

概述: (S) 最简单的PM只提供了存储和检索的功能, 许多其它技术用于改进设计, 但也存在一定安全缺陷, 例如PM未及及时lock, 存储在其中的口令很容易被窃听。(T) 本文旨在不影响可用性的情况下提供安全保障, (A) 本文方案无需master password, 需2个设备, 1个是在PC上安装的浏览器插件, 1个是智能手机上安装的app, 插件中含有k用于加密口令, 密文存储在手机中。当两个设备之一丢失时, 用户无法恢复出用户的帐户口令。(R) 本文给出了安全性分析, 通过用户研究进行了可用性分析, 并通过SP'12的框架对比了Firefox PM和 Password-only, 结果表明尽管存在一定问题, Tapas仍具有较高的安全性和可用性。

- 优点: ①文章结构完整, 包含设计实现, 安全性分析, 可用性分析和对比  
②给出基于 dual-possession 的认证方案, 当设备之一丢失时敌手无法恢复口令  
③较给出了本方案的劣势, 分析较好。④不需要 master password。  
问题: ①当手机丢失时(或没电), 用户无法登录 ②本方案依赖于可信的信道, 要求Manager和Wallet均有公私钥, 该要求应尝试放弱 ③当提供 out-of-band 服务时该方案比传统PM慢 ④本文只提供了单PC与单Phone的配对, 可扩展 ⑤Manager与Wallet之间的通信依赖于Rendezvous Server

### Tapas-based authentication using a smartphone

本文旨在提供易部署, 安全且可用的PM方案, 避免更改服务器端的配置

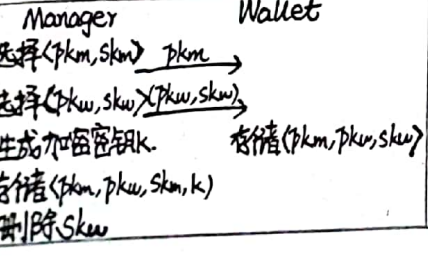
- #### 1. Dual-possession Authentication:
- 使用多个匹配的设备进行口令管理可以提供一定程度的 theft resistance
- ▲包括两类应用, Manager和Wallet, 分别处于不同的设备上, 参与3个协议 Pair, Store和 Retrieve, 目标: By stealing the data of either the Manager or the Wallet, an adversary cannot determine the stored password for any given account with any greater success than attacking the account directly)
- 使用Manager中的key加密口令, 将密文存储在Wallet中。
- ▲为使Store和Retrieve可以在不安全的网络中进行, Pair在 authenticated and secret out-of-band (AS-OOB) channel, 一旦pair, 设备会建立双向认证的安全通道。

### 2. Tapas设计架构

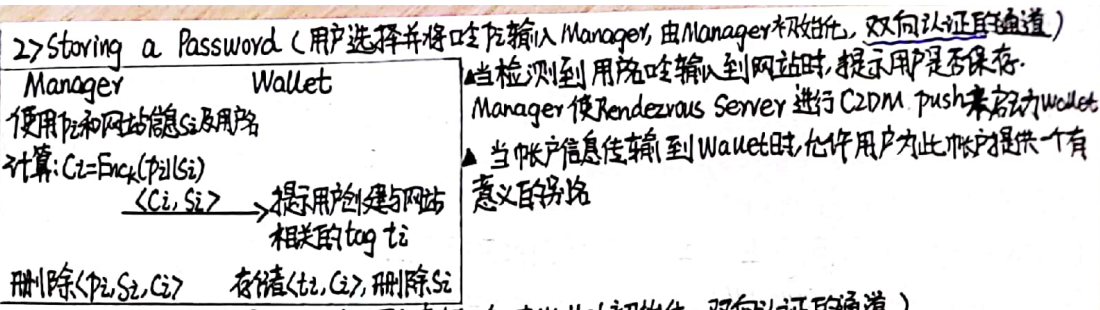
▲为使处于不同网络的两个设备通信, Tapas使用Rendezvous Server促进通信(其不可信)

另外, Rendezvous Server用于连接与Google Cloud to Device Messaging (C2DM) service 的服务, Google要求所有使用C2DM的应用需预注册以获取API认证token, Manager通过C2DM发送push message给设备, 进而自动启动Wallet应用

#### 1> Pairing Manager and Wallet (用户安装应用, 协议由Manager初始化, 双向通信渠道)

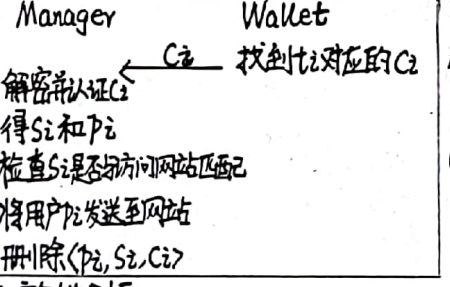


Manager计算认证密钥对并生成对应的TLS证书, 将网络信息, 证书指纹, Wallet的证书和相应的secret key嵌入到QR code中, 产生单向的AS-OOB通道。  
Wallet通过扫码进行配对并获取相应的证书信息



▲当检测到用网站输入到网站时, 提示用户是否保存。  
Manager使Rendezvous Server进行C2DM push来通知Wallet。  
▲当帐户信息传输到Wallet时, 允许用户为此帐户提供一个有意义的标签

#### 3> Retrieving a Password (用户查找口令, 由Wallet初始化, 双向认证的通道)



Tapas需要用户操作两台设备才可以获取口令

- #### 4> Tapas的局限性
- ①依赖于网络连接且Rendezvous Server必须可以工作
  - ②配对的设备必须同时可用才能认证
  - ③目前的配对只允许一台电脑和一台手机

#### 3. 安全性分析

▲敌手能力除了AS-OOB之外, 敌手可以拦截, 记录和修改Manager和Wallet之间的通信

②允许敌手控制Manager或Wallet (theft), 但不考虑同时被窃的情况。

- #### 1> Resistance to Theft
- ①Smartphone可能丢失, 但其中存储的口令是通过对称加密算法加密的, 密钥只存储在Manager中, 另外, 其中所有的其它信息也全部加密
  - ②敌手wallet的认证key使敌手可以伪装成Wallet, 但由于所有口令的密文通过Manager的解密密钥k认证, 因此敌手无法从Manager获取 decryption oracle
  - ③Manager被敌手获取, 敌手可以拿到k和  $sk_m$ , 需要提供PFS的安全信道才可以保证无法从丢失的  $sk_m$  中获取过去的  $sk$ 。

#### 2> Resistance to Malware (在电脑中的malware)

若设备中安装了malware, 敌手总是可以在用户提交时拿到口令的明文。在传统的PM中, 敌手可以立即拿到所有的网站口令; 但在Tapas中, 敌手只能在用户使用口令时拿到该网站口令, 其余口令安全。

#### 4. 可用性评估

1> 采用 in-person 而非机械化的研究的两点原因: ①Tapas需要Android且要安装特定的app, 本文提供的是安装好应用的手机; ②可以直接观察到用户使用PM的行为

- #### 2> 任务:
- ①配置 Password Manager: 对于使用 master password 的应用, 启动 master password 并创建 master password; 对于 Tapas, 进行扫码
  - ②创建并将帐户信息存储到PM: 访问博客A和B, 注册帐户信息并将信息存储到PM
  - ③给定用户一个博客C的帐户, 让用户登录, 存储帐户信息并登出。
  - ④登录blog, 首先进行 distraction task (减弱用户的记忆), 依次登录blog C, A, B (关闭浏览器并重新打开, 因为一些浏览器只有在打开时才会提示输入 master password)



## 5. 用户研究结果

1> Statistical tests: 采用 Kruskal-Wallis non-parametric one-way analysis of variance test;  $p$ -value 若为 0.05 表明参与者的响应与提出的问题无关, 为了确定哪种情景下独立, 独立的对进一步通过 non-parametric Mann-Whitney test 来进一步分析

2> Post-test Questionnaire.

① PM setup 阶段的可用性 ② 口令存储阶段的可用性 ③ 用户是否喜爱

④ General participant observations: 部分用户担心一旦 PM 不可用了, 将无法访问这些帐户 (尽管可以采用网站的恢复口令功能), 但应解决 loss-of-access 情景

→ 可提供 Tapas 的加密备份功能

3> 改进 Tapas 之后的用户研究: 表明改进后的 Tapas 可以让用户更好地理解 Tapas 的用法

6. 比较总结 (采用 SP12 的 Usability-Deployability-Security (UDS) 框架)

① Tapas 在 PM 不可用时不能为用户生成口令

② Tapas 自身不能改善口令的属性

③ Tapas 提供了钓鱼攻击保护

④ 相比于 MP (Master Password) Firefon, Tapas 不需要 MP 但需要智能手机; 可以在 device 丢失时抵抗离线攻击; 在 malware 安装在 PC 上时, 泄漏口令的速率更慢。

⑤ Tapas 可以结合其它方案一起增强口令存储的安全性, 例如利用 master password 保护 wallet 中密文的备份用于恢复。