NSPW'14 - Stobert - A Password Manager that Doesn't Remember Passwords

概述：(S)安全的口令难以记忆，用户口令数量太多，用户很难将口令与自己的帐户对应起来，口令管理器和cued图形口令是两种解决方案，但单独一种还不能解决口令的问题。(T)本文旨在将二者的关键思路结合提出一种解决方案。(A)提出了Versipass，PM不存储口令，而是图形口令的cue，可以帮助用户记忆口令，而且可以更好地与帐户关联，另外还允许用户使用相同的image达到安全重用口令的效果。(R)本文给出了实现的原型，分析了安全性，并通过用户调研和认知走查法对方案进行了评估。

优点：① 本文首次结合了cue图形口令和PM的特征提出了一个口令管理器

② 对于Versipass的评估过程较好，讨论很深入。

问题：① 本文最初提出的目标之一是可以帮助用户区分不同的帐户和口令，但文中没有给出具体的方案，实际上PM自身可以提供关联帐户和口令的功能，并非较解决的

② 对Image PassTiles的钓鱼攻击的描述中，攻击可能在什么时候获知用户名，为什么获知用户名将导致cue泄漏。cue应由PM保护的。本文应给出具体解释。

③ 本文方案很难自动化满足各种口令策略（目前仍处于研究中）

④ Versipass细节介绍不清楚，而是直接引用之前的研究，应解释技术细节，如cue如何存储，如何与图片和帐户对应起来

1. Graphical 口令，利用心理学中的picture superiority effect，用户更容易记忆图形（相比于文本）。有研究表明当口令空间相同时，图形口令比文本口令更容易记忆 (SOUPS'13)

▲ 图形口令的cue可以帮助用户更好地区分口令

▲ 但用户仍无法记忆大量的图形口令

2. 新的模型

1> Cue Model：Versipass不存储口令，而是存储口令的cue，帮助用户生成口令

PM将cue发送给用户，用户可以通过cue获取口令并登录网站

2> Category Model：一个口令可以用于一组帐户（允许用户对帐户做分类） 用户不可见

用户可以使用相同的口令在各个网站上进行不同的加盐哈希方法，实现安全的口令重用（重用是用户不愿意放弃的习惯）

▲ 提供explicit cues给用户，帮助用户区分不同帐户的口令

▲ 采用hashing PM的工作方式，引入cue支持随机口令，允许用户保护不同类的帐户，避免单点故障。

3. Versipass原型（使用Image PassTiles图形口令方案）

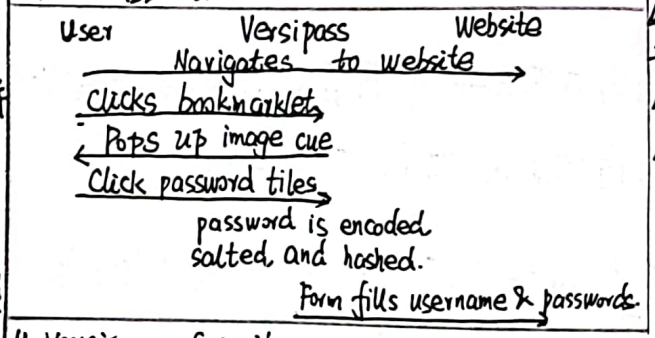
1> Image PassTiles：提供给用户一张由网格覆盖的图，用户口令由一组方格组成

▲ 口令由系统决定，用户无法决定选用哪所方格（已知有研究证明此类口令比同等安全的随机文本口令更容易记忆（背景图用于帮助用户记忆，且可以区分不同的口令）。

▲ 口令是随机生成的，与image cue无关，编码成文本串（每个块用字符串标记）

文本串以一种标准的顺序排序并用于比较，编码文本可以被哈希加盐并用于存储

2> 口令管理器



▲ 用户可以选择字符串与URL一起作为salt，并且salt可后续用于更改口令。

▲ 允许用户在生成时选择口令策略

▲ 可以由bookmarklet修改为browser extension，将解决bookmarklet需要从一个tab拷贝口令到另一个tab的问题

4. Versipass Security

1> Image PassTiles

① Guessing Attacks

在默认画配置下，在6x8的格子中以任意顺序点击5个，可以得口令的熵为：$\log_2\binom{48}{5}=21$ bit

可以通过画配置口令长度进一步增强抵抗猜测攻击的能力

② Capture Attacks

- 建立在隐私空间完成点击操作，避免通过肩窥或录屏的方式获知点击的图片
- 由于每次登录的图片和点击位置不同，重放攻击将比较困难。
- 钓鱼攻击者若可以获取username，则可能拿到cue，进而提供给用户登录口令。
- 可通过TLS抵抗中间人攻击。

2> Password Manager

- 可以对存储的数据部署离线备份，防止存储数据丢失
- 通过在运算口令时增加URL，并且Versipass会提示未知的URL，防止钓鱼攻击。
- 为了防止PM的server被破坏时用户无法登录，可以部署离线存储，但无法在多个设备登录。
- Versipass为登录网站提供了另一层认证方法，因为用户需要登录Versipass检索cue

5. 评估

1> 初步的用户调研（5修结，4个使用过PM），完成特定的4个任务

2> 认知走查法 ① 用户知道要做什么吗？② 用户知道怎么做吗？③ 用户知道他们做的正确的事吗？

3> 结果（没有参与者成功完成所有的任务）

① Mental Model Problems：对PM的理解/认知有误导致的问题。

▲ 许多用户对PM的功能和优点有误解。

▲ 一个较大的可用性障碍为已知网站帐户对应的口令必须修改为Versipass生成的口令。

▲ 当错误发生时应如何修正，对不理解PM工作原理的用户是一种挑战

②Security Issues: 几乎没有参与者认识到 Versipass 可以如何增加帐户安全性

③Incorrect Interface Elements: 用户界面中的部分元素存在误导性，影响 usability.

6 讨论

1> Mental Models of Versipass

许多用户在未正确理解 Versipass 的情况下使用 → 用户需要对口令和次击理解到什么程度才能安全、成功地使用 PM.

让用户理解 Versipass 提供的功能并且避免用户对某些功能产生误解.

2> Memory and Passwords

需要例如 SSO 和 PM 等工具帮助解决用户记忆负担与口令数日渐增多的问题

3> What is Password? (用户不清楚哪个口令为网站口令)

认知走查法调研中发现，用户希望控制自己的口令，而使用 PM 则要求用户可以相信 PM 每次生成相同的口令，并且正确存储了信息

▲ This is a complex issue: users do not want to have to remember their passwords, but they also don't want to trust someone else to remember their passwords.

▲ 需改进设计细节让用户理解 PM 在做什么，但不会陷入 PM 功能的细节中.