

系统安全配置

杨波

yangbo@ccert.edu.cn

- 精简系统服务
- 访问控制
- 日志
- 恶意代码扫描
- 数据安全
- 备份
- 关注安全新闻和技术发展

精简系统服务

- 为什么要精简系统服务？
 - 操作系统厂商为了让产品提供较好的out-of-the-box体验，缺省启动了很多服务，这些服务不是所有实际场合都需要
 - 这些服务程序的缺陷或配置不当增加了系统被攻入的可能。
- 精简原则——最小化原则
 - 一个服务除非是必要的，否则应该禁用它。
 - 系统中安装和运行的服务越少，受攻击面就越小。

- 精简步骤：
 - 识别已启动的服务
 - 关闭不必要的服务

(如果不能关闭，则可以升级和封堵)

关闭： `services.msc`，控制面板，注册表

升级： 补丁，更新

封堵： 防火墙，IPSec Security Policy

Windows XP Pro.中可关闭的非基本性服务：

- Computer Browser： 计算机列表浏览
- Messenger： net send 信使服务
- Remote Registry： 远程注册表
- Server： 文件、打印机共享
- Terminal Services： 远程桌面、远程协助
- Windows Time： 日期、时间同步
- Wireless Zero Configuration: 无线网卡参数配置

- C:\WINDOWS>netstat -ano

- Active Connections

•	Proto	Local Address	Foreign Address	State	PID	
•	TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	884	---
•	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4	---
•	TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING	976	
•	TCP	0.0.0.0:5000	0.0.0.0:0	LISTENING	1160	
•	TCP	166.111.203.10:139	0.0.0.0:0	LISTENING	4	---
•	UDP	0.0.0.0:135	*:*		884	
•	UDP	0.0.0.0:445	*:*		4	---
•	UDP	0.0.0.0:500	*:*		704	---
•	UDP	0.0.0.0:1026	*:*		1112	
•	UDP	0.0.0.0:1027	*:*		976	
•	UDP	127.0.0.1:123	*:*		976	---
•	UDP	127.0.0.1:1900	*:*		1160	---
•	UDP	166.111.203.10:123	*:*		976	---
•	UDP	166.111.203.10:137	*:*		4	---
•	UDP	166.111.203.10:138	*:*		4	---
•	UDP	166.111.203.10:1900	*:*		1160	

- Solaris中的inetd超级守护进程
/etc/inetd.conf, 每个服务一行
- Linux中的xinetd超级守护进程
/etc/xinetd.d 目录, 每个服务一个文件
- restart inetd/xinetd
kill -s HUP <pid_of_inetd_or_xinetd>
- Solaris/Linux运行级别和启动脚本
/etc/init.d 目录

- 口令访问控制

- 口令策略:

- 口令生命期、最短长度、错误尝试次数、

- 口令复杂度

- 1) windows:

- Control Panel -> Admin Tools -> Local Security Policy -> Account Policies

- 2) Solaris / Linux

- a) /etc/shadow b) /etc/default/login (Solaris)

- c) /etc/default.defs (Linux)

- 文件系统访问控制

- 1) Windows

NTFS: 文件夹选项 → 去掉 “use simple file sharing”

- 2) Unix/Linux:

owner, group, other rwx

umask 027 设置缺省的新文件权限

- 网络访问控制

Windows防火墙, tcpwrapper,

- Unix 日志: /etc/syslog.conf
 - /var/adm/ (solaris)
 - /var/log/ (Linux)
- Windows Event Viewer
- 应用程序日志:
 - eg. 网络登录系统日志:
 - 帮助确定笔记本被盗时间
 - eg. 邮件服务器的登录日志:
 - 用户可以检查自己邮箱是否被他人登录
 - eg. Web服务器日志:
 - 协助确定攻击的发生。
- 日志的完整性
 - 日志文件的访问控制，数字签名，审计。

- 安装防毒软件
- 安装防火墙
- 及时更新病毒库和攻击特征

- 信息安全的三个要素：
 - 机密性： Confidentiality
 - 完整性： Integrity
 - 可获得性： Availability

保证C-I-A，需要做哪些配置呢？

- 保证网络通信的机密性

校园网中的常见网络应用:

Telnet → SSH v2: Linux/Unix登录, BBS

HTTP → HTTPS: 表单数据的提交

POP3 → POP3 over SSL

SMTP → SMTP over SSL

FTP → SFTP, SCP

当今, 主流的客户端软件(IE/Firefox, OE/Foxmail)都支持安全通信的情况下, 校园网中还有多少口令是以明文在传递的?

- 网络通信的机密性（续）

校园网的“统一口令”系统易出现的薄弱环节：

- 1) 多个应用：

有的采用安全方式接收用户认证信息

有的采用非安全方式接收用户认证信息

只要后者被窃听，则前者的安全措施

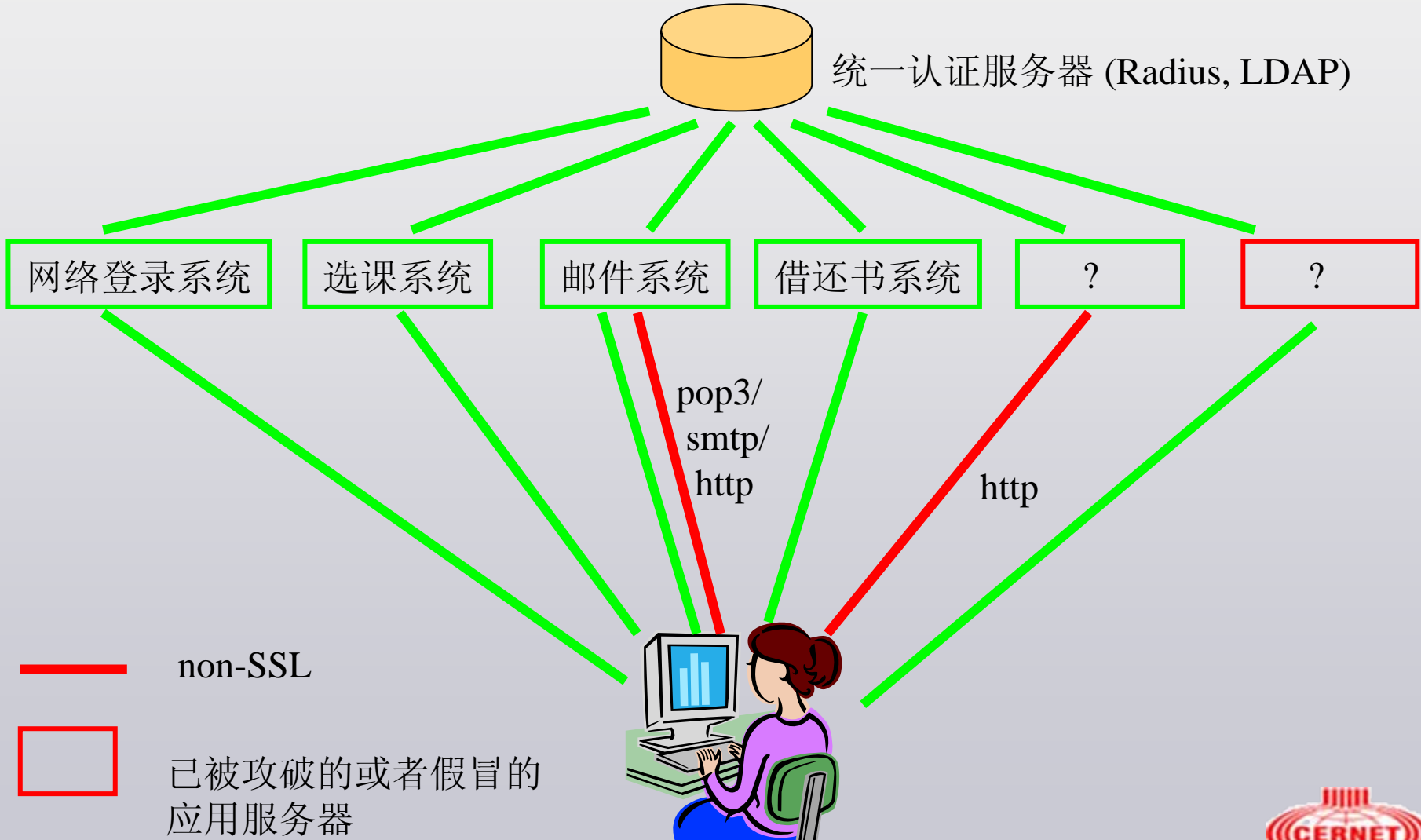
就前功尽弃了，损失比不统一口令还大。

- 2) 同一个应用，同时提供安全的和非安全的服务端口：

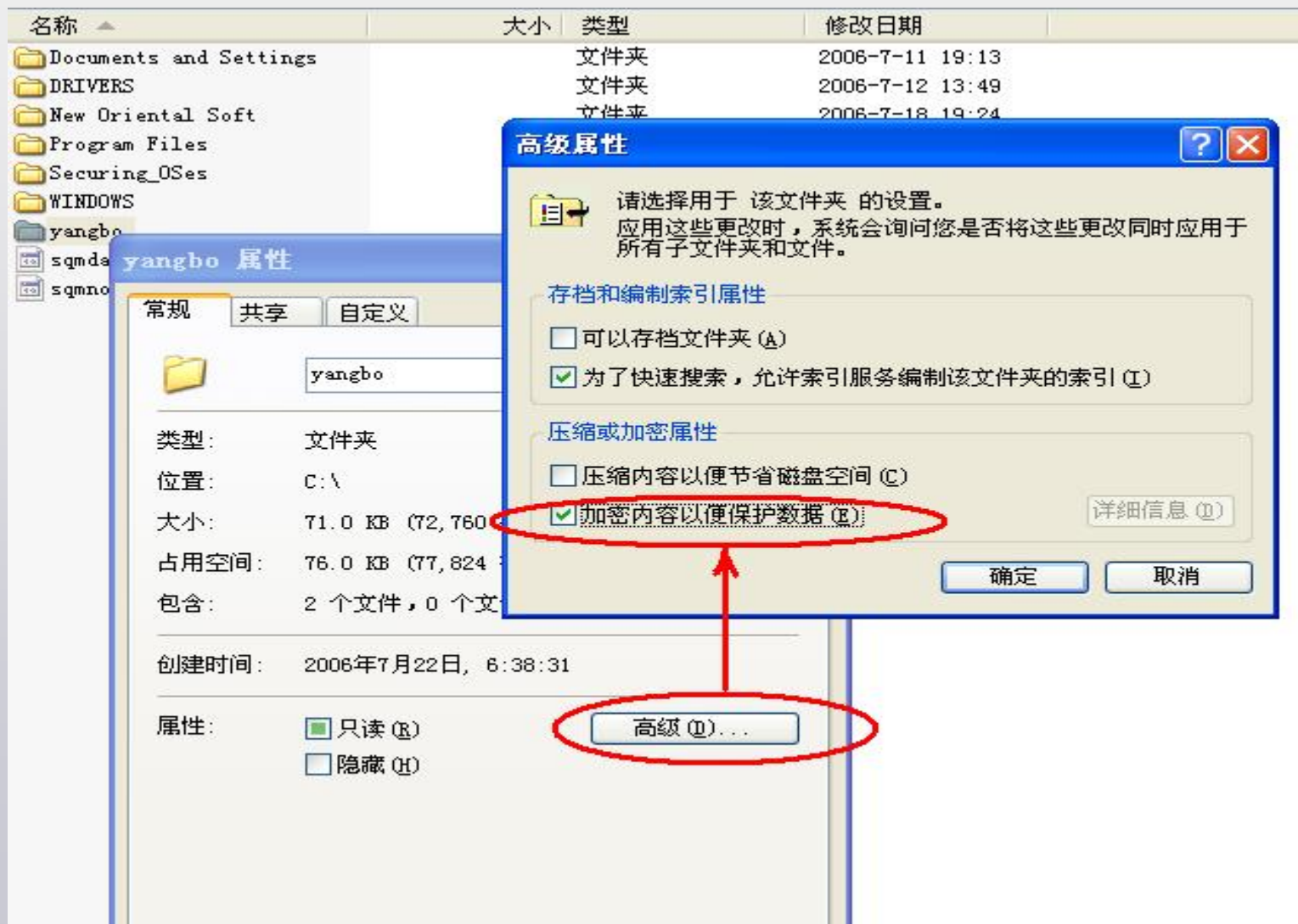
口令安全性取决于最弱的方式

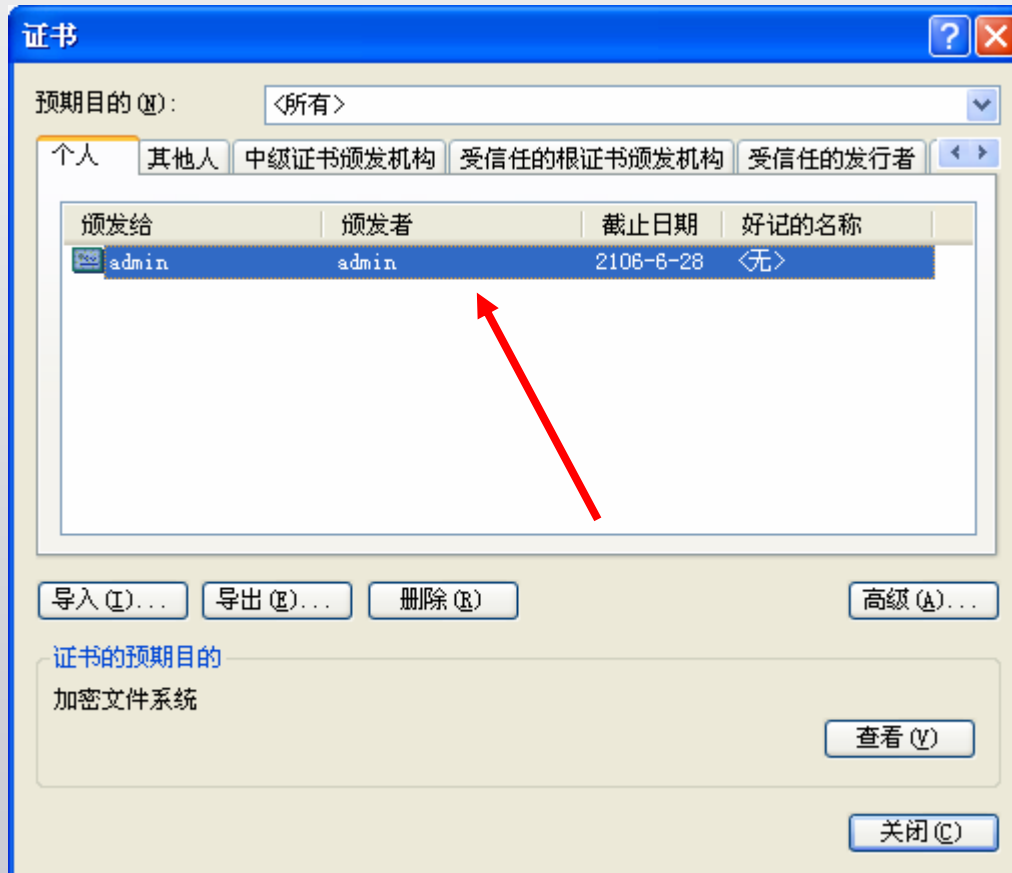
- 网络通信的机密性（续）
 - 3) 被攻破的应用服务器

数据安全



- 存储中数据的机密性（以Windows系统为例）
 - 误区： 只需把分区格式化为NTFS格式就可以保密数据
 - 实际： 只需把该硬盘挂到其他电脑上，无需原来用户的口令，即可轻松查看NTFS卷中的内容
- 如何保证数据的机密性：
 - 1) 手工对文件加/解密： GnuPG, OpenSSL, WinRAR
 - 缺点： 对用户不透明； 如果文件需要经常修改，则经常手工加/解密很麻烦
 - 2) 对用户透明的加/解密： EFS（加密文件系统）
 - 对NTFS卷上的文件和文件夹，可以启用EFS基于X.509公钥证书实现透明的加/解密。





名称	大小	类型	修改日期
Documents and Settings		文件夹	2006-7-11 19:13
DRIVERS		文件夹	2006-7-12 13:49
New Oriental Soft		文件夹	2006-7-18 19:24
Program Files		文件夹	2006-7-19 15:21
Securing_OSes		文件夹	2006-7-22 10:13
WINDOWS		文件夹	2006-7-22 6:44
yangbo		文件夹	2006-7-22 10:27
sqmdata00.sqm	1 KB	SQM 文件	2006-7-17 17:13
sqmnoopt00.sqm	1 KB	SQM 文件	2006-7-17 17:13

后退 搜索 文件夹

转到

C:\yangbo

名称	大小	类型	修改日期
digitalsig01.JPG	63 KB	JPEG 图像	2006-7-22 10:25
efs01.JPG	64 KB	JPEG 图像	2006-7-22 10:27
efs02.bmp	398 KB	BMP 图像	2006-7-22 10:46
efs02.jpg	398 KB	JPEG 图像	2006-7-22 10:46

图片任务

- 作为幻灯片查看
- 联机订购照片
- 打印图片
- 复制所有项目到 CD

文件和文件夹任务

- 创建一个新文件夹
- 将这个文件夹发布到

- 保证数据的完整性
 - 1) 散列值
 - 2) 数字签名

-- 开源软件:

多使用散列值或OpenPGP签名来保证完整性

```
c:\> gpg --print-md mds <file_to_be_hashed>
```

```
c:\> gpg --verify file.sig
```

-- Windows下的非开源软件：

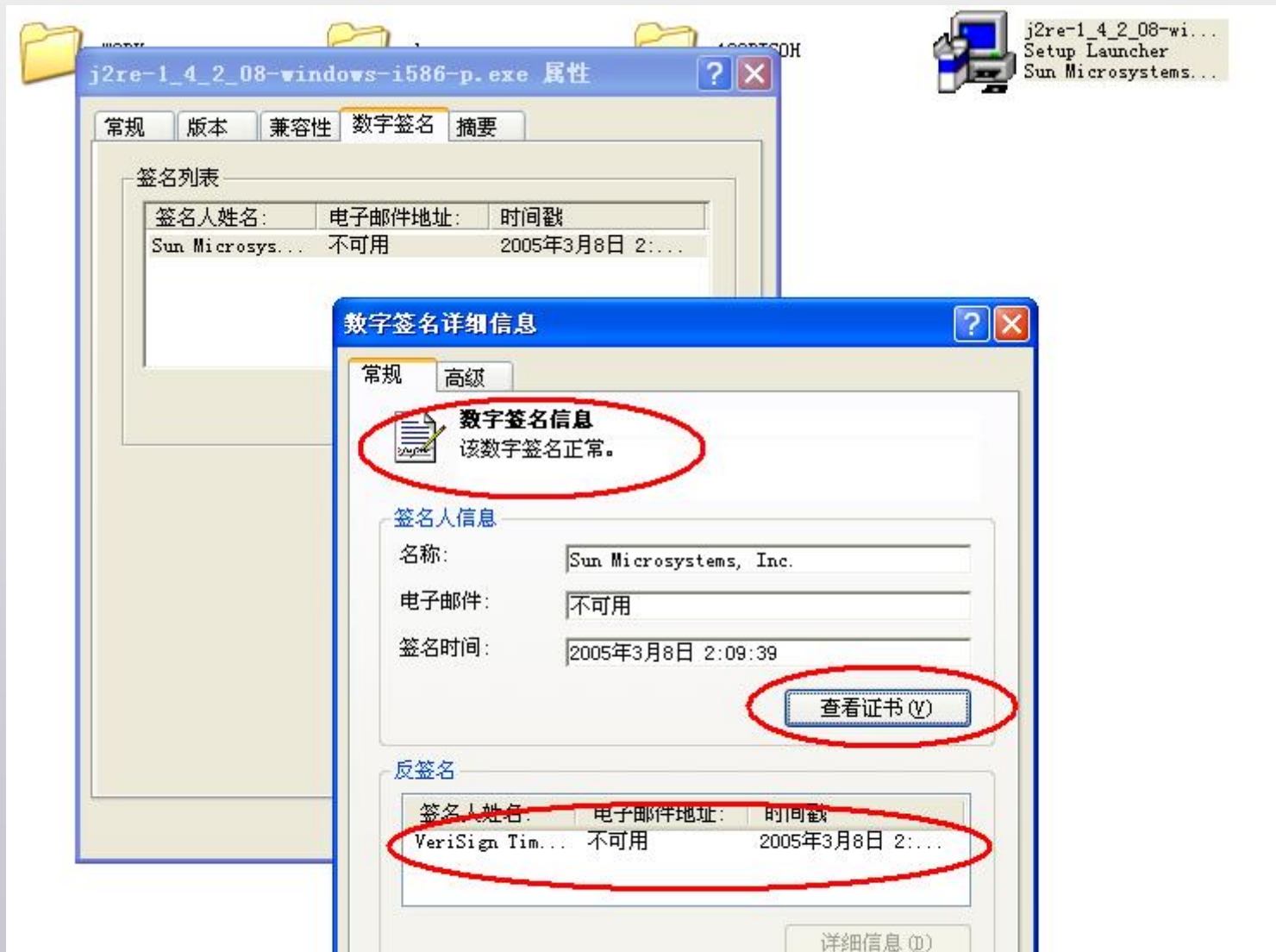
多使用微软的Authenticode技术对待发布的PE格式文件 (*.exe, *.msi, *.dll等) 进行数字签名。用户在执行程序前，可以在GUI中轻松地验证签名，确保程序来自于可信源且未被篡改。

-- 常见的被签名对象：

安装程序(*.exe, *.msi)

动态链接库 (*.dll)

补丁程序(*.exe): OS补丁, nav每日病毒库



- 备份策略

- 安全是一个过程，而不是一个结果。
- 关注安全新闻：
 - www.cert.org
 - www.ccert.edu.cn
 - www.securityfocus.com
 - 软硬件厂商的安全页面
- 关注安全技术发展
 - 避免使用不再受支持/更新的产品：
 - 多少连网机器还在使用RH 9, FC2/3, Win98se?
 - 避免使用安全性已经受怀疑的技术：
 - 多少程序员仍然在用MD5作散列函数?
 - 多少无线AP仍然停留在WEP加密?

- 关闭、升级或封堵不必要的系统服务
- 访问控制
- 保证网络通信和存储中的数据安全
- 关注安全新闻和技术发展

谢谢！
请各位老师和专家指教。