1992 IEEE Symposium on Research in Security & Privacy. Bellovin & Merritt

Encrypted key Exchange: Password-Based Protocols Secure Against Dictionary Attacks

总结：本文讲述了一种结合非对称和对称密码体制的允许参与方共享口令来进行密钥交换的协议EKE，可防止主动攻击并保护口令免受字典攻击，在弱口令存在的网络环境中为通信安全提供了保障。主要介绍传统口令密钥协商协议的问题[1]，EKE如何解决这一问题[2]及EKE的几种变体[3]（RSA-EKE，Diffie-Hellman EKE和ElGamal EKE）以及EKE在实践中的应用和建议[4]。

注：R: session key；P: password；Ex：X的公钥；Dx：X的私钥.

传统PKA协议的问题

A ⟵ 共享口令P ⟶ B

随机R

$\xrightarrow{P(R)}$ $R=P^{-1}(P(R))$

解密 $\xleftarrow{R(\cdots)}$

P为一低熵口令，持久化

窃听者可拿到：P(R)，R(…).

对P做离线字典攻击，求 $R'=P'^{-1}(P(R))$.

若 $R'^{-1}(R(\ldots))$ 有意义则 P' 可能正确

问题：如何在不安全的网络环境中实现抵抗离线字典攻击的KA协议

EKE协议

A ⟵ 共享P ⟶ B

随机E_A, D_A

⇒ $P(E_A)$ $\xrightarrow[RPK\cdot1]{A,\,P(E_A)}$ $E_A=P^{-1}(P(E_A))$ ⇒随机R

$R=D_A(P^{-1}(P(E_A(R))))$ $\xleftarrow[RPK\cdot2]{P(E_A(R))}$ ⇒$P(E_A(R))$

生成挑战C_A

$\xrightarrow[RPK\cdot3]{R(C_A)}$ ⇒ C_A，生成C_B ⇒$R(C_A, C_B)$

解密⇒$C_A C_B$ 比较C_A ✓ $\xleftarrow[RPK\cdot4]{R(C_A, C_B)}$

发送$R(C_B)$ $\xrightarrow[RPK\cdot5]{R(C_B)}$ 解密⇒C_B并比较 若匹配则可通信

①对于RPK1,2，窃听者可得$P(E_A)$，$P(E_A(R))$ 假设还有R(…)

→猜测P'只能得到E_A'，验证猜测只能通过$E_A'(R')=E_A(R)$且$R'^{-1}(\ldots)$有意义

但E_A和R的密钥空间很大，若验证只能穷举(不做密码分析)，使猜测P的代价也变大，抵抗离线字典攻击.

②RPK3~5：挑战响应，常用于验证密钥使用能力，保证新鲜度。如A发送R(C)，并收到另一个包含C的密文则可认为对方有使用R加密的能力(防止重放攻击)

▲口令password的使用

(P可用于加密两次，1. $P(E_A)$ 2. $P(E_A(R))$)

根据公钥算法，两个过程可省略一个，也存在一些情况不可用P加密。

P加密的消息有特征，可能导致分区攻击.(应尽可能随机)

比如RSA的e一定为奇数，n无素数小因子等，若无预防措施可能导致口令空间以对数级别下降，即几次拦截会话就足以拒绝所有对P的不合法猜测

另外：① 模素数p，P加密n比特，则解密结果区间为$[p, 2^n-1]$的可排除若p与2^n接近，则排除很少，但若$p=2^{n-1}$等差距大，则比p大的都被剔除

② 若分组很大，可能需要高位添0，这可能导致攻击。可填随机数

以上攻击可以通过给输入的分组添加 ip 来解决$i\in[0, x-1]$，$x=\lfloor \frac{2^m}{p} \rfloor$，

加密哪个消息与协议设计也有关，不加密的一方不可先生成挑战，

如A不加密发送E_A，且先生成挑战$R(C_A)$，R本身由P和E_A决定，E_A已知，P空间小，可能被攻击。

RSA-EKE

如何得到公钥⟨e,n⟩，使其尽可能随机

对于n，n=p.q，由两个大素数组成，若加密，则可通过猜测P'来看结果是否有小的素因子来排除，故n一般明文传输(可能被密码分析而因式分解)

对于e，上述提到只为奇数，故可以以½概率e+1，窃听者不知道偶数为e+1还是真偶数，e足够随机。

接收者收到e后若为偶数，e-1即可.

e要与φ(n)互素，假设 $p=2p'+1$，$q=2q'+1$，p', q'为素数，此时大部分奇数 mod n 都与 $(p-1)(q-1)=4p'q'$ 互素，e可选范围很大。

若n, e均以明文传输，攻击者可伪装成A，生成p, q, e, n.

若e不满足 $ed\equiv1 \pmod{\varphi(n)}$，则可发动攻击。

$E_A(R)=R^e \pmod n$ 会产生e次剩余、有特征，只需测试 $P'^{-1}(P(E_A(R)))$ 是否会产生e次剩余即可发动离线字典攻击.

一个防范方法是，B识别虚假的e，通过交互，B发送r^e给A，若A可返回r则A是合法的，但交互代价较大。

ElGamal-EKE

(基数α，模β，在0~β-1均匀分布的k)

RPK·1 $P(\alpha^{R_A} \pmod\beta)$，RPK·2 $P(\alpha^k \pmod\beta)$，$R\alpha^{R_A\cdot k} \pmod\beta)$

考虑到挑战响应的类型，第二条不可以明文传输，否则：

攻击者拦截了$P(\alpha^{R_A} \pmod\beta))$，将RPK.2换为：$\alpha^k \pmod\beta$)，$RX \pmod\beta$)

A仍计算 $k\equiv\alpha^{R_A\cdot k} \pmod\beta \Rightarrow R'\equiv\frac{RX}{\alpha^{R_A k}} \pmod\beta \Rightarrow R'(C_A)$.

若C_A有冗余信息如校验和，则猜测 $P'\Rightarrow(\alpha^{R_A})'\Rightarrow R'$ 可验证猜测

▲与RSA相比，这种攻击是无需私钥即可拿到M，即需公钥和k，因此对k要严格保护 (disclosing encryption system).

▲如何抵抗密码分析攻击?

攻击者恢复了部分会话密钥有助于攻击P，尝试攻击E_A并去匹配$(P'^{-1}(P(E_A)))(R)$. 验证猜测

→对策：在挑战响应中，A, B生成子密钥S_A和S_B，用R加密

RPK·3 $R(C_A, S_A)$，RPK·4 $R(C_A, C_B, S_B)$，⇒会话密钥 $S=f(S_A, S_B)$

R只用于加密随机信息，且不包含S.

▲攻击者也可能通过收集挑战响应对攻击，此时可用单向函数加密挑战

Diffie-Hellman EKE

A ⟵⟶ B

随机R_A，

$P(\alpha^{R_A} \pmod\beta))$ $\xrightarrow[RDH\cdot1]{A,\,P(\alpha^{R_A} \pmod\beta))}$ 选R_B，$\alpha^{R_B} \pmod\beta$)

$K\equiv\alpha^{R_A R_B} \bmod \beta$

得k，C_B 生成C_A $\xleftarrow[RDH\cdot2]{P(\alpha^{R_B} \bmod\beta),\,k(C_B)}$ 随机C_B.

$\xrightarrow[RDH\cdot3]{k(C_A, C_B)}$ 验证C_B

验证C_A. $\xleftarrow[RDH\cdot4]{k(C_A)}$

▲ 若攻击者选0为指数，k=1，这可以检测(但未知其他情况)

▲ 一般选较大的β=2p+1，p素数，α为GF(β)的本原根.

▲ α和β一般以明文传输，首次会话时公开.

实践应用建议

1> 对称加密体制加密不能泄露信息，尤其是口令加密

2> 公钥应足够随机，有特征如素数应不加密或不使用

3> 有关联的对称和非对称算法不应同时使用。