基于 USB Key 的 Windows 凭据提供登录系统的设计与实现

杨 海[1] 赵文涛[1] 张乃千[2] 番丝江[1]
(国防科学技术大学计算机学院 长沙 410073)[1] (国防科学技术大学光电科学与工程学院 长沙 410073)[2]

摘 要 目前,Windows 操作系统得到广泛应用,其登录系统的安全性是人们重点关注的问题。首先分析比较了 Windows 的 GINA(图形标志与身份验证)登录模型和 Credential Provider(凭据提供)登录模型的安全性,通过引入 USB Key 第三方认证方式,提出了基于 USB Key 的 Windows 凭据提供登录系统设计方案,有效地将 Credential Provider 登录模型和 USB Key 认证方式的安全性相结合,提高了传统"用户名+密码"登录方式的安全程度。基于 Windows 7 操作系统,选用 USB Key3000D 身份认证锁为开发平台,基于 Windows Credential Provider COM 库设计并实现了基于 USB Key 的 Windows 凭据提供登录系统。

关键词 图形标志与身份验证,凭据提供模型,Windows 登录系统,U 盘锁,强身份认证
中图法分类号 TP319 **文献标识码** A

Design and Implementation of Windows Credential Provider Logon System Based on USB Key

YANG Hai[1] ZHAO Wen-tao[1] ZHANG Nai-qian[2] FAN Si-jiang[1]
(College of Computer Science, National University of Defense Technology, Changsha 410073, China)[1]
(College of Opto-electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)[2]

Abstract Windows operating system is widely used nowadays and the security of its login system has become the issue people concerned. We first analyzed and compared the security of GINA login module and Credential Provider login module, then proposed the idea of a design of Windows Credential Provider login system based on USB key, which perfectly combines the superiority of Credential Provider login module and USB key, improving the safety of traditional way of login by using user name and password. We developed our system based on windows 7, choosed USB key3000D as development platform. The system was developed based on the COM library of Windows Credential Provider.

Keywords GINA, Windows credential provider, Windows logon system, USB key, Strong identity authentication

Windows 操作系统的登录安全一直是人们广为关注的问题,目前应用最广的是传统的基于"用户名+密码"的登录方式。这种登录方式虽可以通过密码进行身份认证,提供一定程度的计算机使用安全保障,但用户密码极易被窃取,对合法用户也存在密码遗忘的危险。通过结合第三方身份认证方式等多种因素,基于硬件的进行身份认证,可以有效地提高操作系统的安全性[1]。随着 Windows 操作系统的不断发展,Windows 操作系统登录模型也在不断升级改进。在 Windows NT/2000/XP 系列系统中,Windows 采用的是交互式登录支持的 GINA(图形标志与身份验证)登录模型。时向卫[2]等人设计了基于 GINA 登录模型的 USB Key 登录方式,万海山[3]等人基于 Windows 2000/NT 系统对 GINA 登录模型进行了细致研究,具有一定的应用前景。在 Windows 7/8 系列系统中,微软采用了 Credential Provider(凭据提供)登录模型取代了 GINA 登录模型。

1 Windows 登录模型分析

1.1 GINA 登录模型简介

Windows NT/2000/XP 系统的交互式登录方式是通过 Winlogon 可执行模块(Graphical Identification and Authentication, GINA)登录模型、安全账号管理数据库(Security Accounts Management, SAM)和本地安全授权机构(Local Security Authority, LSA)模块相互调用和传输数据来完成安全登录的,具体过程如图 1 所示。

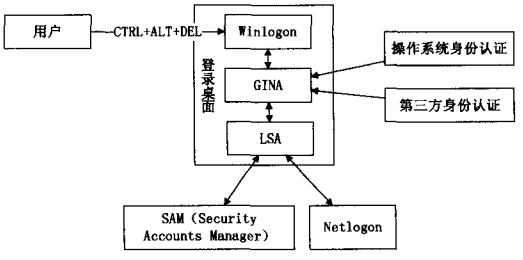


图 1 GINA 模型登录过程

其中,Winlogon 进程负责管理登录工作,交互式登录的支持靠 Winlogon 调用 GINA DLL 来实现,由于是交互式的登录方式,因此 Winlogon 进程在运行中需要不断加载 GINA DLL,并且只有在机器重启时才会卸载 GINA DLL,以确保没有内存泄漏。登录过程中首先创建 Winlogon 进程,初始化时

本文受国家大学生创新性实验计划项目(201390002054,201390002060)资助。

杨 海(1994—),女,CCF 学生会员,主要研究方向为信息安全,E-mail:zonga_cn@foxmail.com;赵文涛(1973—),男,教授,硕士生导师,主要研究方向为信息系统安全、网络安全;张乃千(1993—),男,CCF 学生会员,主要研究方向为信息安全;番丝江(1993—),男,主要研究方向为信息安全。

会在系统中注册一个 SAS(Secure Attention Sequence——安全警告序列)。SAS 是一组组合键,默认情况下为 Ctrl+Alt+Delete。它的作用是确保用户交互式登录时输入的信息被系统所接受,而不会被其他程序所获取。当Winlogon注册了SAS后,它就调用 GINA 生成 3 个桌面系统,分别是 Winlogon 桌面、应用程序桌面和屏幕保护桌面,登录身份的验证则全部由 GINA 登录模型实现。GINA 登录模型执行与用户身份识别和认证策略有关的操作过程包括:检测安全警告序列(Secure Attention Sequence,SAS)的发生状态;在没有用户登录时,负责收集用户身份验证信息;在用户登录时,进行用户身份验证;为用户创建初始化进程等。

计算机启动后,操作系统首先加载所有自启动服务,之后 Winlogon 进程加载 GINA 模型。在没有用户身份验证时,调用 GINA 模型的 WlxDisplaySASNotice 函数创建对话窗口,提示用户按 Ctrl+Alt+Del 继续操作。当用户按下这 3 个组合键时,Winlogon 会收到 SAS 并调用 GINA 模型的 WlxLoggedOutSAS 函数邀请用户输入用户名和密码信息。在用户身份验证成功后,如果用户锁定计算机,Winlogon 会调用 GINA 模型的 WlxDisplayLockedNotice 函数完成锁定;当用户选择解锁时,Winlogon 会接受到 SAS 并调用 GINA 模型的 WlxWkstaLockedSAS 进行用户身份验证。

1.2 凭据提供登录模型简介

从 Windows Vista 系统开始,由于 GINA 登录模型一向被开发人员难以理解和实现以及昂贵的 Microsoft 支持费用而广为诟病,因此 Windows 推出了全新的 Credential Provider(凭据提供)登录模型来代替传统的 GINA 登录模型。凭据提供登录模型的原理如图 2 所示,它是一个全新的 COM 组件,可以从底层实现多种身份认证方式的同时支持,每种认证方式对应一个凭据提供程序,这些凭据提供程序都被内置在 LogonUI 组件之中,用于向 LogonUI 提供对应的用户身份信息。LogonUI 是 Windows 7/8 系统中的新组件,可以替代 GINA 登录模型提供的登录界面功能,这样可以避免登录界面由第三方组件来完成而带来的登录过程的安全风险。

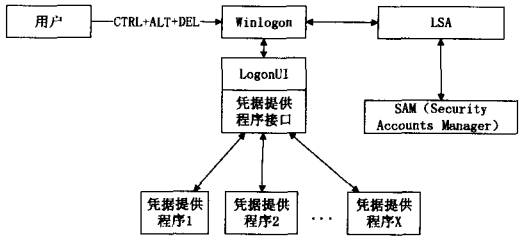


图 2 凭据提供登录模型

LogonUI 的优点在于它是根据底层加载的 Credential Provider(凭据提供)登录模型所定制的 UI 界面,将登录界面内嵌于登录桌面实现二者合为一体,以便于凭据提供程序收集所需要的用户身份信息。

在 Windows 7/8 系统登录过程中,系统建立了一个专门的会话边界将所有计算机系统进程与用户进程隔离,并通过严格控制内核全局命名空间来提高用户登录的安全性。Windows 7/8 登录体系结构如图 3 所示。

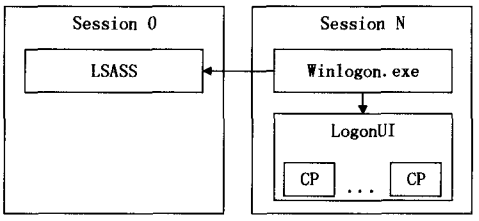


图 3 Windows 7/8 登录体系结构

在 Windows 7/8 登录体系中,每一个登录会话都会有一个专门的 Winlogon 实例[4],多个凭据提供程序通过 LogonUI 进程加载后与 Winlogon 进行交互通讯,再由 Winlogon 与会话 0 层进行交互通讯。在 Windows 7/8 登录体系中,"凭据提供程序"体系结构要求每个提供程序都要列举说明它所需要的 UI 元素。例如,在某个指定的方案中,提供程序可能会向 LogonUI 表明它需要两个编辑框、两个标题、一个复选框和一个位图。然后,LogonUI 为凭据提供程序显示这些控件。通过统一的开发模块可以简化用户的开发流程,用一致的外观和方法来广泛支持不断修改完善的用户验证方案,实现一致的外观表现,这增加了开发的稳定性以及避免了兼容性问题。

1.3 GINA 登录模型与凭据提供登录模型的比较

与 Windows 7/8 的登录方式类似,GINA 登录模型中,每一个会话也都有一个 Winlogon 实例来实现会话的交互式登录,但 Winlogon 实例的实现过程不同。GINA 模型的安全体系结构如图 4 所示。

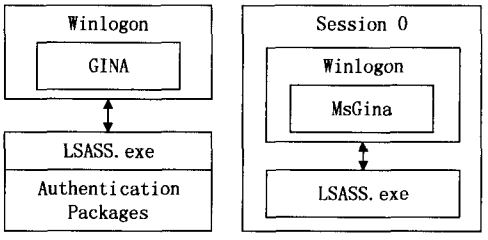


图 4 GINA 登录体系结构图

与 Credential Provider(凭据提供)登录模型相比较,在 GINA 登录模型中,会话 0 层一直负责执行交互式登录并承载着运行系统服务等关键进程。而在 Windows 7/8 登录体系中,会话 0 层不再用于交互式登录[5]。其中一个明显的变化是,在 Windows 7/8 系统中,会话 0 层没有 Winlogon,而是增添了 LogonUI 模块,会话 0 层只包含系统服务而不再负责交互式登录。用户登录会话与系统服务分离,系统服务不再需要与桌面进行交互。

因此,凭据提供登录模型有效避免了 GINA 登录模型的复杂繁琐,开发第三方认证时无需对函数进行重写,开发过程更加易用、安全。GINA 登录模型需要直接与 Winlogon 交互信息,用户界面设计复杂,第三方认证开发时负担极大[6]。凭据提供登录模型只需要选择并完成程序中相应 UI 元素的注册即可,用户的体验更为一致。因此,凭据提供登录模型具有极大的进步和优点。Windows 2000/XP 系统登录中使用的 GINA 登录模型在理解程度、开发难度上存在问题,且用户难以上手,这影响了多种登录系统的普及使用。改进后的 Windows 7/8 系统中的 Credential Provider(凭据提供)登录模型为用户提供了更好的发环境和更安全的登录界面,具有更广阔的应用前景。

2 基于 USB Key 系统登录的设计原理

目前，Windows 操作系统已经得到了广泛的使用，为了提高系统使用的安全等级，在原有的基于“用户名＋密码”登录方式的基础上，又出现了结合第三方身份认证方式的多因素强身份认证系统，USB Key 是第三方认证方式的一种，通过分析其独特的应用优势，可以将其与 Windows Credential Provider(凭据提供)登录模型相结合来为用户提供安全等级更高的登录系统方式。

2.1 第三方认证方式简介

2.1.1 基于指纹特征的身份认证系统

指纹特征识别技术是最早使用的、目前较为成熟的模式识别技术[7]，主要利用传感器技术、生物电子技术和数字图像处理、模式识别算法对人体的指纹信息进行解析判读。指纹识别技术的算法可分为：图像预处理、特征提取和特征比对[8]。利用指纹特征识别进行身份认证，计算机必须对输入的指纹图像进行分类、定位、提取等预处理操作，之后再根据提取的特征进行指纹比对。这种身份认证方式的优点包括：指纹身份的唯一性和不变性、采集终端易集成、指纹识别算法较为成熟等，因此其也在电子商务、公安、医疗等领域得到了广泛的应用。但由于计算机在进行指纹处理时，只能提取、处理指纹的有限特征信息，比对算法的精确度有待提高，识别准确性尚未达到 100%[9]；且其在系统登录时需要占用一定资源来完成认证过程，指纹信息容易伪造，因此这并不是最安全的身份认证系统。

2.1.2 基于动态口令的身份认证系统

动态口令是通过使用动态令牌根据时间、使用次数等要素而不断产生的、随机变化的、无重复的口令密码，该口令密码的安全性较高，每个登录密码只能使用一次。动态口令主要解决了“用户名＋密码”登录方式中口令易被猜解、难以记忆等缺点。基于动态口令的身份认证系统主要包括挑战/应答方式和时钟同步机制，采取一次一密机制[10]，在下一个动态口令生成之前，用户当前使用的动态口令是唯一有效的口令密码。由于每次使用的口令密码都不同，即使口令被截取也不存在安全隐患。基于动态口令的身份认证系统可以有效地提高系统登录的机密性、完整性、不可依赖性[10]，但由于动态令牌技术需要用户提前熟悉掌握，每次登录存在延时，因此限制了它的使用。

2.1.3 基于笔迹信息的身份认证系统

笔迹鉴别技术是生物识别技术的一个分支，主要利用人的手写笔迹信息进行身份鉴别。由于人体笔迹信息的稳定性和广泛的行为特征性，因此该技术被广泛应用在政府部门、公安法律、贸易金融领域。笔迹鉴别的主要过程包括：笔迹特征的表示与提取、笔迹特征的初分析和预处理、图像纹理特征提取和样本信息分析比较等。进行笔迹信息鉴别时，不要求用户每次必须书写相同的信息，经过改进优化的笔迹信息识别系统识别精度可以达到 97%以上[11]。基于笔迹信息的身份认证系统已经做到了系统设计，预期其会有广泛的应用前景。

2.1.4 基于 USB Key 的身份认证系统

USB Key 由 CPU、COS(片上操作系统)和 USB 接口模块 3 部分组成[12]，采用内部特定命令格式，可以同时进行加解密运算，可以有效防止用户信息泄漏[13]。USB Key 中存储用户的数字证书、密钥等身份认证信息，具有成本低、易携带、专人专用、安全性高等特点。使用 USB Key 进行登录时，用户必须插入正确的 USB Key，系统通过读取 USB Key 中的用户身份信息来判断用户身份。进行 USB Key 管理时，需要将用户的用户名和密码存储在用户专有 USB Key 介质中，并配置好正确的 PIN 码。

由于 USB Key 内部采用专有格式存储用户信息，因此即使用户本人也无法直接读写相关敏感信息，这极大地提高了登录系统的安全性，可以有效防止用户信息的泄露和伪造。相比于采用智能卡等其他身份认证系统，USB Key 不需要额外配备专用设备，不需要加载专门驱动信息，内部存储更加稳定高效，具有很好的应用前景。经过以上考虑，我们选用 USB Key 作为系统登录的身份认证部分。

2.2 基于 USB Key 登录系统的基本原理

基于 USB Key 的 Windows 凭据提供系统登录流程如图 5 所示。

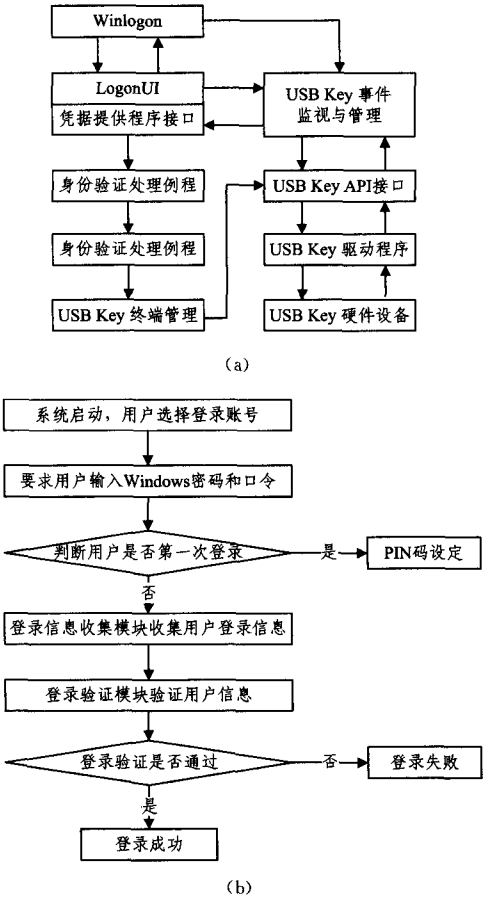


图 5 USB Key Windows 开机登录流程

当 Windows 系统启动到登录界面时，用户插入 USB Key 设备，凭据提供模型检测到 USB Key 并通过 LogonUI 发送通讯给 Winlogon，Winlogon 通知 USB Key 内部的事件监视与管理模块，获得 USB Key 事件监视与管理例程并弹出 PIN 码输入对话框以获取用户输入的 PIN 码。当 USB Key API 函数接口接收到 PIN 码后通过 USB Key 驱动层面传递给 USB Key 中的认证 PIN 码进行核对比较，并将比较的结果反馈给 Winlogon。如果验证失败，则再次对用户输入的 PIN 码进行验证，若验证 3 次 PIN 码都输入错误，则锁定计算机；若正确则通过验证完成 Windows 开机登录。

凭据提供模型通过调用身份验证处理机制发送从 USB Key 中获得的用户名和密码操作请求，USB Key 终端管理程序将该请求传递给 USB Key API 接口，接口与 USB Key 驱动程序通信并将其传递给 USB Key 硬件设备端。USB Key 从设备内读取用户名和密码后返回给凭据提供模块并进行 LSA 验证，通过后即可完成系统登录。USB Key 在设备内存储用户名和密码时采用了加密算法，可以保证用户信息的安全性。

3 基于 USB Key 系统登录的实现

3.1 USB Key 的开发平台及初始化操作

我们使用的是东莞市乐程电脑软件有限公司的 UKey3000D 身份认证锁，开发环境为 C# 平台。UKey3000D 使用增强型 TEA 算法和 SM2 国密算法，拥有全球唯一 ID，具有高安全性和可扩充性好等特点。它的内部结构特点如图 6 所示。

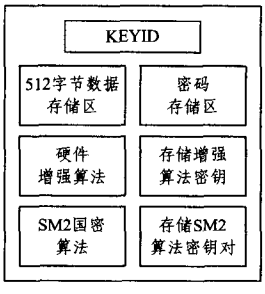


图 6 UKey3000D 内部结构特点

用户名和密码绑定服务程序主要包括两个部分：用户打开用户名密码绑定程序后，要求输入 USB Key 的 PIN 码值，并对 PIN 码值进行身份校验，完成用户身份认证过程；校验用户身份后，运行用户登录信息绑定模块，将用户录入的用户名和密码信息进行绑定。一组用户名和密码，智能地对应一个特定的 Windows 登录凭据信息。用户完成信息绑定后，登录凭据信息将通过 USB Key 的 API 加密保存到 USB Key 内部存储系统中，其中加密密钥是 USB Key 初始化时写入的密钥。

USB Key 初始化操作主要包括绑定用户所需要的用户名和密码。依靠用户名和密码绑定程序，可以实现输入系统的用户名和密码并将该信息写入 USB Key 设备中，实现 USB Key 的智能登录。基于 USB Key 内部存储功能，完成绑定的用户名和密码将加密保存在 USB Key 设备中，除非删除或重新绑定，否则将长期有效。加密方式如下：使用 SM2 公钥加密算法，加密结果由 3 部分组成：1）SM2 加密过程使用了随机数发生器来产生随机数并计算出曲线点 2 个 32bytes 的大数；2）则是真正的密文，这是对明文的加密结果，长度和明文一样，而加密过程中使用的公钥则是使用用户需要输入的 PIN 码作为参数；3）是杂凑值，用来校验数据。

Windows Credential Provider COM 不存在自动判断用户修改密码而导致绑定关系改变的接口，因此需要安装用户名和密码绑定辅助服务程序。该服务可以轮询检查用户名和密码信息是否处于有效状态，并在绑定关系发生变化后完成 USB Key 的重新绑定。

3.2 基于 COM 库的程序设计

Windows Credential Provider COM 库包括自定义用户登录的界面接口模块和收集、提交用户登录信息的登录凭据提供模块。这里我们尝试通过注册新的 COM 库的方式将 Credential Provider 注册到 Windows 操作系统中，在保留原有 Credential Provider 模块的同时实现用户同时选择两种登录方式登录的智能程序，即用户可以选择通过传统 Windows 登录方式或只用 USB Key 直接登录。

当系统启动到登录界面时，可以通过 FindPort 函数查找系统中是否存在第 N 个 USB Key 设备，如果存在，则返回该加密锁所在的设备路径，并通过 GetID 函数返回指定 USB Key 设备路径的加密锁的 ID 号，加密锁的 ID 号由 8 个字节组成。可以使用 YReadEx 函数读取 USB Key 存储的信息，使用 YWriteEx 函数实现用户登录信息的写入。当用户需要修改 USB Key 的 PIN 码时，可以调用 YtSetPin 函数实现 PIN 码的修改。

通过 Windows Credential Provider 可实现定制登录标题图片和设置登录凭据按钮等功能。设置定制登录标题图片可将图片信息以资源的方式插入到 DLL 中，可设置 IDB_TILE_IMAGE 的 ICredentialProviderCredential 接口代码：

```
HBITMAP kbmp=LoadBitmap(HINST_THISDLL,MAKEINTRESOURCE(IDB_TILE_IMAGE));
*phbmp=kbmp;
```

可以通过修改 COM 库来实现插入 USB Key 后 Windows 自动提醒使用 USB Key 登录的功能，参考代码如下：

```
static const FIELD_STATE_PAIR s_rgMessageFieldStatePairs[] =
{CPFS_DISPLAY_IN_BOTH,CPFIS_NONE},
{CPFS_DISPLAY_IN_DESELECTED_TILE,CPFIS_NONE},
};
```

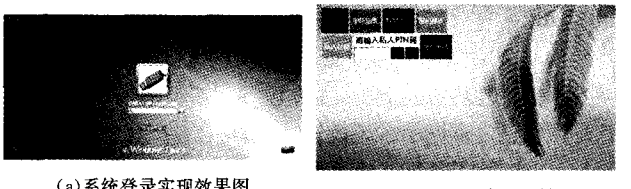
用户在完成 PIN 码输入后，USB Key 调用 ICredentialProviderCredential::GetSerialization 函数检验 PIN 码输入是否正确，若校验成功，即解密并读取 USB Key 中加密保存的用户登录信息，并返回 GetSerialization 函数的输出参数，从而完成 Windows 的登录。

完成 Windows Credential Provider COM 的定制后，需要将该部分程序拷贝到 Windows 系统盘目录 System32 下，并通过注册表注册到 Windows 系统，即可实现开机 USB Key 的登录。需要注册的位置包括：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Authentication\Credential Providers\]
[HKEY_CLASSES_ROOT\CLSID\]
[HKEY_CLASSES_ROOT\CLSID\**\InprocServer32]
```

3.3 登录系统实现效果图

基于以上的系统设计，我们实现了一个基于 USB Key 的 Windows 凭据提供登录平台。实现效果如图 7(a)所示。在选择使用 USB Key 登录后，会看到专用的登录界面，用户输入 PIN 码后即可完成系统登录。除此以外，我们还结合系统 USB Key 内部加密算法设计了用户平台，用来进行数据加密操作，实现效果如图 7(b)所示。



(a)系统登录实现效果图　(b)用户平台实现效果图

图 7

(下转第 398 页)

(1)数据复制。当台站系统储存数据至数据库时,同步监听器复制其数据,通过 ESB 将数据存储到台站系统的数据交换区中,并修改相应的数据增量表。同步监听器同时更新台站系统以及数据共享中心的数据字段表。

(2)数据清洗。同步控制器通过匹配共享数据中心的数据字段表,将数据交换区中的数据按照数据清洗规则进行清洗,并存储到共享数据中心。

(3)数据分发。同步控制器将共享数据中心增量表中的数据匹配每个应用系统的数据字段表,并整理每个系统需要更新的数据再推送至相应应用系统的数据交换区中。

(4)数据传送。若应用系统没有对需要同步数据的访问请求,则按照同步控制器之前设定好的同步时间间隔将数据交换区中的数据统一同步传送至相应的应用系统数据库。这一过程也由同步控制器完成。如果有对为同步数据的访问请求,则通过访问控制器暂停对数据库的访问,直到数据同步完成。

同步类图如图 4 所示。

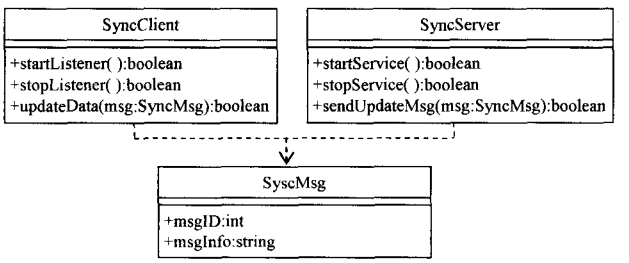


图 4 同步类图

结束语 基于 ESB 与 Agent 的共享数据中心同步模型,可以有效地解决云南省无线电监测中心当前的多系统多数据库数据同步问题,降低耦合性,便于系统的更新与扩展。访问控制器在控制系统访问数据库的过程中可能造成的延迟对用户体验的影响,有待进一步研究。

参 考 文 献

[1] 黄序鑫,聂瑞华,罗辉琼,等. 基于 SOA 的数据同步技术研究与实现[J]. 计算机工程与设计,2009(14):3338-3340

[2] 邵欢庆,康建初. 企业服务总线的研究与应用[J]. 计算机工程,2007,33(2):220-222

[3] Gartner. Service-Oriented Architecture Scenario [R]. Technical report. 2003

[4] 邢少敏,周伯生. SOA 研究进展[J]. 计算机科学,2008,35(9):13-20

[5] 帅晓华. 基于 WebService 的应用系统数据同步的实现[J]. 决策与信息,2008(11)

[6] 邱宁,吕何新,冯淑娟. 基于 Web Service 的数据一致性维护方法[J]. 计算机工程与设计,2006,27(14):2564-2565

[7] 黄安安,王丽芳,蒋泽军,等. 基于 ESB 的企业应用集成研究[J]. 微计算机应用,2007,28(9):965-970

[8] 李素萍. 分布式数据库的同步更新技术研究[J]. 中国科技信息,2008(16):94-95

[9] 汪雄杰,熊前兴. 基于 Mobile Agent 和 Web Service 的移动数据同步模型[J]. 计算机与数字工程,2010,38(4):78-81

[10] 蒋敏,董亚波,鲁东明. 一种基于 Agent 的数据同步方法[J]. 江南大学学报:自然科学版,2005,4(6)

[11] 张芬琦,李仰东,崔丽萍. 浅析 EAI 技术[J]. 山西通信科技,2004,25(2):3-7

[12] 肖万贤,刘江宁. 企业数据集成模型的研究[J]. 计算机工程与科学,2004,26(5):49-51

(上接第 374 页)

结束语 本文通过分析比较 Windows 的 GINA(图形标志与身份验证)登录模型和 Credential Provider(凭据提供)登录模型的安全性,采用 Windows 凭据提供模型结合 USB Key 第三方认证方式,设计并实现了基于 USB Key 的 Windows 凭据提供登录系统。这种登录系统提高了传统"用户名+密码"登录方式的安全程度,是符合当今技术发展趋势和时代要求的产物,具有成本低、易携带、专人专用、可靠性高等特点,是未来大数据时代数据安全、人性化使用、跨多应用密码存储的一个重要发展方向,且实现简单,灵活方便,具有良好的应用前景。

参 考 文 献

[1] 韩君. 基于 USB Key 的 Windows 身份认证与访问控制研究[D]. 武汉:武汉大学,2004

[2] 时向卫,李峥,张少武. 基于 Usbkey 的 Windows 登录系统的设计与实现[J]. 计算机工程与设计,2008,10:2483-2485

[3] 万海山,李国,李大兴. 使用 USB KEY 控制 Windows 2000/NT 开机登录[J]. 计算机应用,2003(S1):254-255

[4] Microsoft. MSDN Library[EB/OL]. [2014-4-2]. http://msdn.microsoft.com/library/

[5] Michael Muckin, Lockheed Martin. Windows Vista Security Internals [J/OL]. [2014-4-2]. http://www.blackhat.com/presentations/bh-dc-09/Muckin/BlackHat-DC-09-Muckin-vista-security-internals.pdf

[6] 李春林,王丽芳,蒋泽军,等. 基于身份认证技术安全体系的研究[J]. 微电子学与计算机,2005,04:8-11,14

[7] 戴平阳. 指纹识别技术研究进展[J]. 厦门大学学报:自然科学版,2002,06:750-755

[8] 卢朝阳,张岗山,刘琳. 指纹识别系统性能评价方法[J]. 西安电子科技大学学报,2002,6:804-808

[9] 吴教育,曾东海. 基于指纹识别的网络身份认证系统[J]. 计算机技术与发展,2007,1:170-171,176

[10] 史晓影. 基于动态口令身份认证系统的设计与实现[J]. 办公自动化,2007,2:19-20

[11] 刘宏,李锦涛,崔国勤,等. 基于 SVM 和纹理的笔迹鉴别方法[J]. 计算机辅助设计与图形学学报,2003,12:1479-1484

[12] Microsoft. Smart card reference [DB/OL]. [2014-4-2]. http://www.msdn.microsoft.com/library/

[13] 杨帆. USB KEY 体系研究与技术实现[D]. 武汉:武汉大学,2004