节、难以复现的用例，后续用于构建Minimal Working Example (MWE)
4) 该实验的局限性。
① 只评估了浏览器扩展。② 对闭源的PWM存在的见解 ③ 评论有限且可能存在偏见
5) 总结出许多交互问题，用于下文的MWE构造。

4、交互问题评估
1) 方法：15个PWM包括前10个PWM，3个开源PWM(KeePassXC和Passbolt)和3个浏览器自带的PWM(Chrome, Firefox和Edge)，针对39个问题实现了585个测试用例
2) 可能的输出情况：
① Seamless：现象与预期相同，无需手工干预 ② Manual：与预期不同可通过手工干预得到预期结果 ③ No Solution Found：无额外交互时无法完成，虽有此功能但无法提供 ④ No Applicable：不支持所需功能
3) PWM的功能：Autosave, Autofill, Autologin，各个PWM实现不同，一些需手工干预，另外一些PWM可以在设置中设定该项。
4) 本实验的局限性：① 取样时间和版本 ② 评价可能存在一定的主观性和偏向性
③ 一些PWM的功能只在特定版本提供 ④ 一些PWM只用于特定网站
⑤ 不能百分百保证映射了所有的现实问题。

5) 交互问题描述。
▲ Additional Elements (Auth)
① 对于1个输入有多个输入密码段如PIN码时有5个输入框 ② 多个登录按钮
③ 网站包含不必需的认证相关的表单 ④ 网站除了用户口令还包括其它认证字段
▲ Additional Elements (No-Auth)
① 网站包括1个用于多个用户身份认证的主面板 ② 包括单选框和复选框等PWM不应识别的字段
③ 具有改变元素的站点(如下拉菜单)。 ④ 包括与认证无关的submit按钮
▲ Domain Matching
① 子域使用相同凭据的基域 ② 多个不同的域使用相同的身份认证方式(域迁移)
③ 子域使用不同服务的基域 ④ 登录可以通过HTTP和HTTPS进行
⑤ 登录后的重定向阻碍自动保存 ⑥ 在iframe的登录表单加载了不同网站

①具有多个有单独服务的路径或页面的基域.

▲Input Fields

①输入字段可能包括"code",易与TOTP混淆 ②输入字段有误导性或不常见

③输入字段具有误导性或不常用的类型 ④在输入字段使用了autocomplete属性

⑤无输入字段类型的信息 ⑥使用textarea 用于 username 输入

⑦输入域元类型属性 ⑧输入域的最大长度小于预生成口令的长度.

⑨网站对输入值做语义等价处理.(如变大写).

▲JavaScript.

① 隐藏口令字段 ②只有注册 keypress 事件后才可以启用提交按钮.

③认证通过几个页面的多个步骤进行,例输入用户名后口令字段才出现

④....多.....口令字段在下个页面出现

⑤网站以某种方式修改输入(替换为%20 添加空格,删除自动输入)

⑥网站的口令字段为假值,而交互时为真值.

▲Non-Standard Form.

①登录不通过表单而通过ajax ②表单元素为自定义Web Component Tag

③Submit 按钮为div定义的 ④表单的submit按钮不是其一部分

⑤通过超链接而不是submit按钮触发JS.

▲Timing

①初始化认证界面时有延迟 ②输入TOTP和提交的延迟.

▲Web Standards

①使用HTTP basic authentication作为登录方法

②HTTP basic authentication 的多个文件向服务器发多个身份认证请求,可能由于request-reply不匹配而失败.

5、讨论

1)用户评论

没有用户反馈包含口令生成,也表明一些问题并未被关注.

2)建议(部分可以通过标准,最佳实践解决,部分不能)

①支持在多主环境中使用凭证(Webstandards):用于解决PWM在多个子域或域间移动是否填充的问题

②更好地支持多页登录(websites)

网站不应更改认证方式而应支持PWM在多页填充用户名口令

③支持自定义字段(PWMs, Websites)

PWM提供一种方式存储凭据的附加数据,网站提供一种方式帮助PWM识别

④避免晦涩的Javascript(Websites)

JS本来是用于提升安全性,但发现可能会影响PWM的可用性,甚至使网站出现故障

⑤支持HTTP Basic Authentication.(Password Managers)

⑥更好地支持TOTP(Password Managers)