Integration'19 - Qingli Cuio - PUFPass: A password management mechanism based on software/hardware

概述：(S) PM可以减轻用户的记忆负担且可以为用户生成安全的网站口令，但很多设计存在codesign在单点故障的问题，即主口令丢失时，敌手可能具有能力生成所有的网站口令。(T) 本文希望从软硬件结合设计的层面解决单点故障的问题。(A) 引入硬件原语PUF，提出PUFPass，利用random physical disorder增强网站口令，给出了详细的设计与实例实现，并分别从4个方面分析了安全性和可用性，并使用UDS框架将PUFPass与其它口令管理方案做比较。(R) 作者分析认为PUFPass在保证可用性的前提下，提升了安全性。

优点：① 从硬件的角度给了提升口令管理安全性的方法，较好(采用了PUF)
② 对安全性的分析有启发，也有具体的实验，且使用客观的指标与其它方案做了评估，较好。

问题：① 本方案需要硬件的支持，且文中提到为满足口令策略，需要App输入ng, l和d，即需要App进行修改，不是很容易实现普及化
② 5.3的Transportability小节，PUFPass不满足，因为需硬件支持比安装软件要困难
③ 一些新的攻击，未考虑，例如SPHINX通过OPRF技术可保证网站口令不会以明文形式出现在设备中。

1、Physical Unclonable Function (PUF) → 一种硬件安全原语 (CRP)

1) 一种物理结构，可以把 input challenge → output response (Challenge-Response Pairs)
其中challenge的bit数目为bitlength.

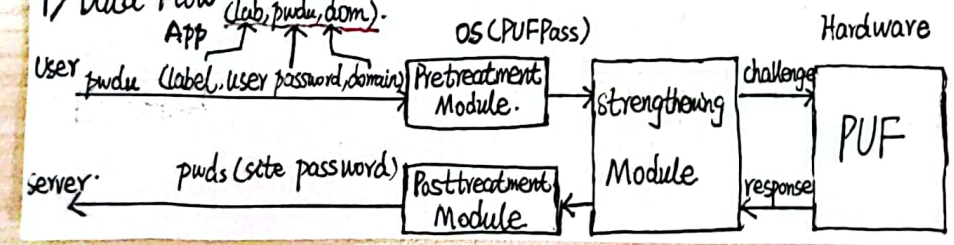
① PUF的CRP由生产IC时的random physical disorder决定，即使设计相同，不同PUF的CRP不同
- hard to be predicted before manufacturing
- hard to be controlled during manufacturing
- hard to be cloned after manufacturing.

② 两个固有的属性.
- Uniformity: 即使是相同设计和相同challenge，不同的PUF产生的response也不同
- Uniqueness: 产生response的0,1 bit的比例相近.

2) 根据CRP的数目，PUF可以分为两类：
① weak PUF: CRP数目较少，若产生更多的response bit，需要更多硬件资源(如SRAM PUF)
② strong PUF: CRP数目与bitlength可呈指数关系，数目较多(如 Arbiter PUF)
▲ 通常来说，由于噪声和其它物理不确定性，PUF的response难以保证完全稳定，但有关于Error Correction Code (ECC)等技术的研究表明ECC可用于确保PUF的稳定性.

2、PUFPass机制.

1) Data Flow.



① 用户需输入用户名，PUFPass生成随机lab，存储在设备本地
② Pretreatment Phrase: 构造PUF challenge.
PUF的硬件设计有固定的bitlength，三元组可进行预处理产生challenge
(i): lab, pwdu和dom连接成Sr，包含lr个字符.
(ii). Sr格式化为一或多个challenge Sc，每个challenge包含lf个字符，则Sr可分为ns个挑战，ns=⌈lr/lf⌉
若无法整除，则进行填充，如6位: abcd → abcdab 填充是为了保证challenge的多样性.
(iii) 根据ASCII表，将字符转换成bit，构成valid challenge
③ Strengthening Phase: 访问PUF.
为指每个site生成唯一的口令，本阶段response生成并发送给下一阶段，response bit数由网站口令的策略决定.
④ Posttreatment Phase: response经过进一步处理，以满足网站的口令策略
▲ 若ns>1，则多个挑战的响应可以异或为一个响应.
响应进一步编码来生成满足口令策略的pws；响应的bit分成多组，每组ng bit，每组模d取余转换成网站口令的一个字符. (ng ≥ log2 d) ▲ ng, l和d由应用开发商设置.

2) Instantiation
① 当敌手可以访问到CRP时，R有arbiter PUF容易遭受modeling attack，本文引入voter based PUF，除了抵抗上述攻击，还提供了较强的reliability (ECC方法也可以提供)
② 希望可以让用户决定是否使用PUFPass，提供了复选框

3、安全性评估(4个潜在的漏洞)
1) User Password: 通过肩窥或钓鱼攻击获取用户口令的敌手由于未知label且没有设备，因此无法获取网站口令
2) Device: 敌手获取设备后，可对user password进行在线猜测，可通过网站的检测机制防止.
3) Site Password: 由于生成的网站口令各不相同，故一个网站口令泄漏不会影响其它网站
4) Server: 破坏Server的敌手可以执行离线猜测，经过Hashcat测试，表明PUFPass可以较好地抵抗离线猜测攻击
5) Device & Site Password: CRP可以建模为R=F(C,P)，R代表response，C代表challenge，P代表由处理过程决定的电子参数
在PUFPass中，R=C(lab, dom, pwdu, P)，其中pwdu和P是敌手未知的.
使用Compound Heuristic Algorithm测试发现，当敌手获取10000网站口令时，能匹配到用户口令的几率只有2.3%。而实际中用户平均帐户更少，故又可以抵抗对user password的离线攻击

4、可用性分析.
1) Ease of use: 用户可通过复选框选择用或不用PUFPass；吞吐量：1s可以生成10.5×10^6响应bit
2) Memory burden: 用户只需记忆1个主口令即可为不同网站生成口令
3) Transportability: 认为目前高安全性的应用对可移植性的需求减少，而且可以通过二维码登录网站，故认为不需要可移植性
4) Password Modification: 若因为口令泄漏，可以更改pwdu或lab值更新口令；若忘记口令则只能利用邮件等更改