Public-key Cryptography and Password Protocols - TOPS'99
Halevi Shai & Krawczyk Hugo

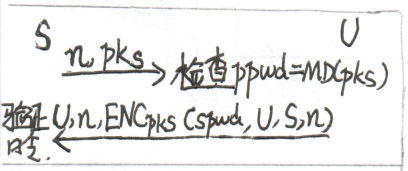
优点：①研究了非对称场景中(即S持有公私钥，而U只有口令)的强鉴别协议和密钥交换的协议，且表明了这些协议可在标准密码下可证明；②严格证明了公钥技术对于抵抗离线猜测攻击是必要的；引入了public password的概念，适用于用户无S的公钥的情况；另外，也介绍了语义安全性无法保证协议的安全性
③文中的证明(特别是指出猜的过程)论述清晰

问题：①文中提出的public password提前提供给用户这一操作，是为了验证月服务器钥匙但提到public password只保证完整性，即用于S是安全的情况，且用户再持有一个public password也会影响可行性；②文中摘要中先提到公钥技术在对抗离线猜测攻击的重要性，后引入到public password，文章中相反
③3.3节介绍Server Compromise时，若口令文件丢失而服务器私钥安全，则敌手仍要猜测p_2，但p_2与p_1结构相同应也需做进一步猜测。

使用S公钥的口令鉴别

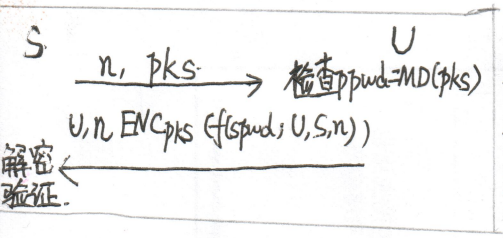
预设public password: ppwd:=MD(pks)

1>加密口令传输



ENC足够随机，
随机数n用于提供freshness

2>通用Challenge-Response协议(后续主要研究)



只通过公钥隐藏响应来防止离线猜测攻击是不足够的.
另外采用了一对一的函数f来使用口令加密

▲ENC的安全性：①语义安全性要求ENC必须足够随机，即给定公钥pk，密文c，可能明文m_1，m_2，只通过加密m_1，m_2去比较是不够的.(但这不足以证明协议安全性).
②抵抗选择密文攻击 弱化→ cipher text-verification攻击
即敌手对给定的(m', c')可知c'是否为m'的密文$(c'=c)$

▲f:;的结构：保证一对一：one to one.(抗碰撞)
其中，$f(spwd;n,U,S)=(spwd,n,U,S)$为一对一

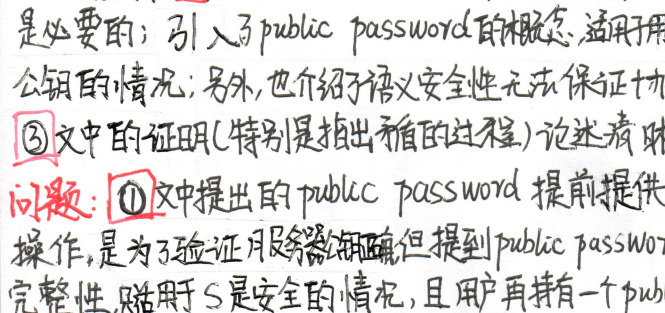
▲实现用户匿名性：用户的U仅在第2步的ENC_{pks}中传输，即S在未知用户身份的情况下发送ppwd和挑战.

▲通过更改f的定义可抵抗服务器被攻破例：
$p_1=H_1(spwd;U,S)$，$p_2=H_2(spwd,U,S)$，$p_3=H_3(p_2,salt)$
$\Rightarrow f(spwd;n,U,S)\overset{def}{=}\langle MAC_{p_1}(n,U,S),p_2,n\rangle$.
可抵抗服务器私钥被破坏及口令文件被破坏.

3.7. 双向鉴别与密钥交换.

▲双向鉴别：U在第2步将一个密钥k(用公钥)加密后发送给S，S使用k来作为MAC的密钥.(只有S可解密)

▲前向安全性：采用DH交换来完成



语义安全性不足以抵抗离线猜测攻击：敌手可通过只替换响应C中的前面的一个或多个比特位来排除多个口令，实现穷举攻击，因此必须要增加抵抗cipher text-verification攻击.

证明单向口令鉴别的安全性.

Game：安全参数k公开.

S：选择公私钥(sks, pks)，公开pks，接收(U, spwd)
可开启会话sid，收到(U, sid, a)
若存在(U, spwd)和sid，鉴别成功输出(U, sid)并删除sid
鉴别失败，输出(U, sid, ⊥).

U：选spwd，发送U和spwd给S，
收到sid时发送⟨U, sid, a⟩，并输出(S, sid).
敌手可窃听、篡改或终止会话、创建用户，

▲证明定理1：一个抵抗密文验证攻击的加密方案，f为一对一函数，则被破坏的概率至多为$G'(k,l,m)=m\cdot l\cdot\varepsilon(k)$
→若敌手产生一个U-reply $y=\langle U,sid,a\rangle$但与用户U的reply均不同且被S接受，则I fool S，只有fool，才能赢得game.→当限制敌手不可转发未更改的U-reply及不可重放时，仍有相同概率→(采用矛盾证明)：若概率p为(l,m)-run，(m次主动猜测，U至多输出l对(S,sid))，则对于(l,1)-run，概率$p_1\geq p_m=\frac{1}{m^l}+\varepsilon_m$，→则敌手在密文验证攻击中有优势$G=\varepsilon_m'$，与假设(抵抗密文验证攻击)矛盾.

安全口令协议需公钥技术抵抗离线猜测攻击；通过证明可保证单向口令鉴别的协议也可完成密钥交换完成.
对于一个抵抗字典攻击的口令认证协议，若字典空间为2，则若S和U选择了相同口令才可交换，否则则重新选择口令，而窃听者无法猜测口令，因此可完成secret的交换

Public Passwords. 用于U无法验证S公钥.，需保证完整性.
一般通过映射为可读字符，提供相似字符串供用户选择，或通过图形完成.