Fukunitsu - A proposal of a password manager satisfying security and usability by using the secret sharing and a personal server

亮点：①使用个人服务器与secret sharing解决了Tapas遗留的问题

②使用UDS框架进行了评估.

问题：①缺少用户调研，未知该方案的实际可用性如何

②作者认为个人服务器将像智能手机一样普及，这一点假设不实际

③本文未涉及性能评估，相比于传统方案引入了较多的公钥操作

▲研究背景

1) PM可以帮助用户解决如何认证相关的问题：口令重用以及遭受攻击的咬.

两种方式：使用主口令或安全令牌

①主口令：用户倾向于选择弱口令，即使是强口令也存在单点故障的问题.

②安全令牌：用户需额外拥有安全令牌，丢失令牌丢失.但用户为了可用性，倾向于将令牌保存在PC

Tapas采用智能手机实现口令管理器，且避免使用安全令牌，达到了使用安全令牌的安全性

2) Tapas存在的问题

①在无配对的手机的情况下，Tapas不可用

②若配对的手机丢失，其中的口令值无法被恢复(包括其中的登录信息)

~~3)~~ ▲研究问题.

1)本文希望扩展和Tapas方案解决它存在的问题，但尽量不减少Tapas的优势.

2)采用的方案：引入用户私人服务器用于实现PM，并且利用(2,3)秘密共享的方式，一方面避免单点故障，另一方面可以在PC或手机丢失时恢复存储的登录信息.

⇒进一步使用UDS框架进行评估.

▲本文方案(个人服务器、用户的PC和用户的智能手机)

→个人服务器是一个有静态IP地址或FQDN的主机，可以执行web程序.

1) Init阶段.

①用户分别安装浏览器插件、智能手机应用、服务器应用

②浏览器插件生成TLS证书 $(pk_{pc}, sk_{pc}, X.509_{pc})$, $(pk_{smp}, sk_{smp}, X.509_{smp})$, $(pk_{svr}, sk_{svr}, X.509_{svr})$

用户需设置服务器登录口令 P_{SVR} 并记忆

③浏览器插件生成BK码，用手机扫码并存储信息，包括其它实体公钥、手机私钥和服务器标识符.同样，通过TLS通道将信息发送给服务器；浏览器插件同理，删除另两个实体的私钥

2) Registering阶段.

①浏览器插件提示用户输入标签 tsite，标识登录信息 site=(URLsite, IDsite, PASSsite)，并且计算URLsite的哈希值 hsite.

②浏览器插件使用(2,3)秘密共享，使得三方的实体共享 site, $S^{(PC)}_{site}$, DE{PC,smp,svr}，对于每个设备，$S^{(DE)}_{site}$ 使用D的公钥加密得到 $C^{(DE)}_{site}$

③浏览器插件将加密共享数据(ESD) Zsite=(hsite, tsite, $C^{(PC)}_{site}$, $C^{(SMP)}_{site}$, $C^{(SVR)}_{site}$)发送到手机和服务器.设备D解密 $C^{(D)}_{site}$，并且存储 $S^{(D)}_{site}$=(hsite, tsite, $S^{(D)}_{site}$).浏览器插件和手机应用删除Zsite.在三个设备均存储 $S^{(D)}_{site}$ 后，服务器才删除Zsite.

3) Recovering 阶段.

①浏览器插件提示用户选择辅助设备.

②smp：提示用户选择标签 tsite，并且把份额 $S^{(SMP)}_{site}$ 发送到PC

svr：提示用户输入服务器登录口令 P，计算URL哈希值h，将(P,h)发送到服务器

若口令匹配，找到hsite=h的记录的份额 $S^{(SVR)}_{site}$

若 $C^{(SVR)}_{site}$ 应在服务器中，则应把PC信息发送并删除

③浏览器插件可以通过收到的份额还原site，若URLsite匹配，则IDsite和PASSsite用于登录.

4) Rescuing 阶段

①如同Init中建立TLS通道.

②浏览器插件发送提示运行此过程来恢复设备：

smp：点击确认按钮，应用发送 $(h_{site}, t_{site}, S^{(SMP)}_{site})$ 到PC

svr：提示用户输入服务器登录口令 P 发送 (P, Rsc) 到服务器(Rsc为调用token)，若P匹配，则服务器应用将所有的(hsite, tsite, $S^{(SVR)}_{site}$)发送到PC

③使用收集的份额恢复site，并使每个设备更新份额.

▲Theft-Resistance.

1) PC或手机失窃.(攻击者可获取1个份额，以PC为例)

①在通信中窃听：受到TLS保护，不可行

②伪装成用户执行Recovering或Rescuing，若是手机，被偷取后运行配对的设备；若是服务器，攻击者需在线猜测服务器登录口令，可被限制.

2) 服务器被攻破.

由于另两个份额在TLS传输且加密，故难以破解.