一个强口令认证协议的漏洞研究

程 英[1] 高庆德[2]
(解放军63880部队研究所 洛阳 471003)[1] (解放军外国语学院军事情报系 洛阳 471003)[2]

摘 要 研究了基于散列函数的强口令密码认证协议,分析了目前该类协议中具有较高安全性的SPAS协议。虽然协议具有较高的安全性,但是通过分析发现协议还是存在安全漏洞。存在安全缺陷的主要原因是协议中使用的密码技术过于单一。该类协议中,如果不使用其它密码技术,很难使协议达到安全。

关键词 散列函数,认证协议,SPAS协议
中图法分类号 TP391.41 **文献标识码** A

Study of the Hole of Strong Password Authentication Protocol

CHENG Ying[1] GAO Qing-de[2]
(The PLA 63880 Unite Research Center, Luoyang 471003, China)[1]
(The PLA Foreign Langue University, Luoyang 471003, China)[2]

Abstract Studied a strong password authentication protocol based on hash function, by analyzing the security of SPAS protocol among this kind of protocols. Although the SPAS is designed meticulously and regarded as more secure, but we also find some secure vulnerability in it. Using single cryptography technology induces this protocol has secure leak. At last we can prove that if this kind of protocol uses single cryptography technology, it can't produce a secure protocol.

Keywords Hash function, Authentication protocol, Strong password authentication protocol

1 引言

随着Internet的广泛使用,在网络中需要使用大量的身份认证,身份认证技术是保证信息系统安全的一个重要手段。一般实现身份认证的方法主要有以下3种方式:(1)基于用户的身体特征,例如指纹、视网膜等;(2)使用用户所拥有的可以证明身份的凭证,例如智能卡、ID卡等;(3)利用用户知道的信息,例如密码口令、PINs等。以上3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。但是,以传统的静态口令为基础的用户身份认证存在很多问题,比如无法避免网络监听、重放、字典穷举攻击等攻击方式,安全性很弱。虽然目前有很多安全的、能抵抗离线字典攻击的认证以及密钥协商协议,比如DH-EKE,SPEKE,SRP,AMP等,但它们都是基于计算量大的公钥算法,无法应用到如PDA、手机等计算能力弱的用户终端设备中。随着移动设备的日益广泛使用,对于安全、轻量的基于口令的认证协议的需求也逐渐加强。

Halevi和Krawczyk证明了为抵抗离线字典攻击,口令认证协议必须使用公钥技术。因此,为更有效地抵抗离线字典攻击但又不使用公钥技术,在设计的协议中要求用户选择使用强口令认证。所谓强口令是指具有较高信息熵的不容易猜测的用户口令字。目前没有通用的标准规定强口令的构成,但微软公司指定了一套强口令的评判依据,比如:(1)至少有7个字符的长度;(2)不包含用户名字、用户名或单位名称;(3)不包含字典中有的单词;(4)与以前使用的口令不同;(5)必须包含大小写、数字和键盘中的符号。

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Diffle-Hellman密钥交换技术来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,由于其中大量运用非对称密码算法(如RSA),导致系统计算开销大幅增长,使其应用范围受到限制,不适合使用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。

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,SAS,OSPA。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。但文献[2]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

到稿日期:2008-12-03 返修日期:2009-02-13 本文受国家863项目(2007AA01Z2a1)资助。
程 英(1970-),女,高级工程师,硕士生导师,研究方向为计算机网络与信息安全,E-mail:cychh2002@yahoo.com.cn;高庆德(1970-),男,博士,研究方向为情报分析、信息安全。

献[3]指出，SAS对重放攻击和拒绝服务攻击是脆弱的，并设计了具有更高安全性的OSPA。但是文献[3]对其进行了有效的攻击，发现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。为了克服OSPA存在的安全缺陷，文献[1]给出了一个安全性更高的SPAS。本文分析了该协议的安全性，发现该协议仅仅使用了hash和模2加运算，因而导致了攻击者只要获得此通信中使用过的$h^2(S||P||N_j)$或$h(S||P||N_i)$这个杂凑值，就可以成功地对协议发起中间人进行攻击。

2 SPAS方案概述与分析

2.1 SPAS方案概述

在文献[1]中给出了一种安全高效的强口令认证协议(SPAS)。SPAS由两个阶段构成：用户注册阶段和用户认证阶段。原方案的具体描述如下。

(1) 用户注册阶段

Step1 用户A通过安全通道向服务器S注册，由S选择第1个随机数N_1，发送给用户，然后用户计算$V_1=h^2(S||P||N_1)$，并存储；

Step2 服务器选择服务器端的安全密钥K用于加强服务器端口令验证因子的安全性，并将K保存在一个安全的地方，然后计算$SV_1=V_1\oplus K$，其中$K_A=H(A||k)$。最后S把$\{IDA,SV_l,N_1\}$保存在口令验证库中，用户注册过程结束。

(2) 用户认证阶段

用户认证协议的符号描述：

Mes1：$A\rightarrow S$：N_A，ID_A，Req；

Mes2：$S\rightarrow A$：N_i，$N_{i+1}\oplus h(h^2(S||P||N_i)||N_A)$；

Mes3：$A\rightarrow S$：d_1，d_2，d_3；

Mes4：$S\rightarrow A$：$h(N_A||N_{i+1}||h(S||P||N_i))$，$Res$；

用户认证协议的详细描述：

Step1 用户A第i次登录时，A产生一个随机数N_A，并将其与ID_A和登录请求Req一起发送到S，要求认证并建立连接；

Step2 S接收到A的认证请求后，从口令验证库中读取该用户对应的SV_1，通过计算$SV_1\oplus H(A||K)$得到$h^2(S||P||N_i)$，然后产生一个随机数N_{i+1}并发送Mes2的信息；

Step3 当A收到Mes2信息后，A输入口令P并计算$h^2(S||P||N_i)$，接着计算$h(h^2(S||P||N_i)||N_A)$，并由此获得服务器端产生的$N_{i+1}=N_{i+1}\oplus h(h^2(S||P||N_i)||N_A)\oplus h(h^2(S||P||N_i)||N_A)$。如果$N_i\neq N_{i+1}$成立，则$A$按照如下公式计算并发送$d_l$，$d_2$，$d_3$：

$d_1=h^2(S||P||N_i)\oplus h(S||P||N_i)$；

$d_2=h(S||P||N_i)\oplus h^2(S||P||N_{i+1})$；

$d_3=h(h^2(S||P||N_{i+1})||N_i||N_{i+1})$。

Step4 在接收到Mes3信息后，S计算$y_1=d_l\oplus h^2(S||P||N_i)$并验证$h(y_1)=h(S||P||N_i)$是否成立。如果成立，则$S$认为该用户是合法用户，然后服务器计算$y_2=d_2\oplus y_l=h^2(S||P||N_{i+1})$，$y_3=h(y_2||N_i||N_{i+1})$，并验证$y_3=d_3$是否成立。如果成立，则服务器端将原来的记录$\{ID_A,SV_i,N_i\}$替换成$\{ID_A,SV_{i+1},N_{i+1}\}$，其中$SV_{i+1}=h(A||K)\oplus y_2$。然后把$h(N_A||N_{i+1}||h(S||P||N_i))$和认证是否成功的结果Res发送给$A$来完成服务器对用户的认证。

Step5 A在接收到服务器端发送的Mes4信息之后，验证该值是否正确，以确保没有攻击者假冒服务器的攻击存在。

2.2 SPAS方案的安全性分析

通过对原方案的分析，发现由于该方案要想实现安全认证就必须保证参数$h^2(S||P||N_i)$是保密的。但是该参数又是极易获取的，只要攻击者获得了协议某次运行时使用过的$h^2(S||P||N_j)$或$h(S||P||N_j)(j<i)$，他就可以通过记录的用户认证信息来冒充该用户和服务器进行认证。也就是说，攻击者只要采用离线攻击，可以获得这些消息。具体攻击如下。

假设攻击者获得了协议某次运行时使用过的$h^2(S||P||N_j)(j<i)$，并且保存有用户A所有的通信记录，那么攻击者就可以从用户第j次通信记录Mes3中的信息进行如下计算：$d_{1j}\oplus h^2(S||P||N_j)=h(S||P||N_j)$，$d_{2j}\oplus h(S||P||N_j)=h^2(S||P||N_{j+1})$。依此类推，攻击者通过用户的第$j+1$次到第$i-1$次通信记录进行如上的运算，就可以获得现在服务器端保存的用户记录$h^2(S||P||N_i)$和$h(S||P||N_i)$，此时攻击者就可以发起冒充用户A的攻击。攻击过程符号描述如下：

Mes1：$I/A\rightarrow S$：N_A，ID_A，Req；

Mes2：$S\rightarrow I/A$：N_i，$N_{i+1}\oplus h(h^2(S||P||N_i)||N_A)$；

Mes3：$I/A\rightarrow S$：d_1，d_2，d_3；

Mes4：$S\rightarrow I/A$：$h(N_A||N_{i+1}||h(S||P||N_i))$，$Res$；

其中I/A表示攻击者I冒充用户A。

攻击的具体描述如下：

Step1 攻击者冒充用户A进行第i次登录，产生一个随机数N_A，并将其与ID_A和登录请求Req一起发送到S，要求认证并建立连接；

Step2 S接收到认证请求后，按照协议的既定步骤进行操作；

Step3 攻击者收到Mes2信息后，由于拥有$h^2(S||P||N_i)$，因此可以计算$h(h^2(S||P||N_i)||N_A)$，并由此获得服务器端产生的$N_{i+1}=N_{i+1}\oplus h(h^2(S||P||N_i)||N_A)\oplus h(h^2(S||P||N_i)||N_A)$，按照如下公式计算并发送$d_1$，$d_2$，$d_3$：$d_1=h^2(S||P||N_i)\oplus h(S||P||N_i)$，$d_2=h(S||P||N_i)\oplus R$，$d_3=h(R||N_i||N_{i+1})$。攻击者因为不知道用户$A$的口令$P$，所以无法计算$h^2(S||P||N_{i+1})$。但是由于服务器也无法计算$h^2(S||P||N_{i+1})$，因此攻击者只需随机选取一个满足hash函数输出长度的随机数R即可。

Step4 显然通过上面的计算发送过来的d_1，d_2，d_3是可以通过服务器认证的，此时服务器计算得到R，认为该值为$h^2(S||P||N_{i+1})$，并将原来的记录$\{ID_A,SV_i,N_i\}$替换成$\{ID_A,SV_{i+1},N_{i+1}\}$，其中$SV_{i+1}=h(A||K)\oplus R$。然后把$h(N_A||N_{i+1}||h(S||P||N_i))$和认证是否成功的结果$Res$发送给$A$来完成服务器对用户的认证。

Step5 攻击者收到确认信息后成功地冒充A，从而通过了认证。

一旦上面的攻击成功，那么合法用户就再也无法通过服务器的认证，要想再次登录就必须重新进行系统的初始化。

3 存在安全漏洞的原因分析

3.1 方案被攻击的原因

通过2.2节的攻击发现，造成攻击的主要原因是以下两

(下转第116页)

线域更改为“是”。

以上3个阶段是针对控制系统网络配置过程而言，在各个阶段进行切换不影响上层控制系统的运行。因为在各个阶段之间切换只是为新接入节点分配IP地址，控制系统的原有节点在各阶段切换过程中其IP地址会保持不变。在系统正常运行时，对于由于节点掉电等原因引起短暂故障的节点，p_DHCP能够确保在故障排除后保留其原有IP，保证其逻辑位置信息正确绑定。网络配置3个阶段状态转换如图3所示。

2.3 p_DHCP与DHCP的对比分析

如上所述，DHCP由传输协议和网络地址分配机制两部分组成。传输协议用于将网络配置参数由DHCP服务器传递到网络上的客户机，地址分配机制为网络上的客户机分配网络地址。P_DHCP协议完整继承DHCP的传输协议，即继承了DHCP的所有消息类型和消息格式以及客户机与服务器交互过程，具体化了地址分配机制。

P_DHCP根据工业以太网控制系统节点逻辑位置信息自动绑定的需要具体化了地址分配机制，将网络配置过程明确划分为节点接入准备和节点接入两个阶段。网络配置完成后，系统进入正常运行阶段。在节点接入准备阶段和系统正常运行阶段，p_DHCP与DHCP完全相同，只是具体化了地址分配机制。服务器收到客户端发来的DHCPDISCOVERY消息后根据CFG_STAT表中的登记分配IP地址。而在节点接入阶段与DHCP不同之处在于，DHCP针对每个DHCPDISCOVERY消息进行响应，以为客户机分配IP地址；而p_DHCP需等待Max_T时间，以收集DHCPDISCOVERY消息，根据MAC地址的大小顺序进行IP地址分配。配合现场维护人员在接入设备时遵循的有关规定，实现节点逻辑位置信息自动绑定。

结束语 本文在DHCP基础上提出p_DHCP协议。P_DHCP协议完整继承了DHCP的传输协议，具体化了DHCP的地址分配机制，实现工业以太网控制系统中节点逻辑位置信息的自动绑定。p_DHCP需要得到现场维护人员的配合。一次更换多个同种类型的节点时，要保证节点MAC地址和节点接入点编号有相同的顺序，即较小的MAC地址接入编号较小的接入点，较大的MAC地址接入编号较大的接入点。p_DHCP在实现节点逻辑位置信息自动绑定的前提下，尽量减少对DHCP协议的修改。p_DHCP与DHCP的客户端完全一致，服务器端也只是在步骤(2)上有一个小的变动，协议实现起来较为容易，不需要修改现有的客户端网络节点。

参 考 文 献

[1] 王平，谢昊飞，向敏，等. 工业以太网技术[M]. 北京：科学出版社，2007

[2] 冯冬芹，黄文君. 工业通信网络与系统集成[M]. 北京：科学出版社，2005

[3] 阳宪惠. 工业数据通信与控制网络[M]. 北京：清华大学出版社，2002

[4] Droms R. Dynamic Host Configuration Protocol[S]. RFC1541. Bucknell University, October 1993

[5] Alexander S, Droms R. DHCP Options and BOOTP Vendor Extensions, RFC 1533. Lachman Technology, Inc., Bucknell University, October 1993

(上接第107页)

个方面：

(1) 协议的安全性主要是通过进行hash函数运算和模2加运算来保证的。但是模2加运算计算简单，这就导致了一旦进行模2加法运算的某些值泄漏，就会导致整个协议被攻击。

(2) 协议为了增加对口令的保护，服务器也不知道用户的口令，所以当用户传送过来计算 $h^2(S||P||N_{i+1})$ 时，服务器也不知道该值是否正确，无法对该信息的正确性进行验证。

3.2 漏洞改进的方法

上节已经分析了协议能够被攻击的原因，本节探讨如何修改协议，使其成为一个安全的密码协议。

协议能够被攻击的第一个原因是模2加运算简单。也就是说，当 $M=M_1 \oplus M_2$ 时，在已知 M 的前提下只要知道 M_1 (或 M_2)就可以通过对 M 模2加法运算求出 M_2 (或 M_1)，那么要克服这个缺陷，可以采取以下两种策略：①加强对信息 M_1，M_2 的保密，增强其机密性；②增加计算的复杂性，即类似 $M=M_1 \oplus M_2 \oplus M_3$。这样，攻击者要想获得 M_1，M_2，M_3 中某个机密信息，就必须先获得其中的另外两条信息，从而增加攻击的难度。

协议能够被攻击的第二个原因是服务器方无法对信息 $h^2(S||P||N_{i+1})$ 的正确性进行判断。要克服这个缺点，可以采用以下两种策略：①让服务器知道用户的密码，这样服务器也能生成 $h^2(S||P||N_{i+1})$，自然也就能验证该信息的正确性；②采用公钥密码技术，让用户对 $h^2(S||P||N_{i+1})$ 连同一个新鲜因子一起进行数字签名，从而保证信息来源的真实性，再通过新鲜因子的新鲜性来保证整条签名信息的新鲜性；③采用对称密码技术，用服务器与用户的预共享对称密钥来加密关键信息。

结束语 本文研究了基于散列函数的强口令密码认证协议，分析了目前该类协议中具有较高安全性的SPAS协议。通过分析，发现协议存在安全漏洞。产生安全缺陷的主要原因，是协议中使用的密码技术过于单一。在具体使用过程中，为了达到安全要求，必须综合使用其他密码技术。

参 考 文 献

[1] 虞淑瑶、叶润国，等. 一种安全高效的强口令认证协议[J]. 计算机工程，2006，32(6)：146-147

[2] 泰小龙，杨义先. 强口令认证协议的组合攻击[J]. 电子学报，2003，32(7)：1043-1045

[3] 李莉，薛锐，等. 基于口令认证的密钥交换协议的安全性分析[J]. 电子学报，2005，33(1)：166-170

[4] 陈开渠. 基于口令的认证：协议和应用[D]. 北京：中国科学院软件研究所，2000

[5] Halevi S, Krawczyk H. Public-key Cryptography and Password Protocols[C]// Proceedings 5th ACM Conference on Computer and Communications Security. San Francisco, CA, 1998：122-131

[6] Ku W C, Chen S M. Weaknesses and improvements of an efficient password base remote user authentication scheme using smart cards [J]. IEEE Transactions on Consumer Electronics, 2004, 50(1)：204-206