软件保护策略研究

常贯明[1],武 波[1],陈保娣[2]
(1.西安电子科技大学 软件工程研究所,陕西 西安 710071;
2.太原科技大学 计算机应用与系统仿真研究所,山西 太原 030024)

摘 要:针对Windows系统注册表的一些缺点,提出一种新的注册表机制,它以Socket通信和公开密钥加密技术为基础,从而实现一个通用软件保护系统。操作系统的一个守护进程开启监听端口,应用程序通过Socket和该守护进程进行通信,从而获取和存储这个应用程序相关的信息,该机制类似于Windows系统注册表,但是它与注册表机制有本质不同,从本质上来看,它更类似于一个小型数据库系统。

关键词:注册表;软件;保护策略;公开密钥;全球唯一标识符
中图分类号:TP311 **文献标识码**:A **文章编号**:1673-629X(2009)05-0013-03

Study on Software Protection Strategy

CHANG Guan-ming[1], WU Bo[1], CHEN Bao-di[2]
(1. Software Engineering Institute, Xidian University, Xi'an 710071, China;
2. Institute of System Simulation & Computer Application, Taiyuan Univ. of Sci. and Tech., Taiyuan 030024, China)

Abstract: In allusion to drawbacks of Windows system registry table, a new kind of registry table mechanism based on communication via a socket and public key encryption technology is proposed, so a universal software protection system can be implemented. While a daemon process of operating system listening on a port, an application communicates with it via a socket, so the application can get and set some related information. This mechanism is similar to the Windows system registry table, but it has the essence dissimilarity with the registry table mechanism. From the essence, it is more similar to a small scale database system.

Key words: registry table; software; protection strategy; public key; global unique identifier

0 引 言

随着计算机逐渐普及,软件业也得到了迅速的发展,软件开发者为了维护自身以及软件购买人的利益,保护科研成果、技术和版权,有必要对软件进行加密保护。而另有一些软件人员为提高自己的编程水平或其他目的,会针对出现的保护方式进行跟踪分析,找出相应的方法或制作出破解工具软件破解软件的保护。这样,随着软件业的发展,相互对立的软件保护技术和破解技术也发展壮大了起来。

软件保护即如何防止合法软件被盗版[1~5],对于应用软件常用的保护策略有软加密和硬加密两种。软加密指通过程序本身防止解密而进行限制性保护,硬加密是通过外置硬件对软件进行授权的加密方式。现有的软加密保护策略有:时间限制保护;菜单功能限制保护;注册文件保护;警告窗口保护;文件加壳保护等。硬加密最常见的就是"加密狗"技术,文中研究的是软加密技术。基于软加密的保护方式可以分为两大类:第一类,程序运行过程中,必须在本地计算机保存有关注册认证的信息;第二类是保存到远程主机。对于第一类方法,一般是把相关信息保存到系统注册表中,由于Windows系统注册表本身具有的致命缺陷(明文存放),这使得用户可以任意修改注册表。如果能够提供一种比系统注册表更安全的机制,则能避免这种事情的发生。文中借鉴了数据库系统的基本原理[6],利用公开密钥算法[7~10]设计并实现了一个实用的软件保护系统。

收稿日期:2008-08-13
基金项目:国家部委重点基金项目(9140A24070106DZ01);教育部重点科研项目(204018);山西省自然科学基金项目(2007011046)
作者简介:常贯明(1981-),男,安徽临泉人,硕士研究生,研究方向为软件工程理论与应用;武 波,教授,硕士生导师,研究方向为软件工程和软件设计理论与应用。

1 软件注册认证系统设计

1.1 系统架构设计

在操作系统中实现一个软件注册认证系统,它由

两个部分构成:系统守护进程 Daemon 和注册表文件 AppDB(经过加密的)。这个注册表文件与 Daemon 拥有相同的 GUID(全球唯一标识符),Daemon 和 AppDB 构成了一个小型数据库系统,应用程序 AP 就是该数据库系统的一个用户,AP 的 GUID 就是它在数据库系统中的用户名。守护进程 Daemon 和应用程序 AP 通过 Socket 握手通信,即 AP 发出请求,Daemon 必须回应,通信信息用公开密钥加密算法加密后传输。

数据库文件 AppDB(解密后)的结构与 INI 配置文件非常相似,每个应用程序 AP 占一个节(Section),AP 的 GUID 就是节名,一个节包含几个键(Key),具体键的名称以及键的个数完全由应用程序 AP 自己决定。其中[main]节对应的是守护进程 Daemon,Daemon 启动的时候,首先读取 AppDB 的[main]节信息:(1)比较其中的 GUID 值和 Daemon 的 GUID 值,如果二者不相同,则终止该进程;(2)比较 LastTime 值和现在系统时间,如果二者相差超过 MAX 小时,则终止该进程。

数据库文件 AppDB 解密后的文件结构示例如下:

```
[main]
GUID=444FD84C-534A-4a71-92C8-AB7DD04B915F
LastTime=2007-05-01-08-00-00
[BBE36528-67E1-4d10-B337-233D6DF91FEF]
AppName=电话银行系统
AppVendor=SEI of Xidian University
AppVersion=1.0.0
AppPassword=123456
AppExpireDate=2008-05-01-08-00-00
[741F0145-59FB-421a-B68D-15D9AB09955D]
AppName=呼叫中心系统
AppPassword=654321
AppExpireDate=2009-05-01-08-00-00
[end]
```

1.2 通信协议设计

应用程序 AP 和 Daemon 之间的通信协议格式如图 1,图 2 所示,Daemon 和 AP 的消息中的明文传输部分是它们的公钥和协议结束符,消息中的协议结束符是 CRLF,即 C/C++ 语言中的 \r\n。

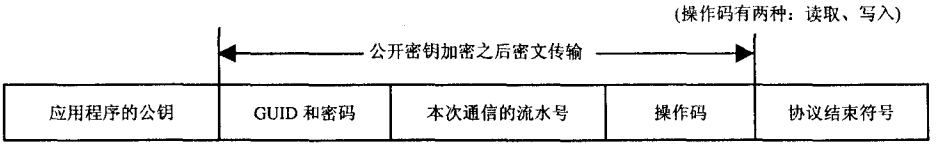

图 1 AP 到 Daemon 的消息

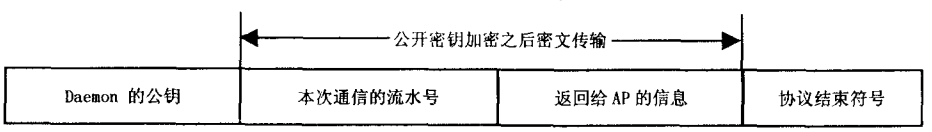

图 2 Daemon 到 AP 的消息

举例说明 AP 与 Daemon 之间的通信过程(如图 3 所示):

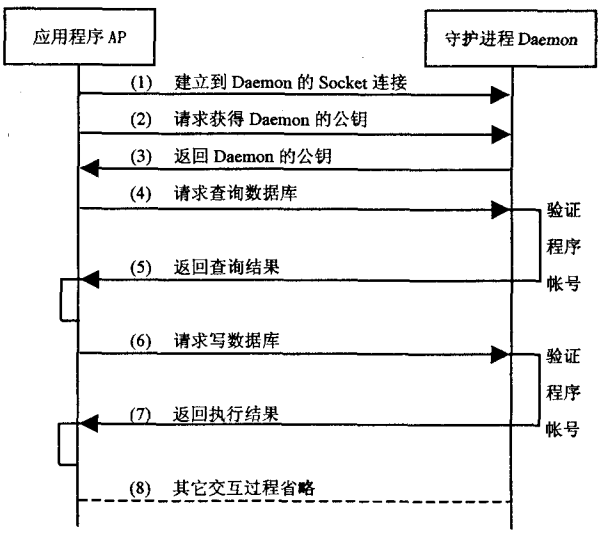

图 3 应用程序 AP 和 Daemon 之间的通信

(1) 操作系统启动时启动 Daemon,Daemon 检验数据库文件 AppDB 的合法性,如果不合法则终止运行。

(2) 应用程序 AP 每次启动时,首先建立到 Daemon 的 Sokect 连接,若连接建立失败则终止程序的运行。

(3) AP 向 Daemon 发送获得 Daemon 公钥的请求。

(4) Daemon 返回它的公钥给 AP。

(5) AP 按照约定的消息格式封装请求消息,并用 Daemon 的公钥把请求消息加密后发送给 Daemon。

(6) Daemon 收到消息后,把消息解密后,根据消息中 GUID 号码和密码验证身份,如果验证通过则查询数据库文件 AppDB,然后把查询到的信息用 AP 的公钥加密后返回给应用程序 AP,如果身份验证未通过则返回失败信息。

(7) 如果 AP 没有收到 Daemon 的回应消息,则表明通信失败,或者消息被拦截,则 AP 终止执行。如果 AP 收到 Daemon 的回应消息,例如,协议字段"返回给 AP 的信息"中存放的是程序已经运行了多少次,AP 可以根据这个信息做相应的处理。

(8) AP 向 Daemon 发送写入信息的请求。

(9) Daemon 收到消息后,把消息解密后,根据消息中 GUID 号码和密码验证身份,如果验证通过则把信息写入数据库文件

AppDB,然后把操作成功的信息用 AP 的公钥加密后返回给应用程序 AP,如果身份验证未通过则返回失败信息。

(10) 如果 AP 没有收到 Daemon 的回应消息,则表明通信失败,或者消息被拦截,则 AP 终止执行。如果 AP 收到 Daemon 的回应消息,则 AP 继续运行下去。

1.3 抗破解性能分析

破解方法有如下几种:

1)截获 AP 和 Daemon 之间的通信消息,然后破解。

这个方法难度很大,这相当于破解公开密钥加密算法,此破解方法基本不可行。

2)截获 Daemon 发送给 AP 的通信消息,把这个信息 OldMsg 保存起来,以后每次 AP 向 Daemon 发送请求都被破解进程 Cracker 截获并抛弃掉,然后把以前保留的消息 OldMsg 发送给 AP。

因为 AP 与 Daemon 的每次通信消息中都有一个流水号,每次通信的流水号都不相同,AP 收到消息后,首先把收到消息的流水号跟它发出请求消息中的流水号做比较,发现不同则终止该进程。此破解方法根本不可行。

3)每次截获 AP 发送给 Daemon 的请求消息,并抛弃之。

AP 与 Daemon 之间是握手协议通信,对于 AP 的请求,Daemon 必须回应,若 Daemon 没有回应,则 AP 认定出现错误,并终止该进程。此破解方法也是根本不可行。

4)备份这个系统的数据库文件 AppDB。

Daemon 进程每隔一个小时,从 AppDB 的[main]节中读取一个属性值 LastTime(时间戳),同时写进去一个新的时间戳 NowTime,如果 NowTime 和 LastTime 的时间差超过 MAX 小时,就表明有破解者把数据库文件替换了。这种防范策略有一个缺陷就是:用户的系统关机时间不能超过 MAX 小时,可以适当增大 MAX 的值来放宽限制,这使得破解者在 MAX 小时内的备份才有效。

5)备份整个操作系统,从而达到恢复到原始状态的目的。

这种破解方法是可行的,但是,在操作系统被恢复后,还必须修改系统时间,否则 Daemon 进程肯定启动不起来,正如第 4)条的情况。

从以上分析可以得出如下结论:

(1) 缺点:这种防范策略可以被破解,尽管破解有一定的难度。

(2) 优点:该系统可以为多个软件提供软件版权的保护,而不必为每个软件做一个保护系统。

2 结束语

计算机网络的面世将人类带入了信息互联时代,也随之带来了计算机安全和网络安全问题,而最终的问题是软件的安全问题。因而软件保护技术一直是一个研究热点,它是以加密技术为基础的,而对于任何加密方法,必然有破解方法,不论采用何种保护方式,可执行程序都可以被黑客用 SoftICE 等工具调试跟踪,找到判断代码处,通过修改可执行文件,跳过此段代码,达到破解的目的,虽然采取一定的反跟踪、反调试技术,可以加大破解难度,但最终还是可以被破解。这使得对于软件版权的保护仅仅靠程序逻辑是不行的,必然要靠社会和法律来辅助保护。

参考文献:

[1] 看　雪.加密与解密——软件保护技术及完全解决方案[M].北京:电子工业出版社,2001.

[2] 周晓东,卢东明.软件保护技术[M].北京:清华大学出版社,1994.

[3] 郭　勇,孔宝根.软件保护及破解策略[J].航空维修与工程,2004(3):37-39.

[4] 罗　宏,蒋剑琴,曾庆凯.用于软件保护的代码混淆技术[J].计算机工程,2006(11):177-179.

[5] 祁　明,容叶飞.一种新型软件保护方法的设计与分析[J].微型电脑应用,2000(12):8-10.

[6] 王　珊,萨师煊.数据库系统概论[M].北京:高等教育出版社,2006.

[7] Peltier T R, Raton B. Information security policies and procedures :a practitioner's reference[M]. Florida :Auerbach Publications,2004.

[8] Garrett P, Lieman D. Public-key Cryptography[J]. American Mathematical Society,2003(5):13-14.

[9] 周玉洁,冯登国.公开密钥密码算法及其快速实现[M].北京:国防工业出版社,2002.

[10] Saloma A.公钥密码学[M].丁存生,单炜娟译.北京:国防工业出版社,1998.

(上接第 12 页)

[6] 薛　冰,营作良.设计模式和数据持久层框架在 Web 系统中的应用[J].天津理工学院学报,2004,20(1):76-78.

[7] 田志魏.对象/关系映射持久化技术的研究及应用[J].微计算机信息,2008,3(3):177-178.

[8] 蒋　科.面向对象技术中 OR 映射框架的研究与应用[J].计算机技术与发展,2007,17(2):59-62.