SecureComm'17 - Yue Li - BluePass: A Secure Hand-Free Password Manager

相关述：(S)PM的同步机制可能导致数据泄漏，master password可能成为单点故障。(T)本文旨在提出一种能在PM可用性和2FA安全性的方案BluePass。(A)将password vault与decryption key存储在不同的位置(吃存储在移动设备中，解密key在browser中发挥作用)，移动设备与browser通过蓝牙通信(R)，实现了系统原型，评估了Security，overhead和usability，并进行了相应的用户调研。

优点：①采用蓝牙实现了hand-free的PM，类似于zero-effort的2FA方案

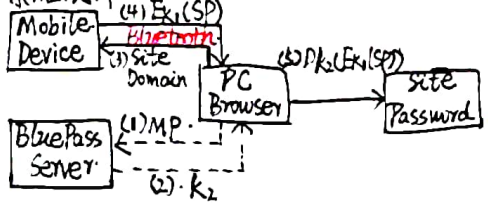
②对原型细节的介绍较详细且清晰。

问题：①4.2的分析有误，当Vault泄漏时，攻击者可通暴力猜测MP获取k_2，进而解密吃

②用户调研中与其它PM的对比，应给出使用PM的信息；且建议让用户同时使用两种做对比才有比较的意义

③没有介绍生成吃的细节内容，以及其中可能与用户有交互的部分

▲系统设计



- BluePass server：用于用户注册和分发key(k_2)
- Mobile Device：安装了app，存储由k_1加密的吃值，通过蓝牙与PC交互。
- Client-side：安装客户端app，检测并填充登录表单，与移动app通信，解密拿到的网站吃
- MP：用户用于向BluePass Server认证并检索k_2
- k_1可在可信设备长期存储，并可短暂存储在不信设备

1) 两条件

①网站吃SP只能通过设备中的$E_{k_1}(SP)$和k_2检索解密得到

②Mobile Device和PC Browser只能通过蓝牙进行交互，即需要较近的距离

2) Threat Model (攻击者希望获取所有的网站吃，无法同时访问到加密吃和解密密钥)

两类攻击：①co-located attacks：在蓝牙通信范围内，攻击者可窃取加密的吃值：(更困难)

②remote attacks：不能窃听蓝牙通信，但BluePass Server或MP可能被攻破。

3) 3个阶段

①Registration　Phone ⇄ BluePass Server　(1) (MAC, MP, PN)　k_1

在手机上下载BluePass应用，在Server中创建主帐户，在登录到app后，可绑定device，可将device的蓝牙的MAC地址上传至server。Server为新注册的设备生成k_1和k_2，并将k_1存储在设备中，k_2仍存储在server端。注册只需一次，设备端初始化password vaults.

■ k_1和k_2为RSA的公私钥对，但均需保密。

②Configuration：Browser ⇄ BluePass Server　(1) (MP)　(2) (MAC, k_2)

用户在客户端安装app，并登录到BluePass Server获取k_2和设备的MAC，

用户可选择设备是否可信，决定k_2和MAC是否长期存储。

Browser可以通过RFCOMM insecure mode与设备通信

③Authentication　Website Server ⇄ Browser ⇄ Phone　(1) Site Domain　(2) Site Domain/$E_{k_1}(SP)$　(MAC)　(3) $E_{k_1}(SP)$　(4) SP

只在HTTPS的网站中进行autofill(其余网站需要用户同意)

若存在多个帐户，用户可以选择登录的帐户

4) 帐户的管理(add, edit, delete)

①add：当无法检索到对应的帐户时，可询问用户是否存储。若存储则由browser使用k_2加密发送到device，使用k_1解密后再加密。$E_{k_1}(D_{k_1}(C))$，其中$C=E_{k_2}(SP)$

②edit：与add类似，当吃值改变时执行

③delete：可以在管理页面执行，但执行前需输入主帐户的MP

5) Recovery (备份与恢复)　Phone ⇄ External storage　(1) Export Vaults　(2) Import Vaults　可通硬件或云端设备

▲安全分析.

1) 7个 Security (双因素检索吃)

①若Master Password被攻击获取(若设备被篡改结果一样，因为k_2可被攻击获取)

只要攻击无法获取password vault，就可以保证BluePass安全；且后续可以更改MP.

②Mobile Device被攻击成功访问：可获取吃值和加密key k_1，但无法获取k_2，可保证安全.

■由于password vault和k_2不在一个位置存储，故很难同时被破坏.

2) Data Breach and Brute-Force Attacks

若BluePass Server被破坏，攻击者可获取k_2，但未拿到吃vaults，故无法攻破BluePass

若吃vault丢失，对k_1的暴力破解不可行.

3) Broken HTTPS or Bluetooth.

若HTTPS连接被破坏，攻击者可获取k_1, k_2，考虑到k_1, k_2只在安装BluePass或首次登录时发生，时间约束较大.

只窃听Bluetooth的数据只能获取加密数据，故不可行.

▲实现

客户端应用包括2个模块：

①Chrome application：用于蓝牙通信 ②Chrome extension：用于吃autofill.

2) 本文采用secure RFCOMM连接模式，Phone和PC需建立连接

▲评估.

1) 使用UDS框架进行评估：BluePass不要求手机有信号或传输数据；可生成高熵吃

BluePass可保证简单清晰的mental model，且增强了usability.

2) Autofill延迟(检测到吃表单到自动填充的时间，T_{bp}；表面加载时间T_{load})

用户感知延迟$T_{bp}-T_{load}$，平均$T_{bp}=81.6ms$，$T_{bp}-T_{load}=181.1ms$，用户很难感知

3) Power Consumption.(消耗电源水平) 观察登录频率与消耗电源的关系.

从的实验发现除非频繁登录(每2s一次)，否则无明显影响

▲用户调研(31名志愿者完成8个任务)

87%(27/31)认为BluePass比之前用过的PM可用性更高；超过70%(22/31)愿意选更安全的吃且不重用吃

但只有半数可使用BluePass生成的吃，94%愿意使用BluePass管理吃

▲1) k_1, k_2在互相推导；②不应过小且RSA不使用CRT加速。2) 用户必须使用有蓝牙功能的设备且特别和才可登录