USENIX'18 - Lai - Simple Password-Hardened Encryption Services

优点：① 本文基于PHOENIX提出了PHE的概念，可以应用于许多保护用户隐私的协议。
② 进一步增强了PHOENIX的安全性定义，特别是strong soundness
③ 引申出几个扩展研究方向，包括口令管理等

问题：① 本文仍有PHOENIX的一些问题，包括 1) 不提供用户匿名，泄漏用户隐私，用户的登录行为均会被rate limiter得知 2) 单点故障(rate-limiter) 3) 无法及时检测泄漏事件 4) key rotation 无法提供 S、R 单独的 rotation.
② 应分析 S、R之间TLS连接可能存在的问题；若恶意S执行了 key rotation，系统会丧失可用性 ③ 用户拥有secret message不太合理，需引入如USB key 的额外设备.

为了加密除口令之外的其它隐私数据本文在PHOENIX的基础上构建了一种简化的Password-hardened Encryption，通过 crypto server 对用户的隐私数据进行加密，相比于PHOENIX，本文方案提供了更高的安全性，更低的开销，且易于部署，无需用户 DB 结构做过多改动。

▲ 研究动机

现实应用场景中，许多用户数据需要加密存储，然而只要 online service provider 可以做对数据库的解密操作，破坏SP的做法可以解密数据库并得到用户的隐私信息.

▲ 一种解决方案，使用 external layer protection，例如 Password-hardening (PH)
server provider ⇒ server(S), crypto server ⇒ rate limiter. (R).
→ 提供3个基本保证：① S和R都无法独立验证 pw 的正确性.
② rate-limiter 可记录不成功登录的次数，进而阻止在线攻击
③ rate-limiter 无法获知 pw 的信息
④ 支持 server 和 rate limiter 的 key rotation (其中更新无需用户参与且 rate-limiter 参与较少，且 record 可以在 server 本地更新)
→ 但PH仅提供对口令的保护且不提供解密功能（即仅提供了认证功能）

▲ PHE可以加密其它数据，server 和 rate limiter 共同产生 record，除了加密 password，还加密了 secret message (例如一个对称密钥 AES key，用加解密隐私数据加密后 discard，解密时再重新生成 key 来解密隐私数据.

▲ PHE 拥有PH的4个基本保证，适用于保护用户隐私数据的基于口令的认证系统，另外还可以用于 password vault，用户口令作为 master password，来加密其它高熵口令.

▲ 本文方案的技术概览：① 将PHOENIX从 non-black-box 的方式转换成 PHE 方案.
② 之前 PH 方案不区分 rate-limiter 由于次数限制还是口令错误而拒绝，本文在 rate-limiter 接收和拒绝时都提供原因，防止 rate-limiter 作恶拒绝合法请求 ③ 扩展并简化原本PH的安全定义

Password-Hardened Encryption (PHE)

▲ 入为安全参数，P,M代表口令空间和 message 空间，(u,v) ←$ P(S(x), R(y)) (t协议P，公共输入l)，空串为ε，包含算法 (Setup, kGen_S, kGen_R, Encrypt, Decrypt, Rotate, Update)

▲ Setup and key Generation: pp ← Setup(1^λ), (pk_S, sk_S) ← kGen_S(pp), (pk_R, sk_R) ← kGen_R(pp)

▲ Encryption: 用户使用pw和M注册，S与R执行加密t协议得到 label 为 l' 的记录 T.
((l', T), ε) ← Encrypt^t ⟨S(sk_S, pw, M), R(sk_R)⟩，公共输入 l = (l_S, l_R).
S输出 l' = (l'_S, l'_R) 的记录 T，R 输出 ε
其中 l'_S = l_S 只在前向安全性定义中出现. ② l = ε，适用于其它情况，在t协议执行时取值
l = (l_S, l_R)，可视作会话标识符或 S、R 给用户的假名.

▲ Decryption: 用户使用pw登录，S找到对应的 T 和 label，与S共同执行解密t协议
((l_f, M), ε) ← Decrypt^t ⟨S(sk_S, pw, T), R(sk_R)⟩.
S输出 flag f 和 M ① f = ⊥，rate limiter abort ② f = 0，T或pw invalid.
③ f = 1，成功登录. R输出 ε

▲ key Rotation and Record Update. 包含2步
① S和R执行 key rotation t协议更新 key 并计算 update token.
((pk'_S, sk'_S, τ), (pk'_R, sk'_R)) ← Rotate⟨S(sk_S), R(sk_R)⟩
② S使用 τ 本地运行更新 T 的算法. T' ← Update^t(τ, T)，(本文不考虑 M 的变化)

PHE的安全性分析(思路). → key rotation 可将t协议执行分成不同 round.
▲ 假设S和R之间合法建立 TLS 连接.
▲ Message Hiding：即使 S compromise，A 无法区分 T* 中是 M_0* 还是 M_1*，即使 M, pw 分布由A选取
A = (A_1, A_2)：S，challenger：R
① A_1 可选择输入进行 encryption, decryption 和 key update oracle，A_1 输出 sk_S*，口令分布 X，两消息 M_0*, M_1* 及 state st.
② challenger 选取 pw*，本地模拟加密t协议，通过 l_S*, sk_S*, M_b*, pw* 得到 T*. (未给 A).
③ A_2 得到 l_S* 和 T*，通过输出 b' 来猜测 M_0*, M_1* 中那个被加密.
故 A 至多可以通过与 R 交互在线猜测口令，|Pr[Hid^0_{PHE,A}(1^λ)=1] − Pr[Hid^1_{PHE,A}(1^λ)=1]| ≤ q_send/|P| + negl(λ)
▲ Partially Obliviousness.，R 无法获取 pw 及 secret message，但未提供用户匿名性.
A = (A_1, A_2, A_3)：R，challenger：S.
① A_1 与 challenger 交互，最终输出两个 pw-M 对 (pw_0*, M_0*, pw_1*, M_1*)，及 st 给 A_2

② challenger 使用上述 $pw-M$ 与 $\mathcal{A}_2$ 交互，最终输出 label 为 l^* 的 T^*，发送给 $\mathcal{A}_3$；$\mathcal{A}_2$ 将state给 $\mathcal{A}_3$

③ $\mathcal{A}_3$ 与 challenger 交互并最终输出 b' 标识 $pw-M$ 是否与所选的 challenge 一致.

$|Pr[Obl^0_{PHE,\mathcal{A}}(1^\lambda)=1] - Pr[Obl^1_{PHE,\mathcal{A}}(1^\lambda)=1]| \le negl(\lambda)$

▲ Soundness (本文提供的 strong 版本)

① 当R正确执行时，可保证pw正确时可恢复出M，而pw不正确时，无法恢复出M.

② 当R为恶意时，其恶意行为也会被检测到：ⓐ S在解密相同输入的T时输出不同

ⓑ 在 label-pw 对不一致时使S相信解密是有效的.

$Pr[Strong\ Soundness_{PHE,\mathcal{A}}(1^\lambda)=1] \le negl(\lambda)$.

▲ Forward Security

即使是恶意生成的 record 和 key，更新的 key 和 record 仍与原始生成的不可区分.

$|Pr[Fwd\ Sec^0_{PHE,\mathcal{A}}(1^\lambda)=1] - Pr[Fwd\ Sec^1_{PHE,\mathcal{A}}(1^\lambda)=1]| \le negl(\lambda)$.

本文方案构造.

▲ $\mathbb{G}$ 为有限循环群，阶为 q，单位元为 $\mathbb{I}$，Π 为 DL 的 NIZKPoK 方案，$H_S, H_R: \{0,1\}^* \to \mathbb{G}$

$p := \{0,1\}^*$, $M := \mathbb{G}$

▲ Setup and key Generation.

Setup(1^λ): $crs \leftarrow \$ \Pi.Gen(1^\lambda)$, $\mathbb{G} \leftarrow \$ \mathbb{G}$

KGen$_S$(pp): $pk_S \leftarrow \varepsilon$, $sk_S \leftarrow y \leftarrow \$ \mathbb{Z}_q$.

KGen$_R$(pp): $x \leftarrow \$ \mathbb{Z}_q$, $X \leftarrow \mathbb{G}^x$, $pk_R \leftarrow X$, $sk_R \leftarrow x$

▲ Encryption (l 若为空，则可随机取值 n_S, n_R，若非空，则解析为 (n_S, n_R)).

S ($pk_R \to X$, $sk_S \to y$)		R. ($sk_R \to x$).
		$H_{R,0} \leftarrow H_R(n_R, 0)$, $H_{R,1} \leftarrow H_R(n_R, 1)$.
		$C = (C_0, C_1) \leftarrow (H_{R,0}^r, H_{R,1}^x)$.
		$stmt \leftarrow$ "$\exists x$ 有 $(C_0, C_1, X) = (H_{R,0}^x, H_{R,1}^x, G^x)$"
		$wit \leftarrow x$ $\pi \leftarrow \Pi.Pok(crs, stmt, wit)$
$H_{S,0} \leftarrow H_S(pw, n_{S,0})$, $H_{S,1} \leftarrow H_S(pw, n_{S,1})$.	$\xleftarrow{(n_R, C, \pi)}$	
$H_{R,0} \leftarrow H_R(n_R, 0)$, $H_{R,1} \leftarrow H_R(n_R, 1)$.		
$stmt \leftarrow$ "$\exists x$ 有 $(C_0, C_1, X) = (H_{R,0}^x, H_{R,1}^x, G^x)$"		
若 $\Pi.Vf(crs, stmt, \pi) = 0$，返回 $\perp$.		
$T \leftarrow (C_0 H_{S,0}^y, C_1 H_{S,1}^y, M^y)$, $l' \leftarrow (n_R n_S)$.		
返回 (l', T).		

▲ Decryption. ($pk_R \to X$, $sk_S \to y$, $sk_R \to x$, $T \to (T_0, T_1)$).

S		R.
		$H_{R,0} \leftarrow H_R(n_R, 0)$, $H_{R,1} \leftarrow H_R(n_R, 1)$.
$H_{S,0} \leftarrow H_S(pw, n_{S,0})$, $H_{S,1} \leftarrow H_S(pw, n_{S,1})$.		
$C_0 \leftarrow T_0 H_{S,0}^{-y}$	$\xrightarrow{C_0}$	$H_{R,0} \leftarrow H_R(n_R, 0)$, $H_{R,1} \leftarrow H_R(n_R, 1)$.
		①: $C_0 = H_{R,0}^x$. 则 $f \leftarrow 1$, $C_1 \leftarrow H_{R,1}^x$
		$stmt \leftarrow$ "$\exists x$ 有 $(C_0, C_1, X) = (H_{R,0}^x, H_{R,1}^x, G^x)$".
		$wit \leftarrow x$.
		② $C_0 \neq H_{R,0}^x$，则 $f \leftarrow 0$, $r \leftarrow \$ \mathbb{Z}_q$, $C_0' \leftarrow C_0^r H_{R,0}^{-rx}$.
		$stmt \leftarrow$ "$\exists (\alpha, \beta)$ 有 $(C_0', I) = (C_0^\alpha H_{R,0}^\beta X^\alpha G^\beta)$"
		$wit \leftarrow (\alpha, \beta) = (r, -rx)$.
→ 成功登录		
① $f=1$, $stmt \leftarrow$ "$\exists x$ 有 $(C_0, C_1, X) = (H_{R,0}^x, H_{R,1}^x, G^x)$"	$\xleftarrow{(f, C_1, \pi)}$	$\pi \leftarrow \Pi.Pok(crs, stmt, wit)$.
$M \leftarrow (T_1 C_1^{-1} H_{S,1}^{-y})^{\frac{1}{x}}$		
② $f=0 \wedge C_1 \neq \mathbb{I}$ T或pw invalid.		
$stmt \leftarrow$ "$\exists (\alpha, \beta)$ 有 $(C_1, \mathbb{I}) = (C_0^\alpha H_{R,0}^\beta \cdot X^\alpha G^\beta)$"		
$M \leftarrow \varepsilon$.		
若 $\Pi.Vf(crs, stmt, \pi) = 1$，返回 (f, M)		
否则返回 $(\perp, \varepsilon)$.		

▲ key Rotation and Update.

Rotate$\langle S(sk_S), R(sk_R) \rangle$. ($sk_S \to y$, $sk_R \to x$)

S		R.
		$\alpha, \beta \leftarrow \$ \mathbb{Z}_q$.
	$\xleftarrow{(\alpha, \beta)}$	
$y' \leftarrow \alpha y$		$x' \leftarrow \alpha x + \beta$
$\tau \leftarrow (\alpha, \beta)$.		
$pk_S' \leftarrow \varepsilon$		$pk_R' \leftarrow G^{x'}$
$sk_S' \leftarrow y'$		$sk_R' \leftarrow x'$

Update$^\tau(\tau, T)$. $pk_R \to X$.

$\tau \to (\alpha, \beta)$, $T \to (T_0, T_1)$.

$H_{R,0} \leftarrow H_R(n_R, 0)$.

$H_{R,1} \leftarrow H_R(n_R, 1)$

$T_0' \leftarrow T_0^\alpha H_{R,0}^\beta$.

$T_1' \leftarrow T_1^\alpha H_{R,1}^\beta$.

$T' \leftarrow (T_0', T_1')$