电子学报'15 基于RSA的网关口令认证密钥交换协议的分析与改进

指出 Wei'11 的RSA-GPAKE协议中"口令保护"目标未能实现的原因，改进为RSA-GPAKE(+)协议，并进行了形式化安全证明

优点：① 指出分离攻击是针对基于RSA的PAKE协议的严重安全威胁

② 描述了形式化证明可能出错的原因及启发式分析的重要性 2015 TDSC54

③ 描述结构和逻辑清晰，读者友好

问题：① 安全性证明中仍略去了认证性

② 口令安全证明结果中应为 $\frac{2q_{oh}}{\varphi(n)}$

③ Game$_2$中，$\mathcal{A}$仿冒用户C，假设$\mathcal{A}$已得到口令pw且计算了α，再验证α正确性的顺序可能会不易读懂

基于RSA的PAKE协议易遭受一类特殊的字典攻击：

分割攻击(Partition Attack)，结合离线与在线字典攻击：

① 仿冒用户参与协议来收集口令相关信息 → 通常多于1个

② 离线地从口令字典中过滤掉非潜在口令 → 只剩1个

主要分为两种 { e次乘余攻击 e-Residue Attack (研究多)
分离攻击 ▲ Separation Attack.

只能从密码协议设计层面防御.

GPAKE中的攻击者能力：Execute、Send、Test、TestPair.

在ROR游戏中，敌手不使用Reveal查询，而是可以使用多个Test，但查询结果仍由掷出特b代替，用于保证sk的语义安全性

安全目标

① 语义安全性：优势$Adv^{ake\text{-}ror}_{P,D}(\mathcal{A}) \le \frac{n_s}{|D|} + \varepsilon(k)$ t为主动攻击次数 区分sk和随机串

② 认证性：敌手的目标为仿冒用户或网关(保证匹配会话正确)

③ 密钥私密性：敌手优势$Adv^{ake\text{-}kp}_{P,D}(\mathcal{A})(k) \le \varepsilon(k)$，降低对S的信任

④ 口令保护：敌手优势$Adv^{ake\text{-}uoda}_{P,D}(\mathcal{A}) \le \frac{n_s}{|D|} + \varepsilon(k)$，保证敌手无法以明显高于一次排除一个口令的优势攻击.

针对RSA-GPAKE的分离攻击→针对"口令保护"的安全目标、敌手可为外部攻击者或恶意网关，可主动、被动攻击，在PPT内终止

▲对于外部攻击者，伪装为用户，① (对于恶意网关，则对B执行此) gcd(α,n)≠1，则拒绝，直接结束会话

C ① G ② S.

重复①② 计算α，检验gcd(α,n)=1是否成立. 提供了分析方法.

直到gcd(α,n)=1成立，终止会话.(可通过S的响应确定)

C可选取pw，计算α^e验证gcd(α^e,n)=1是否成立，不成立则排除

根据上述步骤，若$n_A=3p$，则可以用少于52次假冒会话恢复口令

防御方法(非密码学方式无法解决).

① 避免n含有小因子： 小因子无法界定，过小则敌手仍可通过一次成功测试会话排除掉许多口令，过大则会增加S的负载

② 限制敌手发起假冒会话的次数也无法抵御

a). 限制假冒会话的总次数：易影响可用性(DoS攻击).

b) 限制连续假冒会话次数的方式：敌手可以通过交叉地在用户的正常会话间发起假冒会话绕过此限制.

形式化证明的失误：Provably secure, but actually insecure.

▲对协议的形式化证明是手段而非结果，而启发式分析在建立和保持对密码协议的信任方面仍不可代替.

改进协议RSA-GPAKE+(仅记录修改的部分)

C → G → S.

C, n, e, Y_2, Z ← Y_2, Z

S：计算α，若gcd(α,n)≠1，令Z为G_R之类

否则Z = $E^m(\alpha E(\alpha_1))$.

若gcd(α,n)=1，计算C_1, α_1

否则$\alpha_1 G_R$之类，$C_1 G_R$之类 ...

易知gcd(α,n)≠1时，不会终止会话，而是选择随机值返回Z.

敌手若未知pw，则无法得α，也不知α_1，也无法算出μ.

而实际中用户与服务器的交互与PEKEP类似(可参考证明口令安全)

▲与RSA-GPAKE相比，引入了Hash运算和随机数生成运算未引入幂指运算

基于RSA假设对口令保护的形式化证明，q_{send}, q_{exe}, q_{oh}.

一系列混合仿真游戏，逐步修改预言机的回答方式.

Game$_n$的事件：$Adv^{ake\text{-}uoda}_{P,D}$ 简写为 $Pr[Succ_n]$

Succ$_n$：$\mathcal{A}$成功猜测出α

AskPara$_n$：$\mathcal{A}$查询H_1得到α ($pw||Y_1||Y_2||ID_i$)

AskAuth$_n$：$\mathcal{A}$成功计算出α_1，并查询了H_1或H_2

AskH$_n$：$\mathcal{A}$正确查询了H_1, H_2, H_3.

Game$_0$：在ROM下的真实攻击，有$Adv(\mathcal{A}) = Pr[Succ_0]$

Game$_1$：正常模拟哈希，及Game$_0$，b使用的私有哈希，并维护Hash查询列表，其它查询与真实协议一样，有$Pr[Succ_1] - Pr[Succ_0] = 0$

Game$_2$：去掉不太可能出现的碰撞.

① 通信消息(C, n, e, Y_1), (n', e', Y_2, Z) (C, C_1, μ), (C, η)，pw的碰撞参与方至少一个是诚实的，故Y_1, Y_2至少一个随机，μ, η也随机

② Hash输出的碰撞.

根据生日悖论：$Pr[Succ_2] - Pr[Succ_1] \le \frac{(q_{send}+q_{exe})^2}{2\varphi(n)} + \frac{q_{oh}^2}{2^{|H|}}$

③ 去掉gcd(α,n)≠1的情况，由协议可知，gcd(α,n)≠1时，S设置Z为与口令无关的值，无论$\mathcal{A}$被动攻击还是仿冒成C, C_1者都不会影响$\mathcal{A}$的优势.

终止协议

Game$_3$：若$\mathcal{A}$幸运猜测出了认证元μ和η，即S接受，但$\mathcal{A}$未查询H_1或H_2，但μ, η的碰撞在Game$_2$排除，除非是$\mathcal{A}$自行产生的认证元被拒绝，$Pr[Succ_3] - Pr[Succ_2] \le \frac{q_{send}}{2^k}$ 合法

Game$_4$：若$\mathcal{A}$通过查询H_1或H_2得到认证元，终止协议，则只有AskAuth$_4$发生，Game$_3$, Game$_4$不可区分(即$\mathcal{A}$算出了α_1)

已知α：被动攻击，仿冒C，仿冒C. $Pr[AskAuth_4] \le q_{send}(\frac{1}{\varphi(n)} + \frac{1}{|D|})$ 归约为RSA

未知α：Z对$\mathcal{A}$来说是随机值未查询H_1，则Game$_3$, Game$_4$不可区分：$Pr[AskAuth_4] \le \frac{q_{oh}}{\varphi(n)}$.

则有：$Pr[Succ_4] - Pr[Succ_3] \le \frac{q_{oh}}{\varphi(n)} + q_{send}(\frac{1}{\varphi(n)} + \frac{1}{|D|})$.

Game$_5$ 使用私有Hash函数：μ, η, sk = $H_2(ID_i||Y_1||Y_2||Z)$.

不包含α_1, b_1, b_2，则若AskH$_5$不发生，Game$_5$和Game$_4$不可区分

AskH$_5$ → 可算α_1(在Game$_4$排除)或可解b_1, b_2.

$Pr[Succ_5] - Pr[Succ_4] \le Pr[AskH_5] \le (q_{send}+q_{exe})Adv^{rsa}(O(t))$

Game$_6$：限定到前两轮，用$\alpha = H(Y_1||Y_2||C||G)$代替$H_1$与pw无关.

则除非AskPara$_6$发生，Game$_6$和Game$_5$不可区分

$Pr[Succ_6] - Pr[Succ_5] \le Pr[AskPara_6] \le \frac{q_{oh}}{\varphi(n)}$.

又α完全与pw无关，又也有pw无关，由Game$_2$可知$Pr[Succ_6] = 0$.

综上可得$Adv(\mathcal{A})$值 $\le \frac{q_{send}}{|D|} + O(k)$