办公自动化系统中的安全性

周世杰* 秦志光 耿 技
(电子科技大学微机所 成都 610054)

【摘要】 针对OA系统的安全需要及特点，结合Lotus Domino，讨论了OA系统的网络安全和用户认证协议，着重论述OA系统内部用户和网络用户的安全认证机制、协议及其基本原理；提出了一个OA系统中的用户认证协议，分析了其认证过程。

关 键 词 办公自动化； 网络； 网络安全； 安全机制； 安全威胁
中图分类号 TP309

在OA系统中，许多文件或档案的访问权限是根据不同的用户而设定的；在规划一个OA网络时，必须考虑到安全性的需要。从安全性角度上讲，规划OA网络时，主要应考虑窥探威胁、欺骗威胁和使用防火墙保护[1~3]。在规划OA网络安全时，还必须考虑OA网络与Internet互连后的安全性，常采用防火墙技术保证OA Internet的安全。

本文讨论了OA系统的安全认证协议，当用户通过了网络认证后，OA系统还采用数据库、文档、视图、域等其他级别上的安全控制机制对用户进行相应的验证，其基础仍然是用户认证协议。

1 OA的用户验证机制

在一个典型的OA网络中，存在两种客户：Notes用户和Internet用户，它们在安全机制上有不同的特点。因此，即使采取一定措施保证了OA网络的物理安全性，还必须通过一定的机制确保合法的OA用户不能越权访问服务器。本文采用认证机制很好的解决Notes用户(Notes Client)的安全性问题[4]。

2 用户识符文件

在OA系统中，用户标识符文件(ID文件)是OA安全性实施的前提和基础。在Domino中Notes ID文件是指包含验证者姓名、到期日期、验证者的公开密钥和私有密钥、验证字和加密密钥等信息并用口令加密后保存到Domino Server公用通讯录或软盘中的二进制文件。当创建组织内的第一个Domino Server时，系统自动创建Domino域的最高认证标识符文件(Cert.ID)，并用它来对该组织内的服务器和管理者标识符文件进行验证。对其他用户，Domino采用层次验证法进行安全性认证。典型的层次认证结构如图1所示。

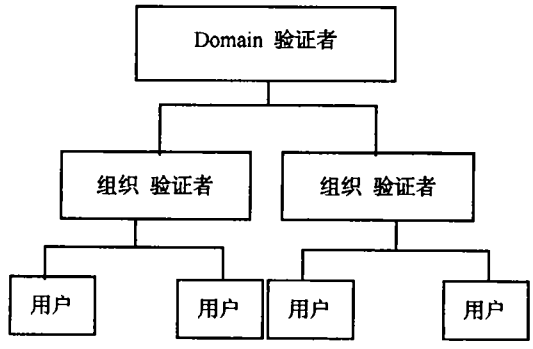

图1 Domino网络域中Notes Client层次命名结构图

1999年10月23日收稿
* 男 28岁 硕士 助理工程师

3 OA 系统中的用户认证协议

OA 系统中采用公开密钥体制实现用户认证协议。在公开密钥体制中每个用户有一个公开密钥和一个私有密钥，它们在数学上有某种联系。公开密钥一般存放在权威的密钥管理中心，用来对信息加密和解密；而私有密钥则存放在用户的标识文件中，用来加 / 解密、数字签名等。

在 Domino 系统中为了确保公用密钥的可靠性、权威性，采用 Domino 域的验证者标识符文件进行验证，在验证的过程中产生一个有验证者签名的验证字(消息)，它指明了某个公开密钥与特定用户名之间的对应关系；只要其他用户信任 Domino 验证者的数字签名，就可以信任用户的公开密钥。因此，验证字和公开密钥标识了一个用户的合法性。

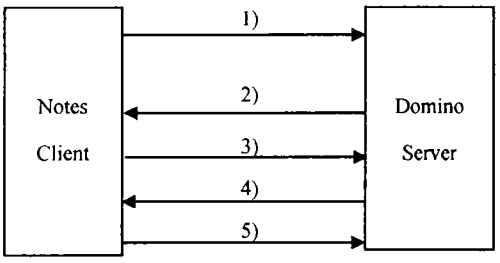

图 2 Domino 网络中 Notes Client 的认证协议示意图

当用户和 Domino Server 通信时(如复制、打开数据库、邮件转送)，都要通过两个过程来完成安全认证[5,6]：建立公开密钥的相互信任和使用客户 / 服务器的公开密钥、私有密钥进行询问 / 应答。图 2 示出了组织单元 OU 内部用户 Client 和 Domino 中的 Server 的认证协议，具体描述如下：

1) Client→Server ：{Client 向 Server 建立连接的请求、其他相关信息}；

2) Server：Server 从公用通讯录中取出 Domain 内的公开密钥(D)、ID 文件，并用 D 对 ID 文件中 OU 的验证字进行验证。如果 OU 验证字无效则访问被拒绝；如果有效则读取 OU 颁给用户 Client 的验证字、OU 的公开密钥，并用 OU 的公开密钥验证用户 Client 的验证字的有效性；若 Client 的验证字无效，则访问被拒绝；若有效则 Server 信任用户 Client 的公开密钥；

3) Server→Client：{随机数(Once0)}；

4) Client→Server：M1=Kd{Once0}；

Kd::Client 的私有密钥

5) Server：Once1=Ke{M1}

Ke:: Client 的公开密钥

If

Once1=Once0

then

信任用户 Client

else

否则拒绝访问。

随后这一过程反向进行，用户 Client 首先建立对 Server 的公开密钥的信任，再验证 Server。

经过上述两个过程，最终完成了用户 Client 和 server 的双向验证。由此可见，Domino 采用双密钥体制，通过请求 / 应答完成了双向认证，而且在该认证协议中口令不需要在网络中传送，安全性非常严格。

4 OA 系统中 Internet 客户认证协议

由于 Internet 客户没有 ID 文件，因而验证过程和本地用户的认证过程不同，对 Intertnet 客户的验证取决于具体的开发平台。在 Domino 中则取决于是通过 TCP/IP 还是 SSL 端口访问 Domino Server。

4.1 通过 TCP/IP 访问 Domino Server

4.1.1 基本口令认证

如果 Internet 客户访问 Domino Server 时，超过了用户缺省的权限和执行受限制权限操作，Domino Server 就回向客户询问用户名和口令，如果用户名和口令都正确则该客户可以访问 Domino Server。这种方式下，用户名和口令均为明文转送，因而容易被攻击者窥探，不能严格保护服务器的数据访问。

4.1.2 匿名访问

这种方法不能验证用户，也不能保护用户和服务器在网络间的数据传送，而是将安全性限制的权限完全交给了数据库设计者。这是一种很不可靠的方法，应尽量少用。

4.2 基于 SSL 的 Internet 客户认证

这是 Domino 网络和 Internet 相连最为安全的机制。Domino Server 支持 SSL3.0，并利用 SSL 进行加密和数据验证。在 Lotus Domino 中，基于 SSL 的 Internet 客户和 Domino Server 连接有三种方法：客户机验证、基本口令验证和匿名访问。

4.2.1 客户机验证

这种方法允许用 Lotus Domino 基于客户机的 SSL 验证字来验证客户，并加密客户和服务器之间的数据，完成了客户对 Domino Server 的认证，保证了双向认证和数据的机密性。

4.2.2 基本口令认证

这种方式类似于 TCP/IP 下的基本口令认证，它使用询问 / 应答方式要求客户输入用户名和口令，然后再进行认证；不同之处在于这种方法加密客户和 Lotus Domino 之间的数据。

4.2.3 匿名访问

和 TCP/IP 下的匿名访问一样，如果不需要知道谁将要访问 Domino Server，可以使用这种方法，不同之处在于这种方法也加密客户和 Domino Server 之间的数据。

由此可见，Domino SSL 提供了保密、消息完整性、客户和服务器双向认证等安全性功能；但是，SSL 的安全性是基于 Domino Server 和 Internet 客户之间的验证字的，因而必须有权威的认证中心(CA)来颁布相应的验证字，以确保验证字的可靠性和可信性。CA 通过发布盖有 CA 数字签名的验证字和在加密文件中包含的信任根验证字来确认 Domino Server 和 Internet 客户。Lotes Domino 既支持内部的 CA，又支持外部的 CA。外部 CA 可以创建服务器和客户机验证字，而内部 CA 只能创建服务器验证字，不能创建客户机验证字。在 Domino Server 内部通过创建 CA 应用程序(CERTCA.NSF)来颁发和验证服务器的验证字；同时，如果得到了客户机的外部验证字，就可以完成 Domino Server 和 Internet 客户的双向认证(Internet 客户只能通过外部 CA 获得验证字)。以下是一个完整的 SSL 认证协议(假设用户 A 希望同 Domino Server B 建立连接)：

A→B:　M1={请求建立连接消息}

B→A:　M2={B 自己的公开密钥(Keb)，验证字消息 M1}

A→B:　M3=Keb{Kw}

　　Kw={A 使用算法生成的工作密钥 Kw}

B:　Kw=Kdb{M3}

　　Kdb::B 的私有密钥

A→B:　M4=Kw{ Signature}

　　Signature::A 数字签名的验证字

B:　Kw{M4}

　　If

　　数字签名没有被篡改

then

则通过验证，允许访问

else

B→A:M5={Reuist UID and Pwssword}

A→B: M6=Kw{UID，Password}

B: Kw{M6}，并同保存的用户名和口令比较，相同则同意访问，不一致则拒绝 A 的访问请求。

5 结 束 语

由以上的分析可知：OA 系统可以通过正确规划网络的结构防止窥探和欺骗，采用防火墙技术可以确保非法攻击者访问服务器，通过用户认证协议可以确保合法用户不能越权访问服务器，通过服务器的的安全通信协议如 SSL 使服务器可以供合法用户适宜的访问。但这些安全方法的前提和基础是用户认证。本文给出的用户认证协议可以很好的实现用户认证、数字签名和口令保护。

参 考 文 献

1 Banks Michael A. Web psychos stalkers and pranksters. 北京:中国水力电力出版社，1998

2 Atkins Derke. Internet security professional reference. 北京:机械工业出版社，1998

3 秦志光，刘锦德. ODP 环境中全局安全系统内的安全域之间的连接. 电子科技大学学报，1995，24(5):520~523

4 北京义驰美迪技术开发有限责任公司. Lotus Domino4.6 应用开发指南. 北京:中国水力电力出版社，1998

5 Jarol Scott, Pena Marisa. Web design & development black book. 北京:机械工业出版社，1998

6 Sikhurana Gunnit. Web database construction kit. 北京:机械工业出版社，1998

Security in Office Automation

Zhou Shijie Qin Zhiguang Geng Ji

(College of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract This paper studies the primary security technology with Lotus Domino, and analyzes the network security in office automation system. The principle and mechanism of user authentication in local area network and wide area network are investigated. A practical user authentication protocol and its authentication process are given.

Key words office automation; network; network security, security domain; security mechanism; security threat