强口令认证协议的组合攻击

秦小龙, 杨义先
(北京邮电大学信息安全中心, 北京 100876)

摘 要: 基于强口令的身份认证机制是目前身份认证技术发展的一个重要方向. 本文对 IEICE 上新近提出的一个优化强口令身份认证协议 OSPA(Optimal Strong2Password Authentication)进行了分析, 并利用本文首次提出的组合攻击方法对其进行了有效攻击. 攻击结果表明该协议对凭证被窃问题、中间人攻击、重放攻击和拒绝服务攻击是脆弱的.

关键词: 身份认证; 强口令身份认证; 组合攻击
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2003) 07-1043-03

Composite Attacks on Strong2Password Authentication Protocol

QIN Xiao2long, YANG Yi2xian
(Information Security Center, Beijing Univ. Of Posts and Telecomm, Beijing 100876, China)

Abstract: The strong2password based authentication mechanism is an important development direction of authentication. In this paper we examine OSPA(Optimal Strong2Password Authentication), a recent solution to authentication, and attack it using composite attack which is put forward firstly. The results of attacks demonstrate OSPA is vulnerable to stolen2verifier, man2in2middle, replay and denial of service attacks.

Key words: authentication; strong2password authentication; composite attack

1 引言

身份认证技术是保证信息系统安全的一个重要手段. 身份认证技术一般分为三大类: (1)基于用户知道的某些秘密信息, 如口令、PIN 等进行身份认证; (2)基于用户持有某些特殊的东西, 如智能卡、USB 安全钥匙等其它身份令牌; (3) 基于用户天生具有的某些独特的生物统计特征, 如通过指印、掌型、虹膜、声音识别、脸形识别、笔迹以及打字速度等来进行身份识别.

以上三类身份认证技术各有优劣, 但相对而言, 基于口令的身份认证由于其简单有效、实用方便、费用低廉、使用灵活, 因而仍是目前最常用的身份认证技术, 尤其在分布式环境(如因特网)和移动应用领域更是被广泛使用.

基于口令的身份认证最易受到的攻击是离线口令猜测攻击, 特别是当用户选择了/ 弱口令0 时, 由于口令的熵较小, 对这种攻击就更加脆弱. 一般弱口令包含以下几种情况: (1) 选择词典(包括外语词典) 中出现的词汇作为口令. 即使这些词汇不常用, 也是不适合作为口令的; (2) 口令来源于某个人的姓名、单位或与其相关的信息. 例如把女朋友的名字、宠物的名字、计算机名或汽车牌照号码等作为口令; (3) 口令来源于用户自身的某些个人信息. 如办公室号码、电话号码、生日日期等; (4) 其它与用户名称相关的信息, 如有时人们把其姓名字母的顺序颠倒、或把某些字母改作大写作为口令; (5) 地名, 文艺作品中的人名或其它公众人物的名称等其它一些流行称谓作为口令. 与弱口令相对的是强口令, 它应满足以下原则: 应是大小写字母的混合体; 其中应有非字母的符号(如$ 、% 、& 等) 和数字; 应该方便用户记忆, 以免用户把它写下来; 至少应有 8 个字符的长度, 对一些安全性要求更高的场合, 还应采用更长的口令.

例如, 可以把两个较短的单词(如 ball 和 eye) 用/ %0 和/ &0 连接起来, 得到一个强口令/ eye%&ball0. 另外我们可以取短语/ With the Fairy hand in hand0 中每个单词的第一个字母, 再增加上数字, 得到一个强口令/ WtFhih430.

强口令的采用可以有效阻止对口令的猜测攻击.

由于强口令和弱口令的存在, 使得基于口令认证协议朝着两个方向发展. 其一是当用户选择弱口令时, 仍要保证认证的安全性. 这类研究主要是通过引入非对称密码技术和 Diffie2Hellman 密钥交换技术以抵御对口令的猜测攻击及其它攻击. 此项研究开展较广泛, 成果也不少, 其中一些协议完成了形式化证明, 具有很高的安全性. 但这类认证系统, 由于其中非对称密码算法(如 RSA) 的大量运用, 导致系统计算开销的大幅增长, 使其应用范围受到限制, 如不适合在当前引起人们极大关注的微支付系统和移动通信安全系统中使用. 基于口令认证的另一个发展方向, 是要求用户选择强口令, 以抵抗

收稿日期: 2002-02-06; 修回日期: 2002-06-08
基金项目: 国家重点基础研究发展规划项目(No.1G1999035805); 国家杰出青年基金(No.69425001); 国家自然科学基金(No.60073049)

口令猜测攻击,同时主要采用对称密码技术,在保证协议安全性的同时,使其运算、保存和传送开销尽量减少.这类协议称为强口令认证协议.目前真正安全有效的强口令认证协议还较少.近年来出现的这类协议主要有 PERM[1]、SAS[2]、OSPA[3].PREM 继承了文献[4]、[5]中介绍的一次口令认证方法,解决了其存在的哈希函数开销大和口令重置问题、以及用户端需要保存随机数的问题.但文[2]中指出 PREM 不能抵抗中间人攻击,并设计出能够抵御该攻击的 SAS.文[3]中指出 SAS 对重放攻击和拒绝服务攻击的脆弱性,并设计了具有更高安全性的 OSPA.

本文在对 OSPA 进行安全性分析的基础上,首次提出了对强口令认证协议的一种新的攻击手段,即组合攻击.然后具体设计了对 OSPA 协议的组合攻击方法.攻击结果一方面表明了 OSPA 协议对组合攻击是不安全的;另一方面也证明了组合攻击方法的有效性.当然本文的研究亦表明要实施有效的组合攻击,需要攻击者具备比实施一般攻击更多的知识,因而使这种攻击手段的使用受到一定限制.

2 对强口令认证协议的几种主要攻击

除口令猜测攻击之外,对强口令认证协议还有以下几种主要攻击手段:

Ó 中间人攻击 攻击者截获用户和认证服务器之间传送的消息,并用自己的消息替代,然后继续传送.这里攻击者在用户和服务器之间扮演着双重角色.对于用户,他是服务器;而对于服务器,他又是用户.

Ó 窃取凭证问题 在很多认证协议中,认证服务器保存着用户口令的凭证,如口令的哈希值,而不是口令明文.攻击者通过窃取口令凭证从而对系统发起攻击.

Ó 重放攻击 攻击者记录用户和服务器之间已传送的消息,然后在适当时机重新发送.

Ó 拒绝服务攻击 这主要是指认证系统因遭受攻击,而使合法用户无法得到服务器的正常认证,不能登录.

Ó 组合攻击 这个概念由本文首次提出,主要是指上述几种攻击方法可以联合使用,从而使得在单一攻击手段下安全的系统出现安全漏洞.这也是许多认证协议设计过程中往往忽视的一点.文献[3]指出 OSPA 协议能抵抗中间人攻击、凭证被窃、重放和拒绝服务攻击.本文将利用组合攻击手段说明 OSPA 实际上对这些攻击很脆弱.

3 OSPA 协议描述

为完整起见,简述文[3]中设计的 OSPA 协议如下.

3.1 符号和定义

A 为用户身份;P 为用户口令;SR 为用户登录请求;n 为正整数,每完成一次认证,自动加 1;h 为强单向哈希函数.$h(x)$ 表示 x 被哈希一次,$h^n(x)$ 表示 x 被哈希 n 次;© 位异或操作;X] Y: M 表示 X 发送消息 M 到 Y.

3.2 OSPA 协议

OSPA 协议分为注册阶段和认证阶段.新用户需要进行一次注册,然后可以进行多次认证.

3.2.1.1 注册阶段

A] S: A, $h^2(P © 1)$,用户 A 用其口令 P 计算 $h^2(P © 1)$.然后通过一个安全通道发送 A, $h^2(P © 1)$ 到服务器 S 进行注册.服务器收到用户注册消息后,保存 A, $h^2(P © 1)$ 作为口令凭证,并置 n= 1,完成用户注册.

3.2.1.2 认证阶段

注册之后,第 i(i\ 1) 次认证过程如下:

(1) A] S: A, SR 用户 A 向服务器 S 发送登录请求.

(2) S] A: n 认证服务器响应用户请求,并向用户发送用户的认证顺序号 n= i.

(3) A] S: c_1, c_2, c_3

( ) $c_1= h(P © n) © h^2(P © n)$ 用来完成当前认证.

( ) $c_2= h^2(P © (n+ 1)) © h(P © n)$ 用来更新口令凭证.

( ) $c_3= h^3(P © (n+ 1))$ 用来对( ) 进行完整性检查.

服务器收到这三个值后,进行以下操作:

(1) 判断,若 $c_1= c_2$,则认证失败,否则继续.

(2) 计算 $h(P © n)= h^2(P © n) © c_1$.这里 $h^2(P © n)$ 是服务器保存的口令凭证.

(3) 计算 $h^2(P © (n+ 1))= h(P © n) © c_2$.

(4) 判断,若 $h(h(P © n))= h^2(P © n)$ 且 $h(h^2(P © (n+ 1)))= c_3$,则认证成功,否则认证失败.这里 $h^2(P © n)$ 是服务器保存的口令凭证.

(5) 若认证成功,则服务器把保存的口令凭证 $h^2(P © n)$ 更新为 $h^2(P © (n+ 1))$,并置 n= n+ 1.

4 对 OSPA 协议的攻击

这里主要采用本文前面提出的组合攻击手段对 OSPA 进行攻击.

4.1.1 中间人攻击+ 重放攻击

在合法用户 A 的第 i(i\ 1) 次认证过程中,攻击者(中间人) 把 A 发出的消息

$c_1= h(P © n) © h^2(P © n)$

$c_2= h^2(P © (n+ 1)) © h(P © n)$

$c_3= h^3(P © (n+ 1))$

替换为:

c_1, c_2 同上, $c_3= x, x X h^3(P © (n+ 1))$

当服务器收到该消息后,确定认证失败,口令凭证保持不变.实际上攻击者修改 c_1 或 c_2 值亦可达到此目的,这里只以修改 c_3 为例.

现在,攻击者即使不知道用户 A 的口令 P,由于服务器保存的口令凭证没有更新,仍可通过重放消息:c_1、c_2、c_3.达到假冒用户 A 成功登录的目的.

4.1.2 窃取口令凭证+ 中间人攻击

假设攻击者知道 x,可以计算出 $h(x)$,那么攻击者通过窃取认证服务器保存的口令凭证,再辅以中间人攻击,则既可达到拒绝服务攻击的目的,又可使攻击者能以合法方式顺利登录.具体步骤如下:

(1) 攻击者窃取认证服务器保存的口令凭证 $h^2(P © n)$.

(2) 攻击者截获在第 i(i\ 1) 次认证过程中服务器 S 发

送给用户A 的认证顺序号n.

(3) 攻击者截获合法用户 A 在第i(i \ 1)次认证过程中发出的消息: c_1、c_2、c_3.

(4)攻击者计算 $h(P \copyright n) = h^2(P \copyright n) \copyright c_1$; 选择某一数 P_1, 计算 $h^2(P_1 \copyright (n+1))$、$h^3(P_1 \copyright (n+1))$.

(5) 攻击者向认证服务器发送消息:

$$c_1 = h(P \copyright n) \copyright h^2(P \copyright n)$$

$$\alpha_2 = h^2(P_1 \copyright (n+1)) \copyright h(P \copyright n)$$

$$\alpha_3 = h^3(P_1 \copyright (n+1))$$

(6) 认证服务器收到该消息后, 计算

$h(P \copyright n) = h^2(P \copyright n) \copyright c_1$. 这里 $h^2(P \copyright n)$ 是服务器保存的口令凭证.

$h^2(P_1 \copyright (n+1)) = \alpha_2 \copyright h(P \copyright n)$

(7) 认证服务器判断 $c_1 X \alpha_2$, $h(h(P \copyright n)) = h_2(P \copyright n)$ 且 $h(h^2(P_1 \copyright (n+1))) = \alpha_3$, 则认证成功, 并将口令凭证更新为 $h^2(P_1 \copyright (n+1))$, 置 n= n+ 1.

(8)用户 A 以后的认证请求都将失败, 因为 $h(h(P \copyright (n+1)) \copyright h^2(P \copyright (n+1)) \copyright h^2(P_1 \copyright (n+1))) X h^2(P_1 \copyright (n+1))$. 而攻击者因为知道 P_1, 则能假冒用户 A 的身份登录.

413　窃取口令凭证+ 中间人攻击+ 重放攻击

假设攻击者知道 x, 不能计算出 h(x), 那么通过这种攻击, 攻击者亦可假冒合法用户身份认证成功. 具体步骤如下:

(1) 攻击者偷听并保存合法用户 A 在第 n- i- 1, (n- i- 1\ 1)次认证过程中发出的消息: $\alpha_3 = h^3(P \copyright (n-i))$

(2) 攻击者窃取认证服务器保存的第 n- i 次认证的口令凭证 $h^2(P \copyright (n-i))$, 偷听并保存在第 n- i 次认证过程合法用户A 发出的消息:

$\alpha_1 = h(P \copyright (n-i)) \copyright h^2(P \copyright (n-i))$

$\alpha_2 = h^2(P \copyright (n-i+1)) \copyright h(P \copyright (n-i))$

$\hat{c}_3 = h^3(P \copyright (n-i+1))$

(3)攻击者窃取认证服务器保存的第 n- i+ 1 次认证的口令凭证 $h^2(P \copyright (n-i+1))$, 偷听并保存合法用户 A 在第 n- i+ 1 次认证过程中发出的消息:

$\alpha_1 = h(P \copyright (n-i+1)) \copyright h^2(P \copyright (n-i+1))$

计算并保存 $h(P \copyright (n-i+1)) = h^2(P \copyright (n-i+1)) \copyright \alpha_1$

(4)攻击者窃取认证服务器保存的第 n 次认证的口令凭证 $h^2(P \copyright n)$, 截获合法用户 A 在第 n 次认证过程中发出的消息: c_1、c_2、c_3.

(5)攻击者计算 $h(P \copyright n) = h^2(P \copyright n) \copyright c_1$, 然后向认证服务器发送消息:

$c_1 = h(P \copyright n) \copyright h^2(P \copyright n)$

$\hat{c}_2 = h^2(P \copyright (n-i)) \copyright h(P \copyright n)$

$\alpha_3 = h^3(P \copyright (n-i))$

(6) 认证服务器收到该消息后, 计算

$h(P \copyright n) = h^2(P \copyright n) \copyright c_1$. 这里 $h^2(P \copyright n)$ 是服务器保存的口令凭证.

$h^2(P \copyright (n-i)) = \hat{c}_2 \copyright h(P \copyright n)$

判断 $c_1 X \hat{c}_2$, $h(h(P \copyright n)) = h^2(P \copyright n)$ 且 $h(h^2(P \copyright (n-i))) = \alpha_3$, 则认证成功, 并将口令凭证更新为 $h^2(P \copyright (n-i))$, 置 n= n+ 1.

(7) 此后攻击者通过交替重放: α_1、α_2、$\hat{c}_3$ 和 $\alpha_1 = h(P \copyright (n-i+1)) \copyright h^2(P \copyright (n-i+1))$, $\alpha_2 = h^2(P \copyright (n-i)) \copyright h(P \copyright (n-i+1))$, $\alpha_3 = h^3(P \copyright (n-i))$.

就可以假冒用户 A 的身份登录.

5　总结

OSPA 是一种新的优化强口令认证协议[3]. 设计者曾认为它具有很高的安全性, 能有效防范凭证被窃问题、中间人攻击、重放攻击和拒绝服务攻击. 但不幸的是, 本文却发现 OSPA 的安全性并不如意.

参考文献:

[1] A Shimizu, T Horioka, H Inagaki. A password authentication method for contents communication on the internet [J]. IEICE Trans Commun, 1998, E812B(8): 1666- 1673.

[2] M Sandirigama, A Shimizu, M T Noda. Simple and secure password authentication protocol (SAS) [J]. IEICE Trans. Commun, 2000, E832B(6): 1363- 1365.

[3] C L Lin, H M Sun, T Hwang. Attacks and solutions on strong2password authentication [J]. IEICE Trans. Commun, 2001, E842B(9): 2622- 2627.

[4] A Shimizu. A dynamic password authentication method by one2way function [J]. IEICE Trans, 1990, J732D2I(7): 630- 636.

[5] N Haller. The S/KEY(TM) one2time password system [A]. Proc Internet Society Symposium on Network and Distributed System Security [C]. San Diego, USA: ISSNDSS, 1994. 151- 158.

[6] A J Menezes, P C van Oorschot, S A Vanstone. Handbook of Applied Cryptography [M]. Boca Raton, USA: CRC Press, 1997, 385- 424.

作者简介:

秦小龙　男, 1971 年生于甘肃省礼县, 现在北京邮电大学信息安全中心攻读博士学位, 主要研究方向为密码学与信息安全.

杨义先　男, 1961 年出生于四川盐亭, 现为北京邮电大学信息安全中心主任, 教授, 博士生导师, 全国政协委员, 长期从事现代密码学、信号与信息处理及网络与信息安全的研究, 在国内外著名学术期刊上发表论文 300 余篇, 出版学术专著 10 余部.