ICDCS'17-Shirvanian-SPHINX: A Password Store that Perfectly Hides from Itself

优点：① 基于DE-PAKE提出了口令管理器SPHINX，使用smartphone作PM，

② 攻击U,D,S任意一方都不会导致pwd泄漏；PM不存储pwd,rwd，D compromise时不泄露口令

③ 对安全性和可用性进行了分析，结果表明SPHINX在安全性及可用性方面均较好。

问题：① 文中的两个假设，smartphone可用和client compromise在实际可能难以满足。

② 若用户使用smartphone登录，则k与pwd在同一设备，可能被攻击同时获取计算rwd。

③ 生成的rwd如何满足网站的口令策略，这一点应具体讨论。▲

④ 用户登录时需输入前缀或按特定键，且用户端需做改动，非用户友好。

Password manager/store/vault 口令管理器，PM

允许用户基于低熵的master password(pwd)与"device"交互，存储和检索用于不同服务的(通常)高熵的account password(rwd) → 从用户端(客户端)缓解server compromise带来的问题（口令重用使server compromise造成的危害更大）

→ PM可以提供的：当存储的rwd为足够高熵时，在server compromise时可抵抗离线字典攻击。 当前的PM存在一定的安全隐患：

▲ 当PM compromise或为恶意时，① 存储在PM中的rwd通常为pwd加密过的。② 用户在使用时可能需要向PM中输入pwd；可能造成pwd被攻击获取。部分研究提出不在PM存储rwd

SPHINX：基于DE-PAKE实现口令管理器，device作为PM，在PM compromise或为恶意时仍可保证安全，核心技术为OPRF，其中device中不存储口令，在运算时也无法获取口令的相关信息

→ 可提供的安全特性

① 由于rwd是高熵且相互独立的，可抵抗在线猜测攻击。

② 由于rwd经过OPRF及单向哈希后存储在Server中，故server compromise时可抵抗离线字典攻击

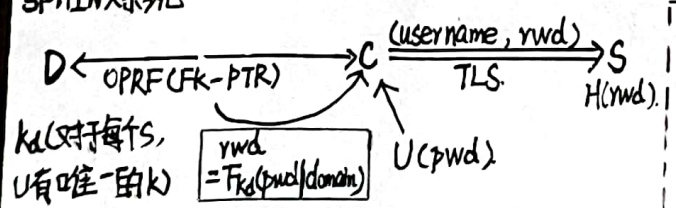
③ 由于存储在device中的信息与pwd,rwd独立，故device compromise可抵抗离线字典攻击

④ 由于计算rwd时使用了domain，故可抵抗钓鱼攻击。

⑤ 由于OPRF运算，D-C之间使用不安全信道可抵抗窃听和MITM攻击。

注：SPHINX提供了一个基于smartphone的方案，需假设smartphone是可用的，且不考虑client compromise

SPHINX系统



Setup：循环群(G, q, g).

哈希函数：$H: \{0,1\}^* \to \{0,1\}^{\lambda}$, $H': \{0,1\}^* \to G$

OPRF：$k \leftarrow Z_q$, $F_k(m) = H(m, H'(m)^k)$.

Parties: U, C, D, S

Initialization：

① D选取并存储OPRF key, $k \leftarrow Z_q$.

② U选取 $pwd \leftarrow Dict$

③ C D构建 $rwd = F_k(pwd|domain)$

④ S存储rwd的单向哈希值。

Login：

1> C $\rho \leftarrow Z_q$. $\alpha = H'(pwd|domain)^{\rho}$ → D；$\alpha \in G$?；$\beta = \alpha^k$ ←

$rwd = H(pwd|domain, \beta^{\rho^{-1}})$

2> C通过TLS向S提交rwd进行认证。

SPHINX系统实例化（C: SPHINX browser extension. D: SPHINX Android application）

C: ① Reading the password：通过特定前缀或按键(或设置)选择使用SPHINX服务

② Hashing the password into the EC：在椭圆曲线上构建群，将pwd映射到群上

③ Fk-PTR OPRF protocol：C得到H'哈希后的值，添加指数ρ，发送给D；C收到响应去掉ρ得rwd

④ Entering the randomized password：在登录界面输入rwd到口令字段。

D: ① Starting the Fk-PTR protocol：收到C的以后，计算$\beta = \alpha^k$.

② a): Explicit Consent Mode：在D中给用户提示，要求登录过程有用户参与

b): zero-Interaction Mode：即D与用户无交互，此时获得pwd的攻击者可能成功登入

③ Completing the Fk-PTR OPRF Protocol：D将β发送给C.

SPHINX提供的usability(可用性)：① 用户只需记忆低熵的pwd. ② 可通过更新D中的k更新rwd ③ 可以使用多种设备替代smartphone.

→ Usability研究：通过a formal lab-based study研究security, usability, adoption potential；通过筛选，对比Explicit Consent Mode SPHINX及Password-only方案

→ 从以下6个方面做实验研究：

① Transparency：与password-only的方案对比给用户的体验。

② Security and Trust：用户是否会信任系统？

③ Necessity：用户在实际中是否愿意采用该系统？

④ Portability：用户是否可以从多个终端登入系统(可移植性)。

⑤ Efficiency：该系统会引入什么延迟？

⑥ Comfort and Learnability：系统是否方便易学？

→ 分为三个阶段：

① Pre-Study Phase：强制参与者的个人信息及计算机技术背景。

② Main-Study Phase：统计每个任务的难易程度和满意程度。

a> Primary Computer Login.（参与者使用提供的laptop登录）。

P_1: Unprotected login ⇔ password-only方案。

P_2: Activation：用户更新口令得到master password.

P3: Protected login: C得到rwd，点击D的按钮，自动填充pw完成登录.
P4: Password Update: 更新pw(rwd).
P5: Protected Re-login: 更新pw后重新登录.

b). Remote Computer Login(未安装SPHINX浏览器扩展).
R1: Direct Login with Randomized Password: 未安装扩展时直接用rwd直接登录
R2: Plugin Installation: 参与者收到一封邮件用于安装该扩展(浏览器插件).
R3: Protected Re-login: 参与者正常使用SPHINX远程登录.

③ Post-Study Phase.
用户填写System Usability Scale(SUS) questionnaire，作者从Transparency、Security and Trust、Necessity、Portability几方面对比SPHINX及Password-only方案，并提出一些开放问题给参与者来改进SPHINX.

讨论、限制和未来工作.
① Online SPHINX Service: 设计Online版本的SPHINX
② key Back-Up and Device Upgrade: 应提供备份功能以便设备更换时k仍可用
③ Alternative Devices: 讨论使用便携式、IoT类型的设备，用于实现SPHINX
④ Client Compromise: PM未考虑client compromise，可使用2FA与PM结合.

将SPHINX与其它PM对比(基于the quest to replace passwords)
→ 研究对象:
PM0 password-only方案.
PM1 SPHINX
PM2 PwdHash
PM3 Password
PM4 Passpet
(PM1-PM4: Hash Based PM.)
PM5 Firefox PM
PM6 Commercial PM
PM7 Tapas (Smartphone-based)
(PM5-PM7: Traditional PM.)

→ 评估方法.
▲ Security
S1: Unique-Password-Enforcer: 对于每个网站生成唯一的rwd值.
S2: Resilient-to-Phising: 抵抗钓鱼攻击.
S3: Offline-Dict-Attack-Resistant-Server-Compromise: 在server compromise时抵抗离线字典攻击.
S4: Storeless: PM中无需存储pwd和rwd
S5: Offline-Dict-Resistant-Device-Compromise
S6: Resilient-Upon-Theft
(S5、S6: 获取设备秘密的攻击者无法获取pwd.)
S7: Resistance-to-MITM over device-client channel. 在D-C之间抵抗MITM攻击
S8: Resilient-to-Physical-Observation: 当pw被拿到时，仍可以保证安全(W-compromise)
▲ Usability
U1: Memorywise-Effortless 用户只需记忆pw
U2: No-Initial-Password-Update: 无从pwd转换到rwd并填充到pw空段的进程
U3: Scalable-for-Users. 当帐户增多时，无需用户增加操作即可完成
U4: Physically-Effortless 用户只需输入pw而无其它操作
▲ Deployability.
D1: Client-Compatible: 无需客户端更改
D2: Nothing-to-Carry: 无需携带额外的硬件设备.