文章编号:1001 - 9081(2006)02 - 0343 - 03

网络存储环境下基于 RADIUS 的 DH-CHAP 方案

刘祥涛
(武汉科技大学 理学院, 湖北 武汉 430081)
(fansy98@163.com)

摘 要:针对现存网络存储系统安全的脆弱性,基于强安全性、高灵活性、可扩展性好的设计思想,设计了一个基于远程拨号用户认证服务(Remote Authentication Dial In User Service,RADIUS)的 DH 挑战握手认证协议(Diffie Hellman Challenge Handshake Authentication Protoco,DH-CHAP)身份认证方案,为数据保护的框架结构提供了授权、机密性与完整性保护的基础。

关键词:远程拨号用户认证服务; 身份认证; Diffie Hellman 挑战握手认证协议
中图分类号: TP309 **文献标识码**:A

DH-CHAP project based on RADIUS for network storage

LIU Xiang-tao
(*College of Sciences, Wuhan University of Science & Technology, Wuhan Hubei* 430081, *China*)

Abstract: Network storage technology is one of the hottest technology in recent several years. Network storage has changed the way enterprises manage their storage environments. It is crucial to safeguard data, regardless of whether it is retained at-rest inside storage systems, or in-flight across the storage network, LAN, or WAN. Aiming at the frangibility of exsiting network storage system and on the basis of the design ideas of strong security, high agility and fine scalability, a DH-CHAP authentication project based on RADIUS was designed, it offered a foundation to authorization, confidentiality and integrality for the architecture of data security.

Key words: RADIUS (Remote Authentication Dial In User Service); authentication; DH-CHAP (Diffie Hellman Challenge Handshake Authentication Protocol)

0 引言

网络存储象其他数据网络一样,存在很多安全威胁,比如:冒名欺骗、非授权的访问、数据偷窃、拒绝服务攻击等。而存储网络本身存在很多弱点:不合理的配置、FC 协议栈与 TCP/IP 的结构相似性而引发的一系列弱点,WWN(World Wide Name)的易修改性等。而一个信息系统的风险 = 弱点 × 威胁 × 系统的价值,在威胁无法减少(总存在很多谋取非法利益的黑客)以及信息系统价值不断增加(因为信息的不断增加,企业一般都有不断扩充存储系统的需求)的情况下,减少信息系统风险的方法只有针对相应的威胁建立一定的安全机制来设法减少系统的弱点。针对冒名欺骗,可以建立对应的身份认证机制;针对非授权的访问可以用访问控制表的形式建立授权机制;针对数据偷窃,可以采取加密的方法满足要求;针对拒绝服务攻击,可以采用数据备份、冗余系统的方法来减少其威胁[1]。

1 存储网络的安全体系结构

在存储网络的环境下,要确保一个系统的安全,必须有一个完整的安全体系结构,见表 1,一般包含如下组件:身份认证基础设施、身份认证机制、授权机制、完整性服务、机密性服务。在此安全体系结构中,下层为相应的上层提供了基本服务,本文主要针对第 1、2 层设计一个身份认证方案。

在现存的信息系统中,有三种不同的身份认证基础设施:基于对称密钥、基于证书和基于密码。对基于对称密钥的身份认证基础设施,有两种分发与管理密钥的方法:

1)分布式分发,即系统中需要认证的实体都保存其他实体的密钥,这样的话系统中需要管理的密钥数 $x = (n^2 - n)/2$(n 为实体数),而且当系统中每加入一个新的实体时,要给新实体配置与其他实体所共享的新密钥,且要对所有其他实体的密钥加入一个新的密钥条目,所以这种基础设施的可扩充性很差。

表 1 存储网络的安全体系结构

第 5 层	机密性服务
第 4 层	完整性服务
第 3 层	授权机制
第 2 层	身份认证机制
第 1 层	身份认证基础设施

2)集中式分发,即用一个专门的服务器(例如本方案中采用的 RADIUS 服务器)保存所有实体的密钥,这样的话系统中需要管理的密钥数 $x = n$,而每个实体仅保存与服务器对应的密钥,新加入实体时,只需要在服务器和新实体中加入一个新的密钥条目,其他实体不用变化,故其可扩充性好。而且分发和管理密钥也相当方便。现存的可在对称密钥的身份认证基础设施上建立的身份认证机制有挑战握手协议(Challenge Handshake Authentication Protocol,CHAP)和 DH 挑战握手协议[2](Diffie-Hellman Challenge Handshake

收稿日期:2005 - 08 - 10;**修订日期**:2005 - 10 - 27
作者简介:刘祥涛(1977 -),男,湖南涟源人,助教,硕士研究生,主要研究方向:存储系统安全.

Authentication Protocol,DH-CHAP)。

基于证书的身份认证基础设施是在系统设置一个认证中心(CA),管理证书的发放和验证。在此基础上,现存的身份认证机制有 FCAP(Fibre Channel Authentication Protocol)。而基于密码的身份认证基础设施是基于零知识证明原理的一个基础设施,每个实体保存自己独有的密码和对方的盐(salt)。和基于对称密钥的身份认证基础设施有很多相似之处,不过因为应用了零知识证明原理,故其安全性得到了进一步的保证。在此基础设施上,现存的身份认证机制有 SRP (Secure Remote Password Protocol)[3] 和 FCPAP(Fibre Channel Password Authentication Protocol)。

2 基于 RADIUS 的 DH-CHAP 方案

2.1 方案配置模型

本方案的配置模型如图 1 所示,RADIUS 服务器保存所有与需要认证的设备对应的用户名和密钥,每台设备(服务器、存储阵列、FC 交换机、网关/路由器等)保存一个自己与 RADIUS 服务器的对称密钥,通过管理平台可以配置 RADIUS 服务器,可以很方便的分发和更新密钥。

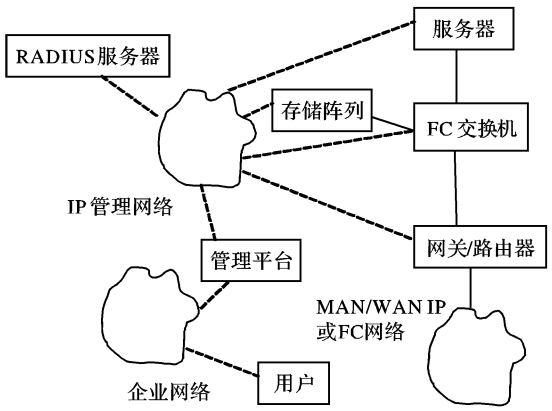

图 1 方案配置模型

2.2 RADIUS[4] 协议简介

RADIUS 定义了在 NAS (Network Access Server) 和集中存放认证信息的 RADIUS 服务器之间传输认证、授权和配置信息的协议。RADIUS 以 Client/Server 模式工作,实现了对远程拨号用户的身份认证、授权和计费功能。RADIUS 是一种基于 UDP 协议的上层协议,RADIUS 信息包被封装为 UDP 数据包, RADIUS 数据包在认证系统的客户/服务器之间传送,RADIUS 认证的 UDP 数据包的目标端口地址是 1812。

标准的 RADIUS 数据包的结构包括 Code、ID、Length、Authenticator 和 Attributes 几部分,如表 2 所示。

表 2 RADIUS 数据包格式

Field	Size (Bytes)
Code	1
Identifier	1
Length	2
Authenticator	16
Attributes	n

1) Code:代码域,长度为一个字节,用来区分 RADIUS 包的类型,如果收到的包含有无效的 Code 值,则将该包丢弃。Code 值 1,2,3 用于用户认证。Code = 1 时,为访问请求包,Code = 2 时,为访问响应包,Code = 3 时,为访问拒绝包。

2) Identifier:标识符域,一个字节,用于区分不同的请求以便给予相应的应答。

3) Length:长度域,二个字节(20 ≤ Length ≤ 4096),用来表示整个 RADIUS 包的总长度,包括 Code、Identifier、Length、Authenticator 和 Attributes 五个数据域的长度总和。其中 Code、Identifier、Length、Authenticator 为定长,Attributes 为变长,超出范围的数据将视为附加数据(Padding)或直接忽略。

4) Authenticator:认证标识符域,16 个字节,在本设计方案中没有用上,设为 0。

5) Attributes:属性域,指定 RADIUS 包中的具体内容,可以为 RADIUS 请求或应答传递详细的认证、授权信息或配置细节等。每个 Attributes 又分为 3 个部分:Type、Length 和 Value。

a) Type: 一个字节,表示 Attribute 的类型,可以取 1 ~ 63。每个 RADIUS 数据包只包含必须的属性,没有必要使用全部属性,本方案要用到的属性类型有 3 个:Type = 1 时,为用户名属性,Type = 3 时,为 CHAP 密码属性;Type = 60 时为 CHAP 挑战属性。

b) Length: 一个字节,表示属性的长度,计算方法为:Type + Length + Value。

c) Value:零字节或多字节,表示属性的具体值。

2.3 基于 RADIUS 的 DH-CHAP 认证过程

本方案中,假设 B 要认证 A,认证发起者 A(被认证方) 被看做是请求服务的用户,认证响应者 B (认证方) 可以看成是网络访问服务器(NAS)或者是 RADIUS 服务器 S 的客户。如果要进行双向认证,则他们的角色互换。

从 RADIUS 客户即 B 的角度看,它会构造一个访问请求包,其包含 3 个属性:用户名属性(类型 1)、CHAP 密码属性(类型 3)和 CHAP 挑战属性(类型 60)。用户名属性被用于传递用户的名字,本方案中名字格式采用 UTF-8[5] (Unicode Transformation Format-8)格式,S 用它来检索与用户对应的密钥。CHAP 密码属性用于发送 A 发来的对应挑战的响应值。CHAP 挑战属性用于发送 B 原来发送给 A 的挑战信息。当从 A 接收到 DH-CHAP 回答时, B 马上给 S 发送访问请求包。

本认证方案要用的数学符号如表 3 所示。

表 3 认证的数学符号

符号	描述
S	RADIUS 服务器
A	认证发起者 (即 RADIUS 用户)
B	认证响应者 (即 RADIUS 客户)
A_R, B_R	实体 A、B 采用 UTF-8 格式的用户名属性
C_1, C_2	DH-CHAP 消息的挑战值,用于 RADIUS CHAP 挑战属性
C_{a1}	扩充的挑战值
R_1, R_2	DH-CHAP 消息的响应值,用于 RADIUS CHAP 密码属性
R'_1, R'_2	Radius 服务器计算的用于认证的响应值
T_i	DH-CHAP 消息的事务 id 最小字节
K_A, K_B	用于 DH-CHAP 认证的管理员配置的密码
x, y	B, A 选择的随机数
H	Hash 函数(e. g. MD5, SHA-1…)
g, p	对应 DH 群的生成子和模数
‖	连接符号

基于 RADIUS 的 DH-CHAP 身份认证过程(如图 2 所示)如下:

1) A 向 B 发送认证协商消息,其中包括 A_R, DHCHAP 协议代号,供 B 选择的 Hash 函数列表(MD5,SHA - 1…),DH

群标识符列表,本次交易的交易标识符 T_ID。

2) B 从列表中选择双方所支持的 Hash 函数和 DH 群标识符,产生随机数 x 和挑战数 C_1,B 计算 $g^x \bmod p$,然后向 B 发送 DHCHAP 挑战消息,消息中包含 B_R,B 所选择的 Hash 函数和 DH 群标识符, C_1, $g^x mod\ p$。

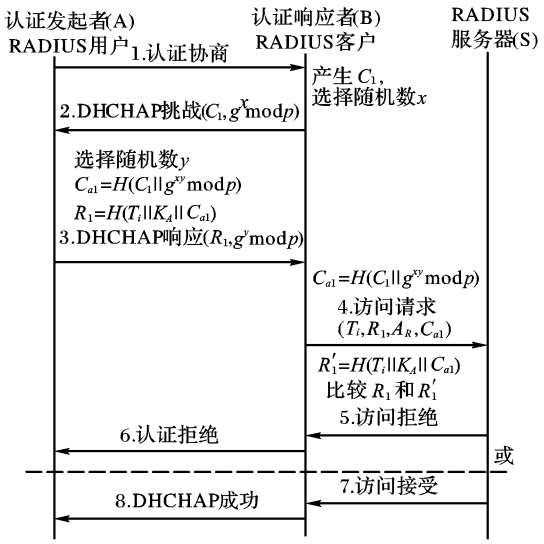

图2　基于 RADIUS 的 DH-CHAP 身份认证过程

3) A 选择随机数 y, 计算 $K_s = H(g^{xy} \bmod p)$ 用于若验证成功后,与 B 共享的一次性会话密钥值,$C_{a1} = H(C_1 \| g^{xy} \bmod p)$, $R_1 = H(T_i \| K_A \| C_{a1})$。产生 DHCHAP 响应消息,其中包括 R_1,$g^y \bmod p$,如果要进行双向认证,即 A 也想认证 B,则 A 必须选择挑战值 $C_2 (\neq C_1)$ 加入响应消息中。

4) B 为了认证 A,向 RADIUS 服务器 S 发送访问请求消息,其中包括 T_i,R_1,A_R,C_{a1}。

5) S 根据 A_R 检索对应的 K_A, 计算 $R_1' = H(T_i \| K_A \| C_{a1})$,并比较 R_1 是否等于 R_1',如果 $R_1 \neq R_1'$,则 S 向 B 发送访问拒绝消息。

6) B 向 A 发送认证拒绝,断开连接。

7) 如果 $R_1 = R_1'$,则 S 向 B 发送访问接受消息。

8) B 向 A 发送 DHCHAP 成功消息,同时计算与 A 的共享密钥 $K_s = H(g^{xy} \bmod p)$。若 A 要求了双向认证,则 B 要重复 A 的动作,计算与 C_2 对应的 C_{a2}、R_2,并在 DHCHAP 成功消息中加入 R_2。此后,A 与 B 的角色将对调,A 将向 S 发送访问请求消息来认证 B。

3　结语

由方案的配置模型和身份认证过程可知,本认证方案具有如下优点:

1) 与无 DH 算法的基于 RADIUS 的 CHAP 身份认证机制是完全兼容的,因为 RADIUS 服务器的操作过程没有变化,这样保证了软件的前向兼容性。

2) DH 算法和随机数 x,y 的加入加强了认证的强度,且能阻止 CHAP 认证情况下的反射攻击,保证了方案的强安全性。

3) 在认证后将产生一个 A、B 双方共享的一次性会话密钥 K_s,可为此次会话后续的数据提供保密性服务。

4) 可以有选择性的提供单向认证或者双向认证,这使方案具有高灵活性。

5) RADIUS 服务器的使用为管理、分发、更新密钥提供方便以及使方案具有良好的可扩充性。

本方案的不足:可能会遭受分布式拒绝服务攻击(DDoS),但是因为 SAN 的特殊性,一般认证都是建立在端口登陆基础上的,所以遭受大规模的 DDoS 是不可能的,但是也不能忽视此威胁的存在。希望在后续方案中能加入一定的机制来避免此类攻击。

总之,本文采用建模和协议流分析的设计方法,设计了一个强安全性、高灵活性、可扩展性好的身份认证方案,为网络存储环境下的数据保护框架结构提供了授权,机密性与完整性保护的基础。

参考文献:

[1] GRUENER J, KOVAR M. The Emerging Storage Security Challenge [EB/OL]. http://www.yankeegroup.com, 2003-09/2005-06.

[2] INCITS T11. FIBRE CHANNEL SECURITY PROTOCOLS(FC-SP) REV 1.71[EB/OL]. http://www.t11.org/ftp/t11/pub/fc/sp/05-163v1.pdf, 2005-03/2005-06.

[3] WU T. The SRP Authentication and Key Exchange System (RFC 2945) [EB/OL]. http://www.apps.ietf.org/rfc/rfc2945.html, 2000-09/2005-07.

[4] RLGNEY C. Remote Authentication Dial In User Service (RFC 2865) [EB/OL]. http://www.ietf.org/rfc/rfc2865.txt, 2000-06/2005-06.

[5] YERGEAU F. UTF-8 a transformation format of ISO 10646(RFC 3629) [EB/OL]. http://www.apps.ietf.org/rfc/rfc3629.html, 2003-11/2005-07.

(上接第 342 页)

查找,并在找到之后返回这个 Engine 的实例。

这样,用户就可以调用 Remove 和 Put 方法在运行时刻替换一个 CSP 所提供的服务的实现方法,并用 GetSpiInstance 方法得到新替换的实现 Engine 的对象。

在整个安全构件中,CSP 的动态管理与 Engine 的动态管理功能,实现了安全构件的可定制特性。

3　结语

本文首先提出了在系统中实现用户可定制的安全性的一种构想,接着以“和欣”操作系统为基础,论述了利用构件技术在“和欣”操作系统上实现可定制的安全构件的方法。此外,按照这个思路设计的安全构件还有着跨平台的特性,因此能够将其应用于不同的操作系统中。

参考文献:

[1] 陈榕. 中间件技术在嵌入式操作系统中的应用[DB/OL]. 万方数据资源系统.

[2] KOOPMAN E. Embedded system security[J/OL]. IEEE Computer Society documents online, 2004.

[3] RAGHUNATHAN A, RAVI S, HATTANGADY S, *et al*. Securing Mobile Appliances——New Challenges for the System Designer [J/OL]. IEEE Computer Society documents online, 2003.

[4] KAN X. Encryption and Decryption: Software protection technique and complete resolvent [M]. 北京: 电子工业出版社, 2001.