一种基于单向散列函数的人机结合认证系统

A New User – computer Combination Authentication Based on Hash Function

诸葛理绣　徐义峰　（浙江 衢州学院 现代教育技术中心 324000）

摘要：本文基于单向散列函数的特性，提出了一种新型的身份认证方案。该方案不仅能够提供通信双方的相互认证，而且能防范重放和窃听等攻击手段。

关键词：网络安全　身份认证　散列函数

1　引言

据有关调查显示，在已破获的采用计算机技术进行金融犯罪的人员中，外部非授权人员占 10%、外部授权人员占 15%、内部非授权人员占 17%、内部授权人员占 58%[1]。以上调查数据说明，加强 Intranet 内部网络安全是十分重要的。Intranet 内部网络安全主要通过认证、访问控制和审计等安全服务来实现。有效的安全认证是其他安全服务得以有效实施的前提与基础。

身份认证是对网络中的主体进行验证的过程。通常有三种方法来验证主体身份：

（1）基于主体所知道的，如口令、密码；

（2）基于主体所拥有的，如智能卡、令牌；

（3）基于主体的个人特征，如指纹、声音、视网膜、虹膜等。这些通过单一元素的认证方式尚不能保证接入网络主机的合法性。事实上，随着信息化进程的推进与计算机的迅速普及，在 Intranet 中，用户一般与所使用的主机有较为固定的关系。如果在 Intranet 中，接入用户只有在指定的主机上才能通过身份认证，既实施“用户只能使用指定主机，主机只能被约定用户使用”的人机双元素认证策略，可进一步保证接入 Intranet 的主机与用户的可信性。内部人员使用网络资源的接入主机是固定的，这样可进一步约束与规范其网上行为。

CHAP 认证方案是最常用的一种基于口令的单向身份认证方法。本文在此基础上，提出了一种实用有效的基于单向散列函数的人机结合双向身份认证方案。该方案通过人（用户）与机（接入主机）两种元素，有效地保证接入用户与主机的合法性；实现了用户和服务器间的相互认证，有效地防止了重放与窃听等攻击手段，能显著增强应用系统的安全性。

2　散列函数

散列函数 H 一般具有如下特性：

（1）H 能够应用于任意长度的输入数据块；

（2）H 产生定长（128 位）的输出；

（3）对于任何给定的数据块 M，H 都能够相对容易地计算出 H(M)，使得软、硬件实现是可行的；

（4）单向（One – way）性质：对于任何给定的 h，寻找满足 H(M) = h 的数据块 M，在计算上是不可行的；

（5）弱碰撞抵抗（Weak Collision Resistance）：对于任何给定的数据块 M，寻找满足 H(N) = H(M) 且 M≠N 的数据块 N，在计算上是不可行的。

输出 h 称作是原输入报文的“指纹”或“报文摘要”。

3　基于散列函数的人机结合认证方案

为方便叙述，做如下符号约定：UID 为用户的身份标识；PWD 为用户的口令字；Passwd 为用户加密后的口令字；PID 为客户端主机的标识；SID 为一次认证会话的标识符；C 代表用户与主机所结合的客户端；S 代表认证服务器端；K 为服务端对称加密算法（如 DES、IDEA 等）的密钥；CH 用作“挑战”字；$E_K(m)$ 使用密钥 K 对明文 m 加密；$D_K(m)$ 使用密钥 K 对明文 m 解密；H

(m)用单向散列函数计算消息 m 的消息摘要；‖为连接操作；X→Y：M 表示从 X 向 Y 发送信息 M。

为了实现通信双方相互认证及对客户端人机绑定功能，本文在设计时对传统的"挑战"字认证方案进行了必要的改进。另外，认证服务器后台数据库至少需要创建如下数据结构(库表)：

UserList：定义了用户对象的属性，如 UID、Name(用户名)、Passwd(用户口令)、EnrollDate(注册时间)、Department(所属部门)等。

PcList：定义了主机对象的属性，如 PID、Station(主机位置)、EnrollDate(注册时间)、Department(所属部门)等。PID 只要在相应的网络区域中具有唯一性即可。为应用方便，PID 可以由主机的某些配件的 ID 构成，如网卡的 MAC、硬盘的 ID、CPU 序列号等。也可以由某配件的 ID 与 IP 地址连接组合而成，如 IP ‖ MAC 等。

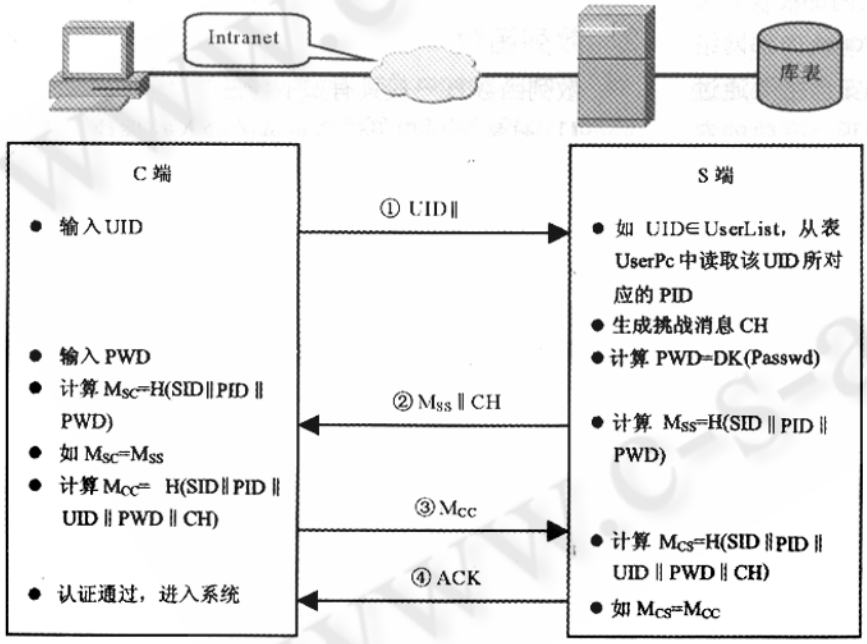

图 1　协议工作流程

UserPc：定义了用户与主机的对应关系。

3.1 初始注册过程

用户在使用系统认证前，必须向认证服务器提交有关用户与所对应的主机的属性信息。具体注册流程为：

步骤 1：C→S：UID，PWD，PID 等；

用户将 UID，PWD，PID 等信息通过安全通道传送到认证服务器(必须保证提交通道的安全性)。

步骤 2：认证服务器对用户提交的口令进行强度检查，如：口令是否为大小写字母的混合体、其中是否有非字母的符号(如 $、%、&等)和数字；口令的长度是否符合设定要求等。如果通不过口令强度检查，则提示用户再次提交符合一定强度的口令，直至成功为止。

步骤 3：如果通过口令强度检查，认证服务器将 UID、Passwd = E_K(PWD)、PID 等注册信息存入相应的库表，并在 UserPc 表中建立用户与主机的映射关系。

3.2 认证过程

为了进入系统，用户在登录时必须执行一次身份认证过程。本方案中认证协议流程如图 1 所示。

步骤 1：C→S：UID ‖ SID

这是认证请求步骤。如用户要登录系统，则向认证服务器 S 端发送自己的 UID 及这次认证会话标识符 SID。SID 应是随机的，并保证每次认证会话的 SID 是不同的。

步骤 2：S→C：M_{SS} ‖ CH

该步完成了对 C 端用户的身份识别。S 端在收到 C 端用户的 UID 后，判断 UID 是否属于 UserList。若 UID ∈ UserList，表明 UID 合法，则从 UserPc 表中读取该 UID 所对应的 PID，由"挑战"字生成函数生成随机"挑战"字 CH，解密 PWD = D_K(Passwd)，计算 M_{SS} = H(SID ‖ PID ‖ PWD)，然后将 M_{SS} ‖ CH 发送给 C 端，并在本端保存 CH、PWD 与 SID 副本；若 ∉ UIDUserList，则说明用户为非法用户，S 端终止与 C 端的会话。

步骤 3：C→S：M_{CC}

该步完成了对 S 端的身份验证。C 端收到 S 端发送的消息之后，由于 M_{SS} 定长(16 个字节)，即可取得 CH，读取本机的 PID，用户输入 PWD，然后计算 M_{SC} = H(SID ‖ PID ‖ PWD)，验证 M_{SC} = M_{SS} 是否成立。若成立，则 S 端的身份得到了验证，并计算 M_{CC} = H(SID ‖ PID ‖ UID ‖ PWD ‖ CH)后发送给 S 端；若 M_{SC} ≠ M_{SS}，为防

止用户口令字输入错误，可提示用户再次输入 PWD（可指定重复输入次数，如三次），如口令确保正确且 $M_{SC} \neq M_{SS}$，则可证实 S 端是假冒的，C 端终止与 S 端的会话。

步骤 4：S→C：ACK

该步完成了对 UID 与 PID 的结合认证。S 端收到 MCC 后，计算 M_{CS} = H（SID ‖ PID ‖ UID ‖ PWD ‖ CH），然后验证 $M_{CS} = M_{CC}$是否成立。若成立，则用户的身份得到了验证并证实是在使用指定的主机登录，S 端发送 ACK—Success 给 C 端；否则，说明用户为非法用户，或未使用指定的主机，S 端发送 ACK—Failure 给 C 端，并终止与 C 端的会话。

另外，初次认证成功后，认证服务器可不定时地发送新的“挑战”字给客户端用户，重复步骤 1～4，以便在通信过程中随时验证通信双方身份的合法性。

4　方案性能分析

下面就方案的功能与安全性进行剖析。

4.1　功能评估

（1）C 端对 S 端的身份进行了验证。C 端通过验证 $M_{SC} = M_{SS}$SC = MSS 是否成立来确认 S 端是否知道 C 端所对应的 PID、PWD 及 PWD 加密保存的密钥 K，从而验证 S 端身份的合法性。另外，由于 SID 是随机不重复的，可防止非法者通过重放 MSS 来假冒 S 端。

（2）S 端对 C 端的用户与主机进行了绑定验证。S 端通过验证 UID 的合法性，并通过验证 $M_{CS} = M_{CC}$是否成立，可验证用户的合法性。同时，由于 M_{CC} = H（SID ‖ PID ‖ UID ‖ PWD ‖ CH），根据单向散列函数的特性与 PID 的区域唯一性，可确定用户是在使用指定的主机。这就实现了“用户只能使用指定主机，主机只能被约定用户使用”的人机结合认证策略。

（3）可实现 IP 地址管理。如主机 PID 选为 IP ‖ MAC 后，接入主机的 IP 与分配 IP 不一致时，有 $M_{CS} \neq M_{CC}$则用户通不过认证，从而实现主机的 IP 地址的管理。

4.2　安全性分析

（1）口令信息的保护。在用户注册阶段，通过口令字强度检查、口令非明文传输及“挑战”字的随机性，提高了口令抗字典攻击与口令字猜测攻击能力。在服务端用户口令通过加密方式保存，提高了口令保密性。

（2）可防窃听攻击。认证过程中，用于身份鉴别的信息都是通过单向散列函数做了报文摘要。由于单向散列函数的单向性，在网上所传输的 M_{SS}、M_{CC}是防窃听攻击的。

（3）可抗重放攻击。由于 SID 与 CH 的随机性与不重复性，所以入侵者重放已经截获的信息是无法通过认证的。

（4）可防假冒攻击。这是身份认证的功能所在。入侵者冒充任何一方，由于他不知道用户口令及其所用主机的 PID，而且这些信息在网上是通过单向散列函数产生“摘要”后传输的，故无法完成协议的认证过程。

（5）认证过程是安全的。假设入侵者可以截获合法认证过程中的任何通信报文进行分析，他从截获的报文中仅能知道用户的 UID，当然直接重发认证步骤 1 的报文也仅能通过服务器的初步认证（身份识别过程）；但由于用户口令 PWD 及主机 PID 根本不通过网络传输，因而他不可能从截获的报文中解析出 PWD 与 PID，准确算出 M_{CC}、M_{SS}等值，从而无法通过下一步的认证，故方案的整个认证过程是安全的。

5　结束语

本文结合 CHAP 认证模型，基于单向散列函数设计了一个有效的适用于网络通信系统的人机结合认证方案。该方案能够满足通信双方进行相互身份认证的要求，并实现了用户与主机的绑定，体现了“用户只能使用指定主机，主机只能被约定用户使用”的人机结合认证策略。该方案有效地保护了用户口令信息，防范重放攻击、窃听攻击、假冒攻击等。

参考文献

1　曹天杰、张永平、苏成，计算机系统安全[M]，北京高等教育出版社，2003.134～161。

2　R. Rivest. The MD5 Message－Digest Algorithm [S], RFC1321, 1992.4.

3　B. Aboba. Extensible Authentication Protocol (EAP) [S], RFC3748, 2004.6.

4　W. Simpson. PPP Challenge Handshake Authentication Protocol (CHAP) [S], RFC1994, 1996.8.

5　任传伦、李远征、杨义先，CHAP 协议的分析和改进[J]，计算机应用，2003，23(6)：36～37。