ACSAC'12 - McCarney - Tapas: Design, Implementation, and Usability Evaluation of a Password Manager

补脏述: (S)最简单的PM只提供存储和检索口令的功能，许多其它技术用于改进设计，但也存在一定的安全缺陷，例如PM未及时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护。(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SPI2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本文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，该要求在尝试放弱 ③当提供autofill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，可进一步扩展 ⑤Manager与Wallet之间的通信需依赖于Rendezvous Server

▲Tap-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

▲为了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，双方通信渠道)

Manager	Wallet
选择$\langle pk_m, sk_m\rangle$	
	pk_m →
选择$\langle pk_w, sk_w\rangle$	
	← $\langle pk_w, sk_w\rangle$
生成加密密钥k.	
	存储$\langle pk_m, pk_w, sk_w\rangle$
存储$\langle pk_m, pk_w, sk_m, k\rangle$	
删除sk_w	

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

2> Storing a Password (用户选择并将口令输入Manager，由Manager初始化，双向认证的通道)

Manager	Wallet
使用p_i和网站信息S_i及用户名	
计算: $C_i = Enc_k(p_i \| S_i)$	
	$\langle C_i, S_i\rangle$ → 提示用户创建与网站相关的tag t_i
删除$\langle p_i, S_i, C_i\rangle$	存储$\langle t_i, C_i\rangle$, 删除S_i

▲当检测到用户口令输入到网站时，提示用户是否保存。Manager使Rendezvous Server进行C2DM push来启动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)

Manager	Wallet
	找到t_i对应的C_i
	C_i →
解密并认证C_i	
得S_i和p_i	
检查S_i是否与访问网站匹配	
将用户p_i发送到网站	
删除$\langle p_i, S_i, C_i\rangle$	

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①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)，但不考虑同时丢失的情况.

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丢失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，其余口令仍安全.

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，注册用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的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SP'12的Usability-Deployability-Security(UDS)框架)

①Tapas在PM不可用时不能为用户生成口令

②Tapas 自身不能改善口令的属性

③Tapas 提供了钓鱼攻击保护.

④相比于 MP(Master Password) Firefox，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，泄漏口令的速率更缓.

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