数字签名（代码签名）流程

数字签名（代码签名）流程

Authenticode： 这里翻译为数字认证代码。
code sign： 字面的翻译为代码签名，但是通常的我们称为数字签名，以下的文中均称为数字签名。

一 数字认证码
如果你是软件开发人员，你可能已经知道windows系统和一些浏览器（例如IE，Firefox）使用一种称为数字认证代码的技术来标识软件的发行商，来检查软件没有被病毒影响。如果你的软件没有用数字认证代码签名，用户将会收到一个警告"此软件发行商不能被成功的验证，你是否要继续运行此软件"，很多的用户为了安全起见将放弃对此软件的使用。

如果你的软件是提供给专业的人员使用，结果肯能会更糟。许多公司的IT安全策略禁止没有用数字认证码签名的软件的运行。

同时微软Windows也使用数字签名证书来判断潜在的恶意软件。如果你的setup.exe没有进行数字认证证书的签名，你的软件的名誉将遭受损害。

在Vista系统增加UAC之后，情况变的更糟，如果你的软件没有使用数字认证证书签名，且在运行时需要管理员的权限，则会出现警告对话框"不可识别的程序想访问你的计算机"，这个时候很多的用户可能认为是病毒，会禁止使用你的软件。

二 数字认证码的原理

数字签名代码是一种技术，它使用数字证书来识别软件的发布商和使用hash算法来确保软件的完整性。数字签名使用公共密匙签名书法被创建，它使用两种不同的密匙：公共密匙和私有密匙，我们称其为密匙对。私有密匙一般为拥有者所有，公有密匙对所有的人都可见。

数字签名的过程本质上为：

签名软件对要签名的软件创建hash；

使用发布者的私有密匙来加密软件的hash；

被加密的hash和发布者的数字证书被插入到要签名的软件；

数字签名的验证过程本质上为：

用户对要验证的软件创建hash；

使用发布者的公共密匙来解密被加密的hash；

比较解密的hash和新获得的hash，如果匹配说明签名是正确的，软件没有被修改过；

三 数字签名
数字签名是对软件进行标识的一个流程，它通过对软件增加了发布商的信息来检查软件在发布后是否被修改或受病毒影响。在软件出售前进行签名已经成为了行业范围的专业实践。随着用户的安全意识的提高，现在越来越多的用户限制下载未签名的软件，因此作为专业的软件公司，在软件出售前进行签名已经成为必不可少的一步。

要进行数字签名，需要以下准备：

Mobile(1)
OtherLanguage(5)
perl(45)
Python(104)
SQL(13)
Web(9)
操作系统(4)
测试安装(1)
分布式(11)
好工具(19)
开源(4)
批处理/Shell(35)
软件架构(13)
新技术(18)
资料收集(27)

持续集成

没头脑的土豆

积分与排名

积分 - 877159

排名 - 95

最新评论

1. Re:python基础31[docstring]

如果给module增加docstring，该docstring必须位于文件的最前面。如果是类似# -*- coding:utf-8 -*-这样的语句是要放在docstring前面的吧。...

--捡了一棵小白菜

2. Re:Linux的inode的理解

棒棒的

--jellyabd

3. Re:Linux的inode的理解

超棒

1）数字证书和密码；
2）数字签名工具；
3）时间戳服务器的URL地址；

四 数字签名工具
数字签名工具， 微软提供了两套数字签名工具，

1）signcode.exe， 从1998年开始使用，随.NET Framework SDK发布。

signcode.exe 数字签名工具

makecert.exe 创建数字证书

cert2spc.exe 将数字证书转化为软件发布者证书格式

2）signtool.exe，随visualstudio 2005及其以后的版本发布。

signtool.exe 数字签名工具

makecert.exe 创建数字证书

cert2spc.exe 将数字证书转化为软件发布者证书格式

pvk2pfx.exe（pvkimprt.exe） 将私有的密匙和软件发布者证书合并为pfx文件，此文件将被signtool.exe使用

上面2中工具的不同是signcode.exe需要输入私有密匙和软件发布者证书（pvk和spc文件），signtool.exe只需要输入由pvk和spc合并产生的一个个人信息交互文件（pfx）。

五 获得数字证书

数字证书，你可以创建自己的数字证书来测试数字签名的流程，但是正式的软件发布，你需要向可信赖的证书颁发机构购买数字证书和密码，例如你可以向以下的证书机构购买Comodo, Globalsign, Thawte and Verisign。

创建自己的数字证书（用来测试）

使用如下命令来创建自己的数字证书：
makecert.exe -sv mykey.pvk -n "CN=Acme Software Inc." mycert.cer你可以将Acme Software Inc.替换为你自己公司的名字。如果mykey.pvk不存在的话，你会要求输入私有密匙的密码，密码可以为空。安全起见最好设置密码，否则别人拿到你的私有密匙后就可以签名了。在上面的命令后，产生了2个文件mykey.pvk和mycert.cer。接下来需要将数字证书（cer）转化为软件发布商证书（spc），命令如下：cert2spc.exe mycert.cer mycert.spc此过程中需要输入私有密匙的密码，创建完成后应该会生成mycert.spc文件，当数字签名时mycert.cer文件是不需要的。

六 对软件数字签名
时间戳服务器，你可以选择下列之一，
- http://timestamp.verisign.com/scripts/timstamp.dll
- http://timestamp.globalsign.com/scripts/timstamp.dll
- http://timestamp.comodoca.com/authenticode

1）使用signcode.exe,如下：
signcode.exe -t <timestamp URL> -spc mycert.spc -v mykey.pvk "<file to be signed>"进行数字签名的文件可以是.exe, .dll, .ocx 或者是其他的可执行文件。

2）使用signtool.exe，如下：

如果你没有pfx文件，需要使用以下的命令来将pvk和spc文件合并为pfx，如果没有设置密码的话必须使用pvkimprt.exe来合并。pvk2pfx.exe -pvk mykey.pvk -pi <password> -spc mycert.spc -pfx mycert.pfx -po <password>pvkimprt.exe -pfx mycert.spc mycert.pvksigntool.exe sign /f mycert.pfx /p <password> /t <timestamp URL> /v "<file to be signed>"
以下是使用signtool.exe签名的一个实例：
signtool.exe sign /f mycert.pfx /p <password> /t <timestamp URL> /v "<file to be signed>"

Here is the Sample Output:
The following certificate was selected:
Issued to: SID Software Inc.
Issued by: Thawte Code Signing CA

--cap_ljf

4. Re:Linux软连接和硬链接

通俗易懂啊，哈哈～

--mingc

5. Re:PDB文件：每个开发人员都必须知道的

不错

--HelloWorldGe

阅读排行榜

1. Linux软连接和硬链接(251856)
2. RSync实现文件备份同步(245380)
3. Jenkins入门总结(195062)
4. Linux的inode的理解(121304)
5. PDB文件：每个开发人员都必须知道的(119493)
6. vi/vim基本使用方法(96167)
7. VMWare网络设置的3中方式(94761)
8. Jenkins的配置(85563)
9. linux上安装配置vsftpd(74543)
10. JAVA的helloworld[转](66112)
11. [MySQL]WorkBench管理操作MySQL(59553)
12. mount命令（用来挂载硬盘或镜像等）(56677)
13. Maven与Ant比较(54931)
14. Jenkins master在windows上安装(53841)
15. Apache与Tomcat整合(53765)
16. ~~~Linux面试题汇总答案~~(52856)
17. 设置su和sudo为不需要密码(50839)
18. python实例32[简单的HttpServer](50395)
19. 免费好用的Diff和Merge工具大总结(48349)

Expires: 10/16/2011 2:17:15 AM
SHA1 hash: 4374SD894388B9H456E206124G06D9AV1535G12E

Done Adding Additional Store

Attempting to sign: jservice.exe
Successfully signed and timestamped: jservice.exe

Number of files successfully Signed: 1
Number of warnings: 0
Number of errors: 0

参考：
http://www.tech-pro.net/code-signing-for-developers.html
http://siddesh-bg.blogspot.com/2008/12/code-signing-process.html

Code-Signing Best Practices ：
http://msdn.microsoft.com/en-us/windows/hardware/gg487309.aspx

作者：iTech
出处：http://itech.cnblogs.com/
持续集成微信公众号ciandcd
持续集成总群172758282 加入QQ群
持续集成2群567940397 加入QQ群
持续集成招聘群567931165 加入QQ群
linux讨论总群426095548 加入QQ群
linux讨论2群483205747 加入QQ群

« 上一篇：Shutdown远程重启机器
» 下一篇：[BRE]软件构建发布自动化

posted @ 2011-07-21 18:08 iTech 阅读(11604) 评论(1) 编辑 收藏

评论列表

#1楼 2011-08-10 12:46 刺客之家

楼主总结的很全面，最近也在做这个，对pfx文件，数字签名，数字证书，CA等概念也有一些了解，看了楼主的文章，很多概念更清晰了

支持(0) 反对(0)

刷新评论 刷新页面 返回顶部

注册用户登录后才能发表评论，请 登录 或 注册，访问网站首页。

最新IT新闻:
· 霍炬：中文分析比特币最早文章之一是我写的 这是第二篇
· Opera 53开发者版上线：Speed Dial新增新闻栏目
· 微信发布谣言治理报告：辟谣中心全年科普4.9亿次
· 因为一张黑板Word图画 微软向加纳老师捐赠电脑
· 运营商被曝即将迎来大调整：流量不分省内省外
» 更多新闻...

最新知识库文章:
· 写给自学者的入门指南
· 和程序员谈恋爱
· 学会学习
· 优秀技术人的管理陷阱
· 作为一个程序员，数学对你到底有多重要
» 更多知识库文章...