ISE Science Journal'13 - Rui Zhao - Vulnerability and Risk Analysis of Two Commerical Browser and Cloud Based Password Manager

优点：①研究了两个基于云的PM的安全性，从底层密码和协议分析较好
②对安全问题进行分评级，并且给出了详细的建议

问题：①部分问题只针对于本地存储，可进一步研究云存储PM的安全性
②记忆主口令是LastPass的配置项，可进一步研究不同PM配置的安全性和可用性影响
③本文对云端存储安全性由于无法获取云端信息，而不够具体深入。

▲研究背景
1）PM可以缓解口令相关的问题，一个显著的优点是不需要输入（记忆）如此多的口令
2）本文研究两个PM的安全性，browser-based & cloud-based BCPM
①browser-based：提供与内置浏览器的PM一样的浏览器扩展
②cloud-based：网站口令存储在云中，允许用户在任何时间和地点访问

▲研究问题 ⇒ LastPass和RoboForm是否真的安全且保护了用户的口令
1）定义安全模型 2）找出BCPM的底层设计原理和机制 3）找出BCPM存在的漏洞
4）分析安全风险的级别 5）提供建议以改善设计 （在Chrome和Firefox浏览器）

▲预备知识 - LastPass和RoboForm的区别与联系
1）LastPass将用户信息存储在本地和云，而RoboForm则是在线时存储在云，离线时存在本地
两个BCPM均需使用用户名和口令认证才可访问存储的数据
2）两个BCPM使用主口令的方式非常不同：例如主口令是否与BCPM的用户名口令相关，主口令是否可以被记忆？是否存储在本地？→对安全性带来不同的影响

▲威胁模型
1）types of credentials：考虑了3种凭证
①websites credentials：用户的登录信息，也是攻击者的最终目标
②BCPM credential：<BCPM username, BCPM password>，允许用户向云存储服务器认证，LastPass可以使用该凭证登录到官方网站
③master password：破解主口令会带来安全风险
2）types of attackers
→outsider attackers：未经授权或非法的实体，从BCPM的安全边界之外发动攻击
①server-side stealing capability：入侵到云存储服务器窃取数据
②client-side stealing capability：攻击用户机器获取本地存储的数据
③client-side computation capability：在用户机器上临时运行程序进行计算
→insider attackers：可以授权访问BCPM的资源，但未以允许的方式使用
①server-side stealing capability：盗窃服务器存储的数据（保证BCPM未知数据）
②server-side monitoring capability：监控BCPM与云的通信（BCPM未知数据）
3）types of attacks under consideration
①brute force attacks：内部/外部攻击者用于破解主口令（人的活动视为上界）
②local decryption attacks：从用户机器破解网站凭证，可由外部人通过drive-by downloads并运行恶意软件完成
③request monitoring attacks：拦截BCPM发向云的请求获取网站凭证。由于通信为HTTPS且恶意软件不会一直存在于用户机器，主要考虑内部人。
4）本文不考虑web攻击（如XSS），浏览器和扩展的特权升级漏洞，以及针对云的特定攻击（如侧信道攻击）。

▲安全分析方法（探索BCPM的密码机制）
1）两个BPM使用JS开发，使用了不同混淆技术。本文使用Eclipse和jsbeautifier去混淆；使用Mozilla的JS调试器和Chrome的开发工具帮助理解动态执行；使用subzilla的HTTP Analyzer监视和分析流量；使用实验验证存储、用户认证和密码生成的功能
2）使用brute force attack评估，两台机器：①$10^6$/s执行1个密码操作 ②$10^{12}$/s执行1个密码操作（例如：DES, AES, SHA-1, SHA-2）

▲LastPass安全设计和漏洞分析
1）LastPass使用JS和（可选）二进制组件实现密码操作，凭证存储在本地和云
用户需要记忆主口令和BCPM用户名
q_local_key = PBKDF2-LP(master password, BCPM username (salt), 500, 32) 加密用户的网站凭证
q_local_hash = PBKDF2-LP(q_local_key, master password (salt), 1, 32) 作为BCPM口令
2）外部人的local decryption attack → 允许记忆主口令 → HIGH可能性，MEDIUM影响
存储之前有三种情况：①PC有二进制组件和TPM，通过TPM支持的Windows API加密
②PC有二进制组件无TPM，则使用无TPM支持的加密 ③无二进制组件，不可加密
具有client-side stealing能力和client-side computation能力可以攻击前两种，第三种主口令以明文形式存在 → 耗时均较短
2）外部人的brute force attack. → 本地用户认证机制的不安全设计和PBKDF2的不安全应用（MEDIUM, MEDIUM）
在无网络连接时需在本地认证用户来使其可以访问凭证，LastPass使用右填码的字符串"lost rocks"使用AES加密，与凭证存储在一起，key为q_local_key，用于本地认证
→外部人可利用client-side stealing能力获取BCPM用户名和上述字符串密文
通过猜测主口令得q_local_key，解密密文并验证，故暴力破解。
8字符的主口令使用第二个主机（10^{12}）可以在15.2小时内破解。
4）内部人的brute fore attack → 主口令与认证标识的关联 → MEDIUM, HIGH
具有server-side monitoring能力的人。

①拦截<BCPM username, G-local-hash>，可抵御与外部A的攻击

②在用户向LastPass认证时，需发送双哈希SHA-256(SHA-256(BCPM Username + Master Password + Master Password)，可抵御更高效的暴力破解.

▲RoboForm 安全设计和漏洞分析

1>安全机制 → 分为两种模式，在线和离线

在离线状态下，使用PBKDF2-RF生成密钥(有两个SHA-1在PBKDF的一次迭代中出现)

key = PBKDF2-RF(master password, random number, 1000, 32)

2>外部A的local decoding attack → 在无主口令时，本地存储是无保护的 → HIGH MEDIUM

在无主口令时，存储在.rfp中的口令值只做了编码，在client-side stealing能力的A下可以很容易被获取

3>外部A的brute force attack → 在使用主口令时本地存储无保护 → MEDIUM MEDIUM

①.rfp文件中存储了完整性校验码使用生成key计算，A可猜测主口令匹配校验码

②在离线状态下，RoboForm创建Smpenc.rfo，存储使用1-DES加密的字符串"MASTER PASSWORD"，key通过用户口令生成，使用该文件认证离线用户

使得具有client-side stealing能力的A很容易进行暴力破解 → HIGH HIGH

4>内部A的server-side request monitoring attacks → RoboForm收到的数据无保护

在线模式下，信息需发送到服务器，但均以明文形式，具有server-side monitoring能力的A可等待HTTPS解密完成窃取

▲风险评估

使用OWASP Risk Rating Methodology. Risk = Likelihood X Impact.

▲建议

1>在发送到云之前，用户数据应使用强的机密性和认证机制保护.

2>外部A的client stealing能力和computation能力应被BCPM设计者认真考虑，例如不允许记住主口令

3>BCPM必须提供主口令机制，且应保证用户使用了强度足够的主口令

4>应使用较大迭代数来应用PBKDF，使得每次主口令尝试需花费一定时间，保证对强主口令的暴力破解在计算上不可行

5>用户的主口令应用于对用户认证，不应与任何存储在本地或发送至云的任何认证标识关联

6>应保证数据真实性，且不应削弱机密性(可通过建议4>实现)