NOTES 的安全机制

陈 霞 （广西师专计算机室）
罗铁坚 （广西大学计算机科学系 530004）

摘要：本文介绍信息系统开发平台 NOTES 的特点，比较了传统 DBMS 与 NOTES 各自的安全机制，最后提出使用 NOTES 安全机制的建议。

关键词：DBMS MAIL RSA

一、引言

八十年代末九十年代初的信息系统应用开发平台多数是在 DBMS 之上完成，进入九十年代中期，以其作为应用开发平台已不能满足需要，特别是 INTERNET 技术的成熟和多媒体、多文档及非结构化应用开发的需求，使多数的软件开发商转向“群件”软件的开发与应用上。Notes 在群件中可谓一支独秀。它是一个杰出的信息系统（IS）开发平台，有许多特性是传统的开发平台所没有的。本文介绍其安全性，可以作为应用系统开发和数据库理论研究的参考。

二、Notes 主要特性

人们谈论“groupware”（群件）时，常常提到 Lotus Notes。自从 1989 年以来，Notes 已成为 groupware 的经典范例，目前已有四百多万用户使用 Notes，它与现存软件有明显的差别是：它一部分是第二代电子邮件，一部分是应用开发平台，在许多方面它类似于网络操作系统，它把网络、电子邮件与数据库应用的复杂性屏蔽起来，把易用性呈现给用户。

1. Notes 是一个多平台，具有一个非常一致的接口

Lotus Notes 应用程序能在四种平台上开发和运行 WINDOWS，MACINTOSH，OS/2 和 UNIX。其使用介面和应用开发平台是一致的，而且能进行交互开发，因为其代码实际上是数据库中文档的一部分，所以在不同平台上使用应用程序不需要修改或重新编译。

2. 非常好的安全工具

Lotus Notes 使用了 public－key 和 private－key（共用密钥和私人密钥）加密。作为开发者，能使用它来确保应用程序是安全的，它的 RSA 许可加密被装入邮件系统，因而任何使用 Notes 邮件的应用程序自动地加密文档，不需额外的工作。而且单个文档段可选择地加密，密钥可以分配给想要访问部分数据的单独用户。

3. 集成的 E－MAIL

Lotus Notes 的电子系统的特点是稳定可靠可配置的和可维护的，而且是面向工作流和归档作为目的。Notes 的应用程序能使用内置的邮件机制在数据库之间移动文档。电子邮件与数据库集成在一起，并且支持各种操作系统、网络操作系统和多协议的传输。

4. 集成的远程访问

Lotus Notes 中的关键特性之一是用于用户的远程访问。而且 Notes 的远程访问不要求用户在工作时联机，这种应用程序适用于经常外出的人员使用。

5. 设有 WAN 的服务器－服务器连接

Notes 的复制（replication）机制能有效地使用拨号线在服务器之间同步数据库。

6. 快速的应用程序原型化和开发

与传统应用开发工具相比，Notes 应用程序平台能非常快速地被原型化和开发，有许多应用模板提供参考和使用。

7. Notes 应用于 Internet

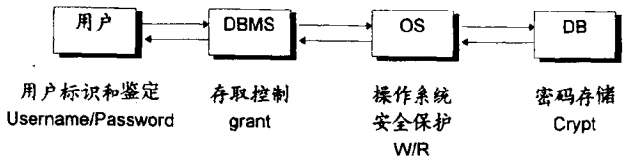
Notes 包括一个 Inter Notes Web Publisher 2.0。这个自动 HTML 创作系统将 Notes 文件转换为 WWW 页。Notes 4.0 本身设有内置 Web 浏览器，但程序可在任何文件中嵌入 Web URL，用鼠标双激 URL，Notes 将自动连接用户和 Web 页。这种页面看上去象是 Notes 文件，实际则是 Web 页。

三、传统 DBMS 的安全机制与 Notes 安全机制比较

1. 数据库安全性一般定义

数据库安全性是指保护数据库以防止不合法的使用。一般的安全措施包括系统处理和物理两方面。其中

的物理安全是防窃取设备，不属于本文论述范围。计算机系统的安全措施主要归纳为如下图：



其中 DBMS 的安全措施多侧重于用户标识和鉴定上，也就是用户名和口令字，以及对基表的存取控制和资源使用控制上，特别采用了授权机制。

2. Notes **的安全机制**

Notes 的安全机制是通过大量的安全性选项设置来完成，它可以维护从服务器级、通过数据库和文档级直到单个文档的字段一级的整个结构的安全性。

(1)对数据库的限制性访问。对数据库的限制访问性可分为两种安全类型：①Notes 服务器的物理安全性；②数据库访问控制表设置。其中①不在本文论述范围；数据库的访问控制表(ACL)是 NOTES 最有效的安全工具之一。该表用来指定谁可访问一个给定的数据库及在那个数据库中用户能完成的任务类型。

一个数据库的 ACL 能列出 PEOPLE(人)GROUP(组)和 Notes Servers(Notes 服务器)，并能将下列七种访问级别(Access Level)中的一种分配给他们。

·管理员(manager)：类似 DBA，能完全控制数据库及其设计，包括设置数据库 ACL 的能力。

·设计者(Designer)：在 ACL 中具有设计访问权的人、组或服务器能改变数据库的窗体、视图和宏的设计。但不能改变数据库的 ACL。

·编辑(EDITOR)：不仅能建立新文档，而且能够编辑和删除由另一位人员构成的文档。

·作者(AUTHOR)一位作者能构成新文档，但受到限制，仅能编辑由本人组织的文档。

·读者(READER)：只能读，不能组织和编辑任何文档。

·委托人(DEPOSITER)：委托人只能在数据库中构成文档。文档在数据库中完成之后，具有委托人访问权的人不得查看该文档。

·无访问权(NO ACCESS)：不能对数据库进行任何操作。

在访问级别中有几个还有附加的属性：

CAN DELETE DOUMENTS(能删除文档)和 CAN CREATE DOUMENTS(能建立文档)。在 ACL 列表中，还包括了对角色的定义。

(2)对窗体和文档的限制性访问。当设计一个窗体时，有两个特殊的窗体属性在 DESIGN FORM ATTRIBUTE 对话框中设置，用于控制谁能使用该窗体构成文档和谁能读取使用该窗体构成的文档，以及在 READ ACEESS 和 COMPOSE ACCEESS 定义什么样的用户，组成角色能用给定窗体读取或构成文档。另外对视图的限制性访问和对宏的限制性访问权限设置与对窗体和文档的限制性访问类似。

(3)加密密封和签名字段。Notes 使用复杂的加密算法选择性地对字段进行加密。当然可以利用其他第三产品加密文件但 NOTES 加密系统是严谨和近乎天衣无缝。NOTES 包含两种加密形式：共享密钥方法，用来为那些拥有加密密钥的个别保护特定字段里的数据；公共/专用加密密钥加密机制("密封")，可用于通过 Notes 邮件机构发送所有文档。

·共享密钥字段

在应用程序中使用加密密钥共有四点，步骤如下：

①建立加密密钥；

②使用窗体指定、字段加密；

③将加密密钥与字段连接；

④将加密密钥与字段连接。

·邮寄时的"密封"字段

与刚刚描述的加密数据的共享密钥方法相对照，Notes 也使用公共/专用密钥加密技术。该加密方法包含在 Notes 邮件系统中。Notes 邮件加密非常类似于共享密钥加密：其中在文档中只有指定字段被加密，并且这些字段必须由数据库设计者指定。如果用户在邮寄文档中选择了 ENCRYPT 选项，则 Notes 建立一个随机密钥，并将该文档中的内容加密。然后用接收者的公开密钥加密该随机密钥，并将加密后的随机密钥加到要邮寄的消息中，从而有效地密封文档，以便只有预期的接收者可以打开文档。

当接收者收到邮件后，他的专用加密密钥(存储在该用户的 ID 文件中)用来解密随机密钥，然后用随机密钥解密消息中的加密手段。

·电子签名字段