NDSS'98 The Secure Remote Password Protocol - SRP

介绍一种口令认证和密钥交换协议，SRP，结合零知识证明和非对称密钥交换，口令以非明文对等的方式存储在server中，可抵抗字典攻击，提供前向安全性。比同时期verifier-based协议的性能高(digital signature, A-EKE, CCS'93 和 secondary one-sided key exchange, B-SPEKE, WETICE workshop'97).

优点：1>指出之前协议普遍存在的问题(明文对等)，提出新方案，并与现存verifier-based方案做了对比；2>对提出的SRP协议的原理、安全性和性能都做了详细描述；3>基于零知识证明和公钥密码技术提出了第三种verifier-based的方案。

问题：1>本文的安全性分析主要以协议可以抵抗各种类型攻击进行说明，仍是以启发式的方法，从后续不断修补提出新版本也可得知。无严格的安全性证明。另在4.3节中也提到可能无法抵御所有攻击，而规约为CDH问题只是被动窃听攻击困难。2>分析5.2节执行速度时定义了三种类型的模幂运算，但是在列表时无分析表中值分别对应哪一步(因为本身数字的大小很难界定，个人认为易产生歧义。3>3.2.2节介绍SRP协议，客户端无需保存服务器口令而是使用固定值，应存在情景限定如S中多个验证题4>部分文字无明显解释：如：①3.1中S(b,v)要保护第2个参数不被泄露，未解释原因。②3.2.4节，u的角色提出问题为何u一直存在，但分析结论为u必须在收到A后生成。③椭圆曲线算法的提出用于提升效率是有意义的。5>本文的威胁模型未给出(或不清晰)

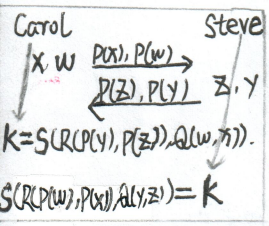
AKE 满足 $\forall w,x,y,z$, $S(R(P(w),P(x)),Q(y,z))=S(R(P(y),P(z)),Q(w,x))$

其中x,z为长期密钥(口令)，w,y为临时参数

P(x)：单向verifier生成器，R：mixing函数

S(x,y)：生成会话密钥，安全性取决于各函数

区别好于EKE等：无需加密，且不共享口令。



▲不加密而采用数学关系的好处：①简化协议。②避免加密过程的脆弱性 ③避免算法等使用权的限制。

▲AKE采用 swapped-secret，一方计算secret执行单向函数生成verifier发送给另一方。⇒仍应保护verifier防止字典攻击，但verifier丢失不足以让敌手伪装成合法实体。

在服务器存储大量verifier时，可以仅客户端生成secret，而注册和更改过程只需传verifier.

SRP 运算于有限域GF(n)，模n(大素数)，生成元g，单向函数 $P(x)=g^x$

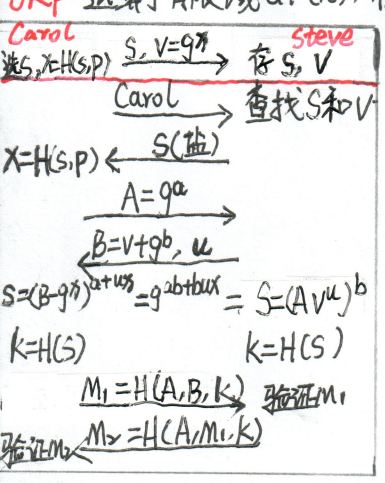
$Q(w,x)=w+ux$, $R(w,x)=w^u$

$S(w,x)=w^x$ $u=f(w,y)$.

u为随机干扰参数，公开的，

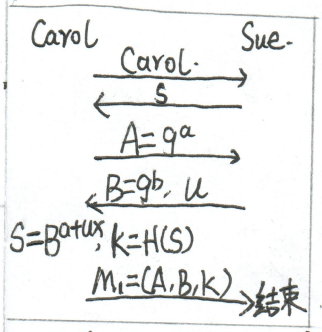
a,b 临时私钥，随机不公开.

A,B公钥，H()单向哈希.



Q1：为什么发 $B=v+g^b$ 而不发 $B=g^b$？易受字典攻击

敌手Sue从合法会话中得到了盐值s.



敌手Sue拥有A, b, M_1, S

可猜口令 $p' \Rightarrow x' \Rightarrow v' \Rightarrow S'=(Av'^u)^b$

$\Rightarrow k'=H(S')$，与M_1信息对比.

若匹配则攻击成功

故应发送 $B=v+g^b$，让Sue无法得到可验证文本(v和g^b应怎样组合).

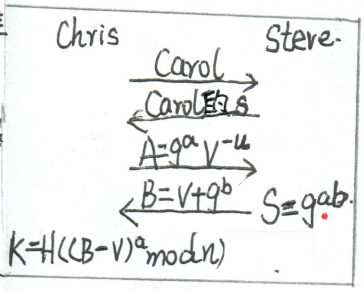
$B=f(v,g^b)$，应保护v(不泄露信息)，(模加运算不泄露v且可抗字典攻击.)

①避免 $f(g^x,g^y)=gf(x,y)$ 中 $f(x)$ 为简单派生函数，如 $f(x)=xy$.

②避免分区攻击，即泄露v的信息，如用 $f(x,y)=x\oplus y$。且要求g必须为GF(n)的本原根，使任何v对应的B值等概率.

Q2：u的作用？

敌手Chris已知u和v，可获取主机访问权。



$S=g^{ab}$，与长期私钥无关.

Chris可以Carol身份访问，

故u应在Steve收到A后再公开

(u=0也是不可以的).

安全性分析(未证明安全性)：该部分的描述挺好的

要求：①一次成功执行不会泄露口令或私钥x的任何信息.

②窃听者无法从成功执行的会话中获取K的信息

③敌手无法通过篡改信息成功访问或获取有用信息.

④敌手即使获取v，也只能通过代价大的字典攻击来伪造.

⑤过去的sk泄露不会暴露口令

⑥口令被敌手获取无法得知过去sk的信息。用户修改口令后被破坏的风险减小。(前向安全性)

▲SRP可通过替换归约为DH，故SRP可以提供DH协议的抗窃听能力

▲SRP中，即使k泄露，也只能计算M_1、M_2，而无法做字典攻击.

▲对文章中考虑的主动攻击可以抵抗，例如敌手未知x无法欺骗Steve，未知v无法欺骗Carol.

安全假设和约束

①$P(x)=g^x$必须为不可逆，保证n足够大.

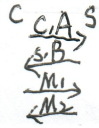
②n必须为non-smooth素数，即n-1不可完全由小因子构成，可令 $n=2p+1$，p也为素数.

③客户端应检查n为大的安全素数，g为GF(n)本原根，B≠0防止字典攻击.

服务器检查A≠0，防止S=0

都应检查 $a,b>\log_g n$，防止直接算对数就恢复n.

消息轮数、消息大小和执行时间都影响SRP性能，可合并独立参数的发送.



执行速度中，群运算中的模幂最耗时，可通过提前计算 g^a 和 g^b