网络服务系统统一身份认证模型的研究与设计

郝 辉 钱华林

(中国科学院计算机网络信息中心 中国科学院研究生院 北京 100080)

摘 要 Internet上服务的增多带来了用户信息管理的各种问题,每个服务商都要维护庞大的用户信息库;用户也要重复提供认证信息以使用不同的服务。本文提出了一个统一身份认证模型,可以实现安全、可靠、高效的用户身份认证。文章先给出设计此身份认证模型的必要性,介绍并分析了当前流行的身份认证机制的特点和性能,然后提出了此统一身份认证模型的结构,并对其能实现的功能做了介绍,最后给出了一个安全、高效的身份认证算法和一个可靠、严谨的身份联合算法。

关键词 统一身份认证,RADIUS,CA,Web服务

The Study and Design of Universal Identity Authentication Model of Internet Service System

HAO Hui QIAN Hua-Lin

(Computer Network Information Center, Chinese Academy of Sciences, Graduate School of the Chinese Academy of Sciences, Beijing 100080)

Abstract The ever increasing Internet applications bring many problems of managing user information. Every service provider must maintain a large information database, and users must provide different evidences for different services. This paper proposes a universal model for authentication. The model can achieve the goal of providing a secure, reliable, efficient authentication. At first, the article gives the necessity of the model, and analyses the features and capability of some popular mechanisms of authentication. And then it proposes the structure of the universal model, introduces some functions it can accomplish. At last, a secure, efficient authentication algorithm and a reliable, closeknit identity alliance algorithm are proposed.

Keywords Universal identity authentication, RADIUS, CA, Web services

1 引言

随着网络安全技术和Web Services的发展进步,一些对安全性能要求比较高,以往只能在非网络环境下的服务也应用到Internet上来,如电子商务、电子政务、电子银行、电子购物等等;另一方面,许多公司、企业及高校的网络环境下都建立了多个信息系统,为企业内部的员工或高校的学生提供多种服务。如办公自动化系统、综合信息系统、综合教务管理系统、网上学术沙龙、选课系统、网络课堂等。今后还会不断增加新的应用系统,用户数量也会不断增加。

这样就带来了两方面的问题,一是上网的信息资源越多,受黑客攻击的可能性越大(尤其是一些敏感数据);二是涉及安全和协同方面的服务都对使用服务的用户身份认证有着各种各样的要求,不同身份的用户享受的服务级别和种类也不同。很多服务性质的网站各自拥有自己一批用户群,并且这些网站使用各自所独有的用户身份标识,网站之间不能实现用户信息的共享。相应地,每个用户在不同的服务网站又会有着不同的标识。用户在新登录一个服务的时候,往往要输入与其他网站类似或者重复的用户身份信息。这些用户信息在各个网站成为孤立的信息孤岛,不能相互沟通,造成不必要的资源浪费,也给用户使用服务带来诸多不便。

如何在Internet上实现统一、可靠的个人身份标识,成为一项亟待解决的任务。在提供身份认证的服务基础之上,可以进行商业的联盟(Alliance)合作,实现单点登录(Single Sign-On),以及提供更多更丰富的方便用户使用的新服务。

本文将分析研究一个安全可靠的网络应用服务统一身份认证模型,目的就是要解决不同的网络应用系统和服务对用户身份认证不统一以及因此而产生的安全问题。

2 常用认证技术分析

对于一些计算机资源,只有经过授权的合法用户才能访问,而如何正确鉴别用户的真实身份是问题的关键。用户认证,也称为用户鉴别,就是用户向服务系统以一种安全的方式提交自己的身份证明,由服务系统确认用户的身份是否真实。

一般而言,认证的机制分为两类:简单认证机制和强认证机制。

简单的认证中只有名字和口令被服务系统所接受。由于明文的密码在网上传输极容易被窃听截取,一般的解决办法是使用一次性口令(OTP,One-Time Password)机制。这种机制的最大优势是无须在网上传输用户的真实口令,并且由于具有一次性的特点,可以有效防止重放攻击(Replay Attack)。根据一次性口令生成机制的不同,通常OTP可分为:Time Synchronization的Secure ID(安全标志符),Challenge-Response的Crypto Card(密码卡)和增强的S/Key(安全密钥)等。RADIUS协议就是属于这种类型的认证协议。

强认证机制一般将运用多种加密手段来保护认证过程中

郝 辉 硕士,主要研究方向为计算机网络与通信,计算机网络系统,互联网寻址技术。钱华林 研究员,博士生导师,中科院计算机网络信息中心总工,计算机软件与理论专业,研究方向为计算机网络、网络工程和网络运行服务。

相互交换的信息，其中，Kerberos 协议是此类认证协议中比较完善、较具优势的协议，得到了广泛的应用。Kerberos 协议的基础是基于信任第三方，用户需要向服务系统提供身份证明时，首先需要向认证服务器(AS, Authentication Server)验证自己身份，通过后用户将会获得一张票据(Ticket)，并提交给票据许可服务器(TGS, Ticket Granting Server)确认有效，并经过服务器和客户之间的相互认证后，才可以使用服务系统提供的服务。Kerberos 协议具有以下的一些优势：

(1)与授权机制相结合；

(2)实现了一次性签放的机制，并且签放的票据都有一个有效期；

(3)支持双向的身份认证，即服务器可以通过身份认证确认客户方的身份，而客户如果需要也可以反向认证服务方的身份；

(4) 支持分布式网络环境下的认证机制，通过交换“跨域密钥”来实现。

Kerberos 机制的实现要求一个时钟基本同步的环境，这样需要引入时间同步机制，并且该机制也需要考虑安全性，否则攻击者可以通过调节某主机的时间实施重放攻击。

另一种强认证机制是基于公共密钥的安全策略进行身份认证，具体而言，使用符合 X.509 的身份证明。使用这种方法必须有一个第三方的证明授权(CA)中心为客户签发身份证明。客户和服务器各自从 CA 获取证明，并且信任该证明授权中心。在会话和通讯时首先交换身份证明，其中包含了将各自的公钥交给对方，然后才使用对方的公钥验证对方的数字签名、交换通讯的加密密钥等。在确定是否接受对方的身份证明时，还需检查有关服务器，以确认该证明是否有效。

3 统一身份认证需求设计

3.1 用例图

此统一身份认证模型的 UML 用例图如图 1 所示。

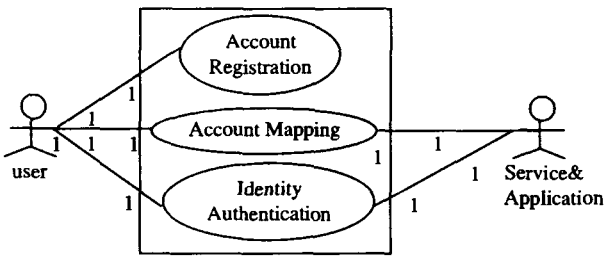

图 1 统一身份认证服务用例

由用例图可以看出，该统一身份认证模型应具备三个基本功能：

1. 用户注册：用户在统一身份认证服务中注册帐号，以后这个帐号可以在所有使用统一身份认证服务的应用系统中使用。此功能也包括用户基本信息修改等辅助功能。

2. 帐号关联：如果用户之前已经在相关的应用系统中拥有帐号，同时也已经设置了相应的权限，那么用户能够将这些应用系统的帐号与统一身份认证服务的帐号进行关联，使得用户登录统一身份认证服务之后，就能够自动使用相关的应用系统用户来访问应用系统。

3. 用户认证：为应用系统提供用户身份认证服务，本系统采用基于挑战/应答的认证机制，应用系统使用统一身份认证服务作为它的用户系统，用户与应用系统进行交互，进行登录操作，应用系统将用户提供的用户名/密码等转发给统一身份认证服务以检验其是否通过授权。统一身份认证服务验证用户的身份后将结果返回给应用系统，如果已经进行了身份联合，则将用户的本地帐号传递给应用系统。

此用例图只是统一身份认证模型的最外层抽象，具体的功能还有许多，包括应用系统验证用户的本地帐号来实现身份联合，用户资料修改等。

3.2 实体

按照以上的功能描述，此认证模型中要考虑的 UML 实体图如图 2 所示。

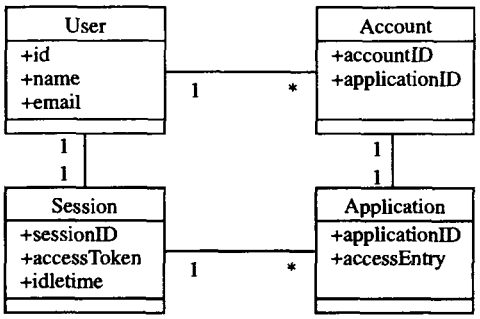

图 2 UML 实体图

在实体图中，各实体之间的对应关系由它们之间的数字来体现，即数字 1 表示对应一个实体，* 表示若干个实体。

1. 用户(User)：即统一身份认证服务的用户，在这里代表一个统一身份认证的帐号。

2. 帐号(Account)：应用系统的帐号，与统一身份认证服务的用户相关联，一个用户可以关联多个帐号。

3. 应用系统(Application)：使用统一身份认证服务的应用系统，这些应用系统可能是不同网络服务提供商的系统也可能是同一网络服务商的不同系统。

4. 会话(Session)：当用户登录统一身份认证服务后，即创建了一个活跃的会话。

4 统一身份认证模型设计

为了减少服务商管理用户信息的负担，解决用户频繁登录的问题，提高认证系统的安全性，并实现不同服务商、不同应用系统间对用户身份认证的统一，设计了本统一身份认证模型。

4.1 结构图

其结构图如图 3 所示。此统一身份认证模型系统主要包括三个部分：统一身份认证服务器、网络服务认证接口模块(包括 Web 认证接口模块，Notes 认证接口模块等)和用户信息数据库。

用户信息数据库存放系统的相关用户信息，包括：用户名、单向加密后的用户密码、用户的权限信息、用户有效期以及用户附加信息等，另外，用户信息数据库还要存放用户的联合属性信息，即用户在不同应用系统上的本地帐号和服务商或者应用系统本身的标识。

用户信息数据库通过信息存取通道为统一身份认证服务器提供各种用户信息。

统一身份认证服务器通过本系统中定义的安全认证通道与各种网络服务认证接口模块进行交互，交互的操作包括：

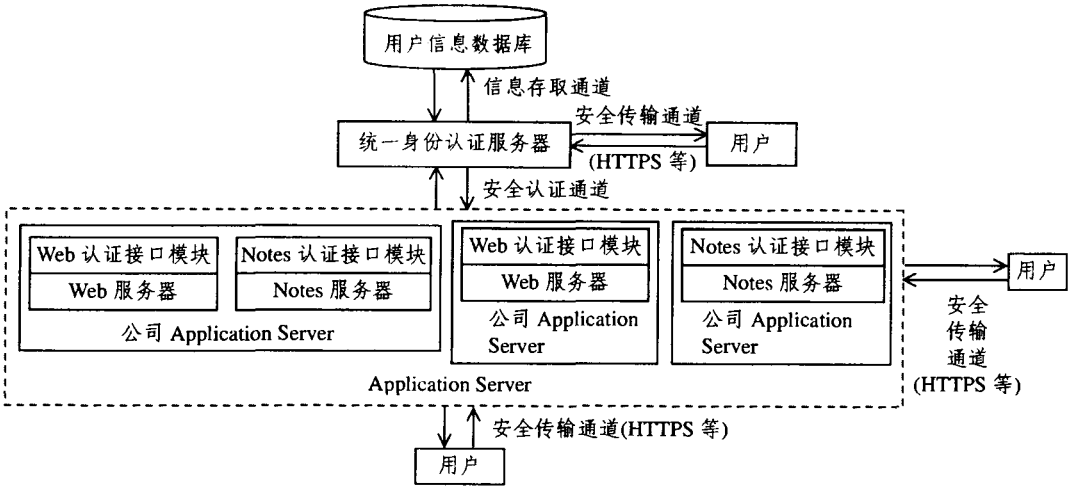

图 3　统一身份认证模型结构图

1)统一身份认证服务器接收认证客户(网络服务认证接口模块)的认证请求,并根据数据库中的用户相关信息确认用户的身份,再次通过安全认证通道返回认证成功或认证失败的信息。如果用户进行了统一身份认证服务帐号和应用系统本地帐号之间的身份联合,则统一身份认证服务器返回用户的本地帐号信息。

2)统一身份认证服务器向网络服务认证接口模块发送验证用户本地帐号的认证请求,网络服务认证接口模块检查本地信息数据库,对用户的本地帐号进行验证,返回验证结果。统一身份认证服务器根据情况将联合属性信息写入用户信息数据库。

另外,统一身份认证服务器还要提供一个让用户进行身份联合的接口,此模型是通过安全传输通道来实现的,用户可以安全地通过浏览器进行身份联合。

应用服务器(例如:Web 服务器、主机服务器、Notes 服务器等)既作为相对用户而言的服务器,又作为统一身份认证系统的客户。它们首先通过安全传输通道(如:SSL 通道)获取用户提交的用户名和密码,然后通过认证系统提供的网络服务认证接口模块经由安全认证通道向统一身份认证服务器提交认证请求,并获得认证结果(成功或失败),最终确定是否给该用户提供服务。

4.2　功能和特性

本认证模型采用扩展挑战/应答(Challenge/Response)方式的身份认证机制,这种机制就是每次认证时认证服务器端都给客户端发送一个不同的"挑战"字串,客户端程序收到这个"挑战"字串后,做出相应的"应答"。这种方式可以有效地防止网络侦听(sniffer)、"重放"攻击(replay)等,保证认证的安全。

模型系统设计的功能和特性主要有以下几个:

1)能够尽可能地利用现有系统的身份认证模块以及现有的用户设置和权限设置,尽量保护现有的投资,减少重新的用户设置和权限设置的费用,同时避免对现有系统进行大规模的修改。用户可以使用统一身份标识与用户在应用系统的本地帐号进行联合,即使用统一身份标识登录也可以使用本地服务,也就是所谓的单点登录。

2)具有良好的扩展性和可集成性,不仅能支持现有的应用系统及其现有的用户系统,当有新的企业应用被部署或开发的时候,这个统一身份认证模型可以作为它的身份认证模块的形式工作,也就是说,新的企业应用可以不自带用户系统,可以通过集成该服务的形式来实现等价的功能。

3)基于简单认证机制中的口令认证机制,以用户名和密码为确认用户身份的标志;这样认证方法简单可靠。

4)有完善的认证接口,让多种应用系统可以方便地通过接口使用本认证系统统一认证用户的身份。

5)用户密码在系统中加密存放,且不可逆;在认证过程中,明文密码绝不能在网络上传输,防止窃听导致泄密,保证用户密码的安全。应用系统和统一身份认证服务器之间传输的任何数据都是经过加密的,数据机密性得到了保证。

6)可以实现认证客户端和认证服务器的双向认证,确保认证双方的身份;

7)能够抵抗重放攻击,即防止攻击者使用窃听到的过时的认证数据包再次获得认证而冒充合法用户的身份,这是通过发送"挑战"字串来实现的。

5　认证算法和关键技术研究

5.1　认证算法

本文提出的认证算法既用于网络服务认证接口模块向统一身份认证服务器请求认证用户身份的情况,也用于在身份联合阶段统一身份认证服务器向网络服务认证接口模块请求认证用户本地帐号的情况。

考虑到系统的安全和高效,要求设计的认证算法亦是安全、高效的。安全主要有三方面:

(1)在认证过程中传输的数据不怕被窃听,通过对传输的数据进行加密实现;

(2)传输中的数据可以防止被篡改,通过对传输的数据进行数字签名实现;

(3)可以抵抗重放攻击,方法是在认证数据包中打时戳,或在认证过程中使用 Challenge-Response 方法实现。采用时戳需要各系统实现时间同步,增加了系统的不安全性,故本模型实现采用扩展的 Challenge-Response 方法。

认证算法采用类似 RADIUS 协议的算法,其符号说明和流程如下:

C:Client,认证客户,一般为网络服务认证接口模块,身份联合时为统一身份认证服务器;

S:Server,一般为统一身份认证服务器,身份联合时为网络服务认证接口模块;

K:C 和 S 之间的共享秘密,即待认证用户的单向加密后的密码,以安全的方式保存在双方的系统中;

N:待认证用户的用户名;

R:S 产生的随机数;

$H\{M\}$:对消息 M 做单向 Hash 消息摘要运算,常用的算法为 MD5 算法;

$CK\{M\}$:以密钥 K 使用对称加密算法对消息 M 进行对称加密,常用的算法为 DES 或 RC5;

r:认证的结果,成功或失败;

1. $C=>S$:N,$H\{N+K\}$

2. $S=>C$:$C_K\{R\}$,$H\{N+C_K\{R\}+K+R\}$

3. $C=>S$:N,$C_K\{R,K\}$,$H\{N+C_K\{R,K\}+K+R\}$

4. $S=>C$:$C_K\{r,R\}$,$H\{N+C_K\{r,R\}+K+R\}$

其认证流程图如图 4 所示。

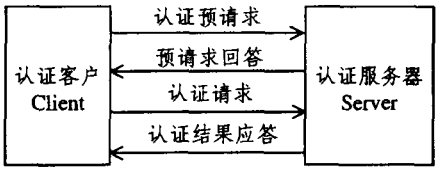

图 4 认证流程图

在认证的每一个步骤中,无论客户端还是服务器端,都要求对数据包中的 $H\{\}$ 域做校验。由于 $H\{\}$ 域中包含了 C 和 S 之间的共享秘密,因此对于不知道此秘密的攻击者而言,是无法伪造合法的数据包的,也由此双向证实了 C 或 S 的身份。认证的过程分为预请求和正式请求两部分,其中预请求是 C 向 S 获取随机数 R 的过程,在正式的认证请求中 C 必须向 S 提交此凭据。由于 R 对于每次认证请求都不同,且在 S 端有记录,攻击者即使窃听到了一个成功的认证请求包,在下次使用时却失效了,因此可以很好地防止重放攻击。

5.2 帐号联合算法

帐号联合算法用图 5 来表示:

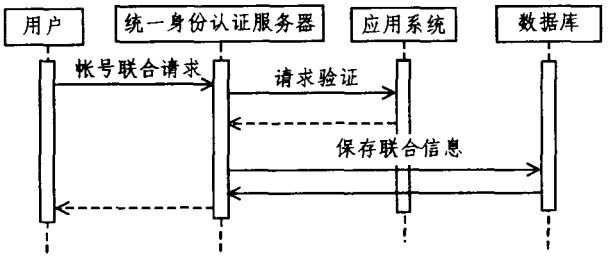

图 5 帐号联合算法时序图

1. 用户向统一身份认证服务(简称服务)发出帐号关联注册请求,用户提供了应用系统的标识 A,同时提供了可以在该应用系统中使用的用户信息(可能包含用户名和密码等)。

2. 服务首先向该应用系统 A 征询,用户信息是否合法。

3. 如果收到合法响应,那么服务就将这个帐号关联注册信息保存到用户注册库中,以后该用户登录统一身份认证服务之后,就能够使用相应的应用系统 A。

4. 当注册库完成保存操作后,统一身份认证服务响应用户,身份联合完成。

5.3 性能问题

用户认证是各个应用系统的门户,每个用户进入到系统中都需要经过认证这一步骤。因此,统一身份认证服务器的性能问题将极大影响各个应用系统的可用性。为了消除认证的性能瓶颈,提高系统的认证响应速度,在系统设计时做了如下的考虑:

(1)采用高性能的服务器,连接到高速网络上,避免网络拥塞;

(2)认证协议采用类似于 RADIUS 协议的方式,通讯数据包使用 UDP 数据包。使用 UDP 方式有许多优势:系统是请求-应答方式,使用 UDP 可以大大简化服务器的处理流程,减少系统资源的消耗,提高系统的响应速度;无连接的 UDP 通讯方式,更适合于多认证服务器做分布式处理;

(3)在服务器上对数据库中的用户信息做缓存,并在服务器轻载的时候与数据库进行同步。这样可以减少连接数据库时的资源消耗,能较大幅度提高系统的处理速度;

(4)如果单台服务器负载过重,无法处理所有的认证请求时,可以很方便增加新的服务器作并行分布式认证请求处理。

经过优化后的统一身份认证服务器完全可以满足多应用系统的认证请求。

结束语 此网络服务统一身份认证模型系统是为了解决多服务商多应用系统之间用户和口令不统一、用户使用不方便的问题,提出了一种安全、可靠、高效的口令认证算法及身份联合算法,对优化系统性能、提高系统响应速度做了一定的探索。此模型能够应用的领域包括:

1)企业、高校,科研机构等单位内部的各种应用系统;

2)跨国企业的各个部门或地区分公司的各种应用系统;

3)行业内各个企业的不同应用系统;

4)Internet 上丰富的应用环境。

统一身份认证模型实现的单点登陆功能,可以让用户只需进行统一帐号的登陆便能进入已经联合的任何应用系统,享受其提供的本地服务。

此统一身份认证模型可以扩展成支持 Web Services 技术框架,使得在对各个应用系统实施基于 Web Services 的应用集成的时候能够使用它进行身份认证。

参 考 文 献

1 Kohl J, Neuman C. The Kerberos Network Authentication Service (V5). RFC 1510, Digital Equipment Corporation, USC/Information Sciences Institute, Sept. 1993

2 ITU-T, Recommendation X. 509. The Directory-Authentication Framework. Consultation Committee, International Telephone and Telegraphm, Inernational Telecommunications Union

3 RFC 1321. The MD5 Message-Digest Algorithm. Internet Request for Comments 1321, R. L. Rivest, Apr. 1992

4 Rigney C, Rubens A, Simpson W, Willens S. RFC 2138Remote Authentication Dial In User Service (RADIUS). 1997

5 Livingston C R. Remote Authentication Dial In User Service (RADIUS). RFC2138. April 1997

6 Livingston C R. RADIUS Accounting. RFC2139. April 1997

7 Leech M. SOCKS protocol Version 5. RFC1928. 1996

8 张晔,刘玉莎,张志浩. 透明网络安全体系结构的研究. 计算机工程与应用,2000,4:119

9 许晓东,荆继武,阮耀平. 一种混合密码体制的认证协议及分析. 计算机工程,2000,2:72