[系统安全] 二十.PE数字签名之(上)什么是数字签名及Signtool签名工具详解

原创

Eastmount 于 2021-02-07 17:37:39 发布 4704 收藏 18

分类专栏： 系统安全与恶意代码分析 文章标签： 数字签名 PE文件 恶意代码分析 Signtool 签名分析

本文链接：https://blog.csdn.net/Eastmount/article/details/113744316

您可能之前看到过我写的类似文章，为什么还要重复撰写呢？只是想更好地帮助初学者了解病毒逆向分析和系统安全，更加成体系且不破坏之前的系列。因此，我重新开设了这个专栏，准备系统整理和深入学习系统安全、逆向分析和恶意代码检测，“系统安全”系列文章会更加聚焦，更加系统，更加深入，也是作者的慢慢成长史。换专业确实挺难的，逆向分析也是块硬骨头，但我也试试，看看自己未来四年究竟能将它学到什么程度，漫漫长征路，偏向虎山行。享受过程，一起加油~

作者前文介绍了宏病毒相关知识，它仍然活跃于各个APT攻击样本中，具体内容包括宏病毒基础原理、防御措施、自发邮件及APT28样本分析。本文将详细介绍什么是数字签名，并采用Signtool工具对EXE文件进行签名，后续深入分析数字签名的格式及PE病毒内容。 这些基础性知识不仅和系统安全相关，同样与我们身边常用的软件、文档、操作系统紧密联系，希望这些知识对您有所帮助，更希望大家提高安全意识，安全保障任重道远。本文参考了参考文献中的文章，并结合自己的经验和实践进行撰写，也推荐大家阅读参考文献。

文章目录

> 从2019年7月开始，我来到了一个陌生的专业——网络空间安全。初入安全领域，是非常痛苦和难受的，要学的东西太多、涉及面太广，但好在自己通过分享100篇“网络安全自学”系列文章，艰难前行着。感恩这一年相识、相知、相趣的安全大佬和朋友们，如果写得不好或不足之处，还请大家海涵！
>
> 接下来我将开启新的安全系列，叫“系统安全”，也是免费的100篇文章，作者将更加深入的去研究恶意样本分析、逆向分析、内网渗透、网络攻防实战等，也将通过在线笔记和实践操作的形式分享与博友们学习，希望能与您一起进步，加油~
>
> - 推荐前文：网络安全自学篇系列-100篇

作者的github资源：

- 逆向分析：https://github.com/eastmountyxz/SystemSecurity-ReverseAnalysis
- 网络安全：https://github.com/eastmountyxz/NetworkSecuritySelf-study

前文分析：

- [系统安全] 一.什么是逆向分析、逆向分析基础及经典扫雷游戏逆向
- [系统安全] 二.如何学好逆向分析及吕布传游戏逆向案例
- [系统安全] 三.IDA Pro反汇编工具初识及逆向工程解密实战
- [系统安全] 四.OllyDbg动态分析工具基础用法及Crakeme逆向
- [系统安全] 五.OllyDbg和Cheat Engine工具逆向分析植物大战僵尸游戏
- [系统安全] 六.逆向分析之条件语句和循环语句源码还原及流程控制
- [系统安全] 七.逆向分析之PE病毒原理、C++实现文件加解密及OllyDbg逆向
- [系统安全] 八.Windows漏洞利用之CVE-2019-0708复现及蓝屏攻击
- [系统安全] 九.Windows漏洞利用之MS08-067远程代码执行漏洞复现及深度提权
- [系统安全] 十.Windows漏洞利用之SMBv3服务远程代码执行漏洞（CVE-2020-0796）复现
- [系统安全] 十一.那些年的熊猫烧香及PE病毒行为机理分析
- [系统安全] 十二.熊猫烧香病毒IDA和OD逆向分析（上）病毒初始化
- [系统安全] 十三.熊猫烧香病毒IDA和OD逆向分析（中）病毒释放机理
- [系统安全] 十四.熊猫烧香病毒IDA和OD逆向分析–病毒释放过程（下）
- [系统安全] 十五.Chrome浏览器保留密码功能渗透解析、蓝屏漏洞及某音乐软件漏洞复现
- [系统安全] 十六.PE文件逆向基础知识(PE解析、PE编辑工具和PE修改)
- [系统安全] 十七.Windows PE病毒概念、分类及感染方式详解
- [系统安全] 十八.病毒攻防机理及WinRAR恶意劫持漏洞(脚本病毒、自启动、定时关机、蓝屏攻击)
- [系统安全] 十九.宏病毒之入门基础、防御措施、自发邮件及APT28宏样本分析
- [系统安全] 二十.PE数字签名之(上)什么是数字签名及Signtool签名工具详解

> 声明：本人坚决反对利用教学方法进行犯罪的行为，一切犯罪行为必将受到严惩，绿色网络需要我们共同维护，更推荐大家了解它们背后的原理，更好地进行防护。该样本不会分享给大家，分析工具会分享。（参考文献见后）

一.PE文件的数字签名

1.概念普及

(1) PE文件

PE文件的全称是Portable Executable，意为可移植的可执行的文件，常见的EXE、DLL、OCX、SYS、COM都是PE文件，PE文件是微软Windows操作系统上的程序文件（可能是间接被执行，如DLL）。后续文章会详细分析PE文件格式。

(2) 为什么要对PE文件进行数字签名呢？

- **防篡改**：通过对数字签名的验证，保证文件未被非法篡改。
- **降低误报**：安全软件通过验证文件是否有正规厂商的数字签名来降低误报。

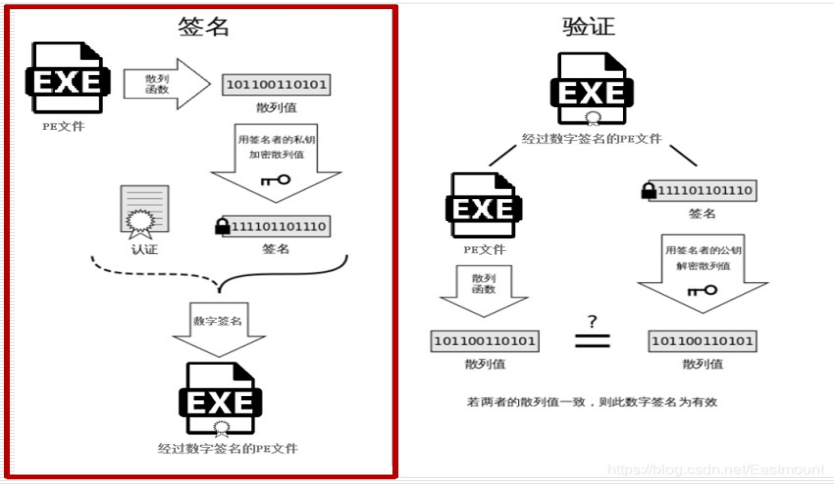
(3) PE文件数字签名及验证过程

签名：

- 软件发布者使用散列算法（如MD5或SHA）计算PE文件的散列值。
- 软件发布者使用私钥对散列值进行签名得到签名数据。
- 将签名私钥对应的公钥和签名数据等以证书的形式附加在PE文件之中，形成经过数字签名的PE文件。
- 软件发布者将经过数字签名的PE文件进行发布。

验证：

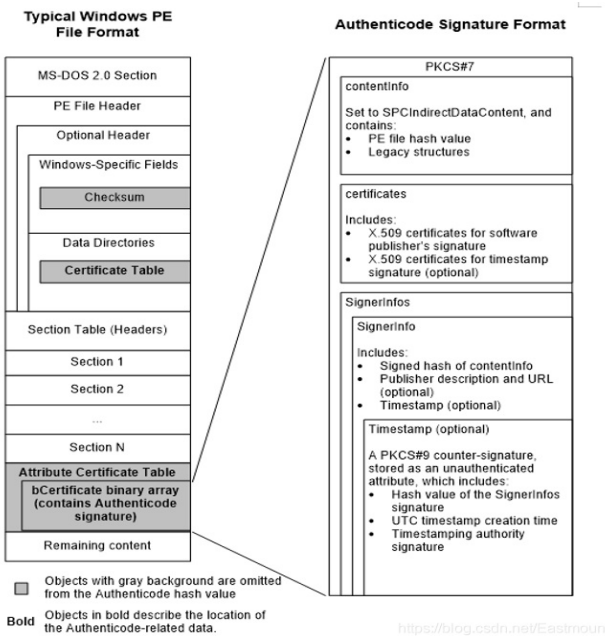
- 从PE文件证书中提取软件发布者的公钥、使用的散列算法、签名算法、原始散列值的签名数据。
- 使用提取的公钥和对应签名验证算法将签名数据还原为原始PE文件的原始散列值。
- 对现有PE文件使用同样的散列算法计算出对应的散列值。
- 对比两个散列值是否一致，从而判断数据是否被破坏和篡改。



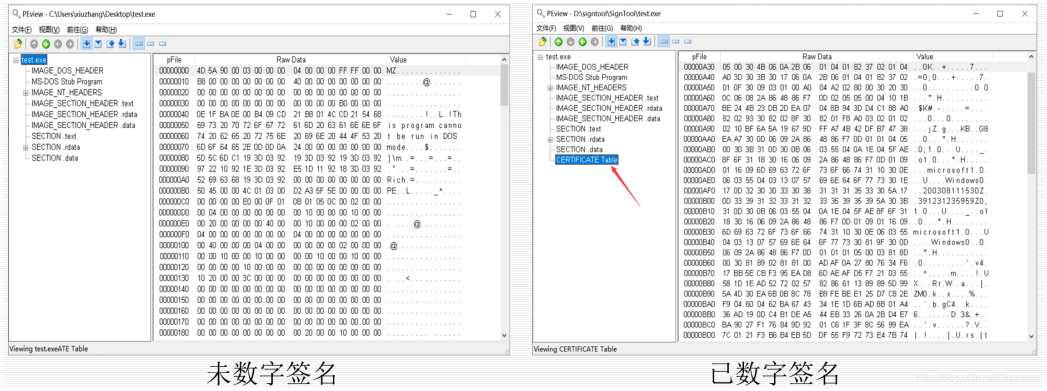
(4) PE文件数字签名的总体结构

PE文件数字签名信息存放在Certificate Table位置，同时PE文件可选文件头DataDirecotry第5项记录文件偏移及大小。

> 下一篇文章作者尝试详细讲解PE文件结构及签名解析。



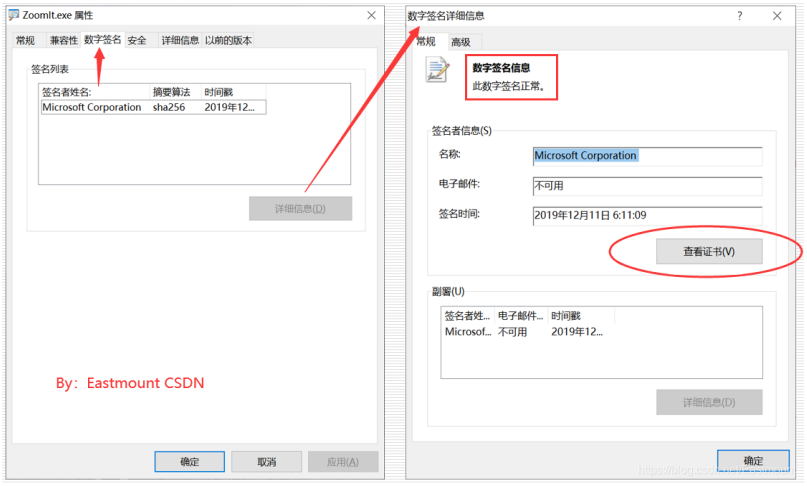
使用PEView查看签名前后对比图，可以看到Certificate Table存储相关签名信息。



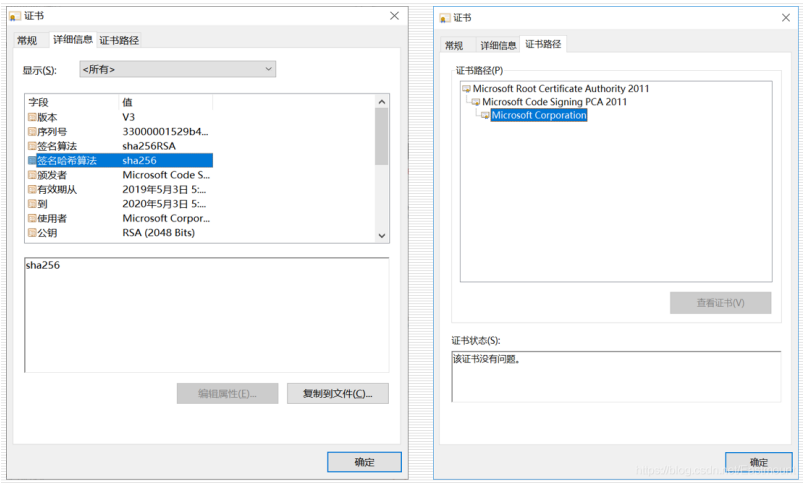
未数字签名　　已数字签名

(5) PE文件数字签名查看

这里以Zoomit.exe程序为例，我们可以看到经过数字签名后的PE文件还会多出一个“数字签名”的属性，点击详细信息可以查看对应的证书。

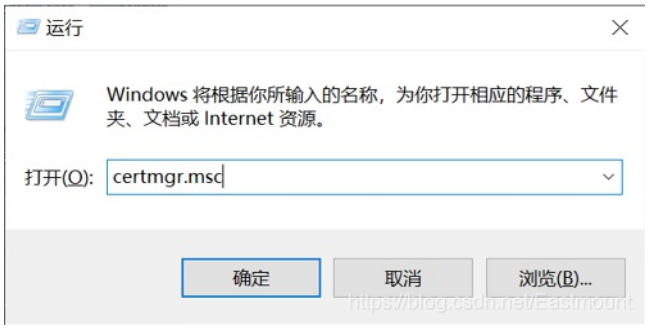


对应的证书信息及证书路径如下图所示，包括签名算法、哈希算法、有效期、颁发者信息等。

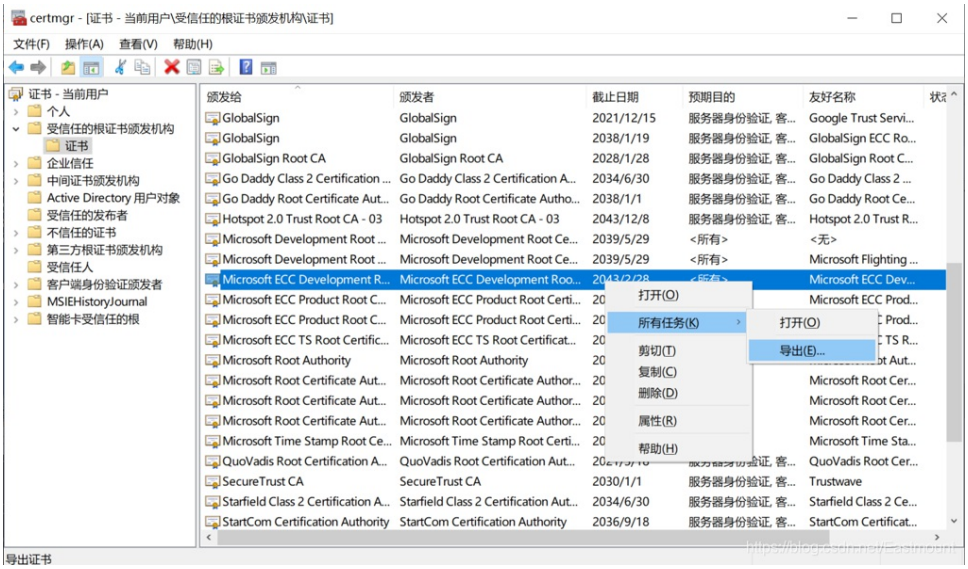


(6) 微软数字签名证书查看

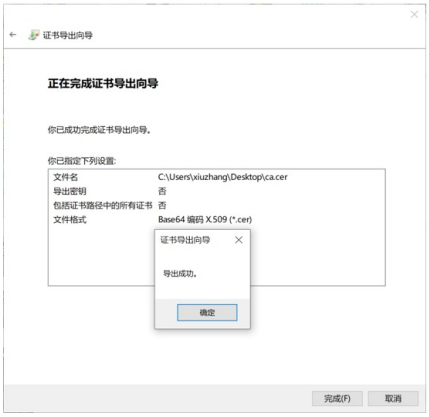
接着，我带领大家看看Windows证书。运行中输入“certmgr.msc”，可以看到这里面有5个系统默认的ECC签名的根证书，如下图所示。



我们随意导出其中一个根证书，导出直接选择Base64编码那个就行。



可以看到导出的ECC密钥证书如下图所示，包括证书的有效期等信息。这就是微软在实现椭圆曲线加密（ECC）算法的数字证书，位于CryptoAPI.dll文件，也是被我们利用来伪造可信任来源的签名漏洞。



(7) 数字签名常用算法及应用领域

数字签名常用算法包括：

- RSA数字签名算法
  基于大整数分解问题，MD5、SHA
- DSA数字签名算法
  基于离散对数问题
- ECDSA椭圆曲线数字签名算法
  ECC+DSA，椭圆加密算法，属于DSA的一个变种，基于椭圆曲线上的离散对数问题

其应用领域包括：

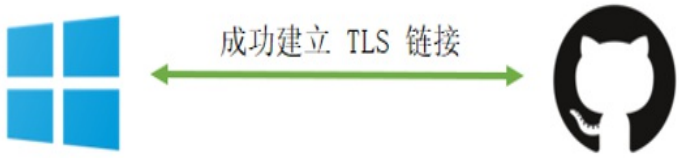
- PE文件数字签名
- HTTPS数字签名
- 电子邮件数字签名
- Office文档数字签名
- 代码数字签名

2.Github网站证书验证过程

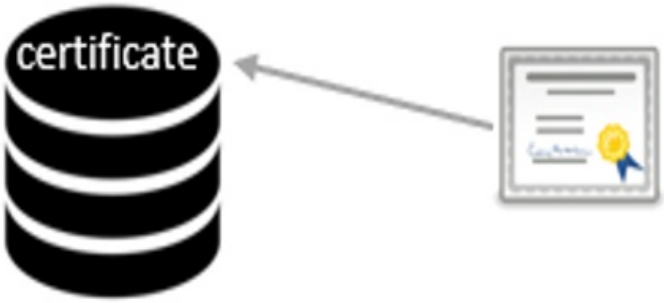
接着看看Github网站进行微软证书验证的过程。

- 在Windows系统访问一个网站(例Github.com)时，该网站会向Windows系统发送由第三方权威机构(CA)签署的网站证书。

- Windows系统则会验证该证书是否由CA颁发，若验证通过，则Windows系统与网站成功建立TLS链接。



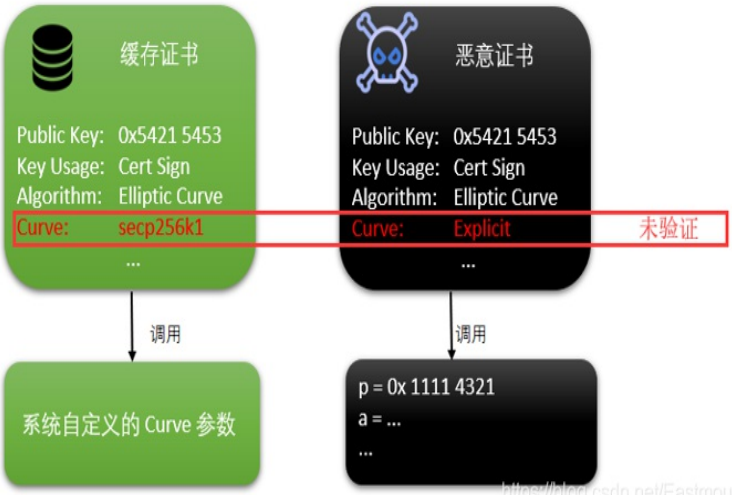
- 为了方便下一次更快的访问，Windows将验证成功的证书放入内存中一块Certificate Cache（证书缓存）中。在下一次校验时，如果该证书存在于缓存中，则直接取缓存中的值进行校验。这里利用CVE-2020-0601。



- 在成功缓存证书数据后，根据下面描述的Windows证书缓存机制，恶意网站可以伪造虚假的网站（例github.com）证书且通过Windows验证，将自身伪装成合法网站。

- 当 Windows 接收到新的证书时，Windows 将新接收的证书与已缓存证书的证书的公钥进行遍历对比，寻找匹配的值。

- 伪造的恶意证书与Windows系统中的缓存证书有同样的公钥，但Curve项没有在校验范围内，所以可以通过构造自定义Curve来伪造证书。使得证书验证流程依然成立，但通过验证的证书已经不是之前成功验证的安全证书。



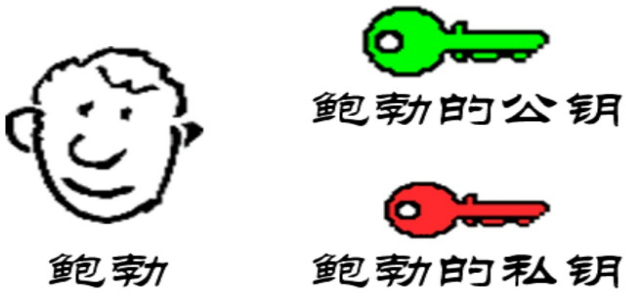
在第23篇文章中，我们将详细复现微软证书CVE-2020-0601漏洞。

二.阮一峰老师告诉大家什么是数字签名

> 参考文章：
> 数字签名是什么？ - 阮一峰
> What is a Digital Signature? - 原始网站

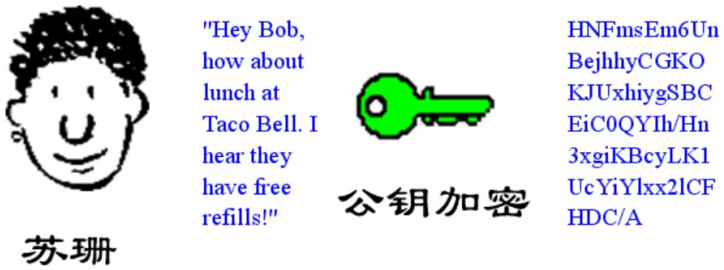
写到这里，您可能还是很疑惑“什么是数字签名”？下面我通过阮一峰老师的博客进行讲解，个人认为这是一篇讲得比较清晰的原理文章，同时也包含了网络安全中加密解密、信息传输等知识。

(1) 假设鲍勃有两把钥匙，一把是公钥，另一把是私钥。



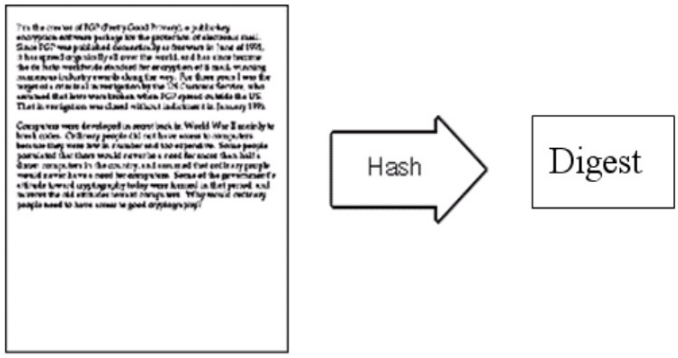
(2) 鲍勃把公钥送给他的朋友们----帕蒂、道格、苏珊----每人一把。

(3) 苏珊要给鲍勃写一封保密的信。她写完后用鲍勃的公钥加密，就可以达到保密的效果。



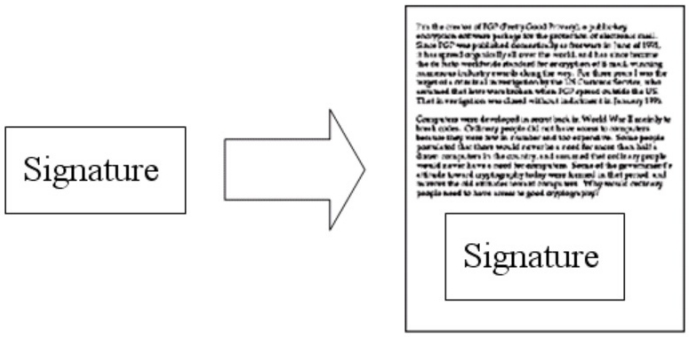
(4) 鲍勃收信后，用私钥解密，就看到了信件内容。这里要强调的是，只要鲍勃的私钥不泄露，这封信就是安全的，即使落在别人手里，也无法解密。

(5) 鲍勃给苏珊回信，决定采用"数字签名"。他写完后先用Hash函数，生成信件的摘要（digest）。



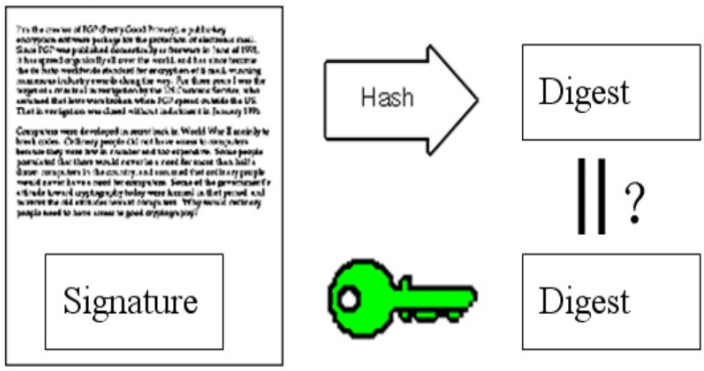
(6) 然后，鲍勃使用私钥，对这个摘要加密，生成"数字签名"（signature）。

(7) 鲍勃将这个签名，附在信件下面，一起发给苏珊。



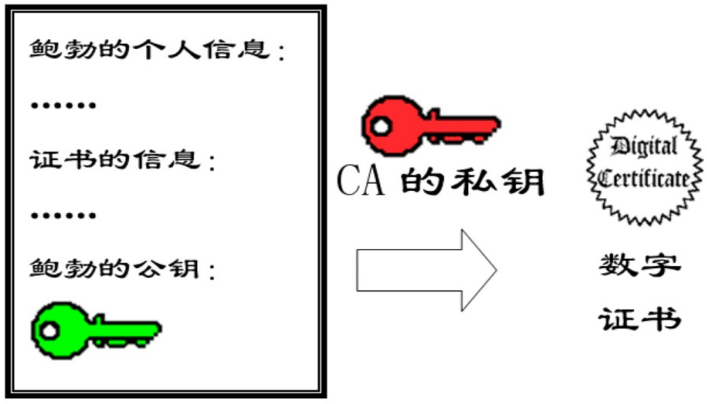
(8) 苏珊收信后，取下数字签名，用鲍勃的公钥解密，得到信件的摘要。由此证明，这封信确实是鲍勃发出的。

(9) 苏珊再对信件本身使用Hash函数，将得到的结果，与上一步得到的摘要进行对比。如果两者一致，就证明这封信未被修改过。



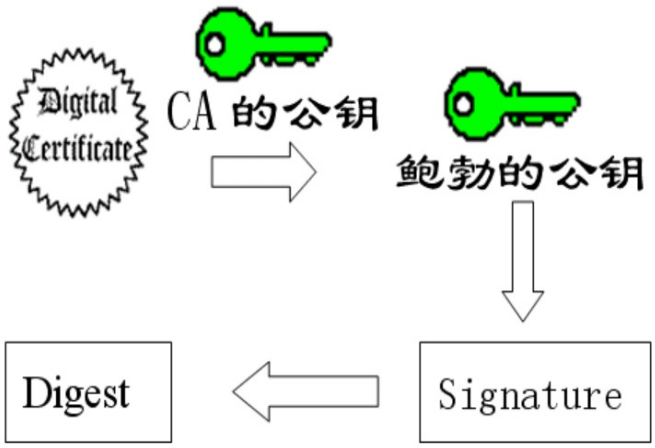
(10) 复杂的情况出现了。道格想欺骗苏珊，他偷偷使用了苏珊的电脑，用自己的公钥换走了鲍勃的公钥。此时，苏珊实际拥有的是道格的公钥，但是还以为这是鲍勃的公钥。因此，道格就可以冒充鲍勃，用自己的私钥做成"数字签名"，写信给苏珊，让苏珊用假的鲍勃公钥进行解密。

(11) 后来，苏珊感觉不对劲，发现自己无法确定公钥是否真的属于鲍勃。她想到了一个办法，要求鲍勃去找"证书中心"（certificate authority，简称CA），为公钥做认证。证书中心用自己的私钥，对鲍勃的公钥和一些相关信息一起加密，生成"数字证书"（Digital Certificate）。

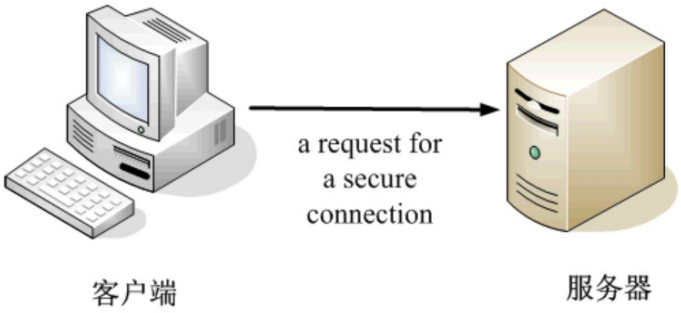


(12) 鲍勃拿到数字证书以后，就可以放心了。以后再给苏珊写信，只要在签名的同时，再附上数字证书就行了。

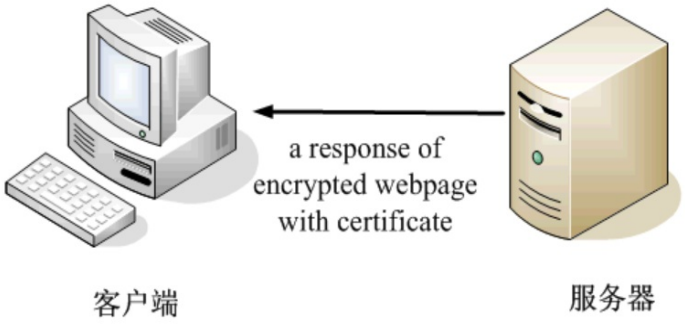
(13) 苏珊收信后，用CA的公钥解开数字证书，就可以拿到鲍勃真实的公钥了，然后就能证明"数字签名"是否真的是鲍勃签的。



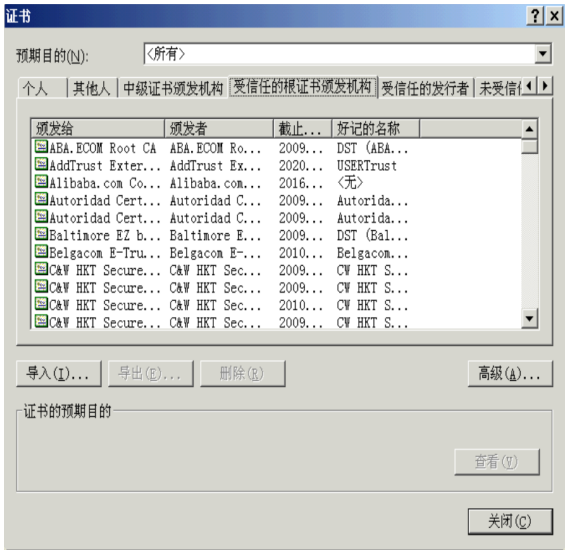
(14) 下面，我们看一个应用"数字证书"的实例：https协议。这个协议主要用于网页加密。首先，客户端向服务器发出加密请求。



(15) 服务器用自己的私钥加密网页以后，连同本身的数字证书，一起发送给客户端。

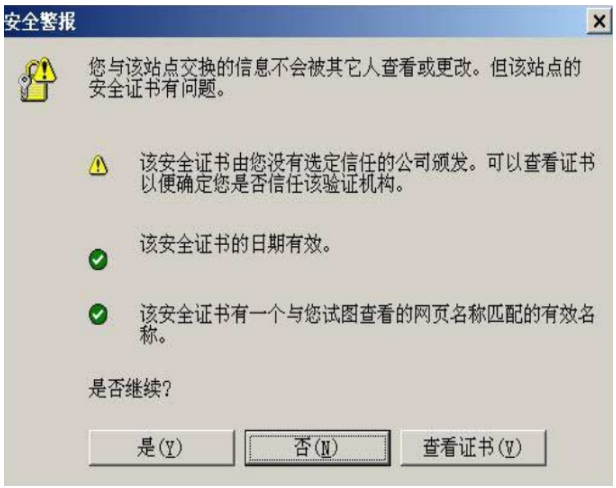


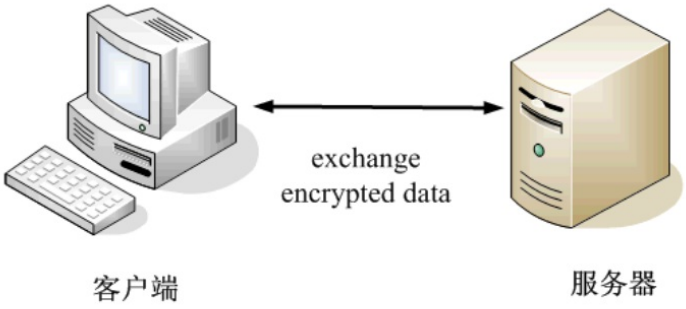
(16) 客户端（浏览器）的"证书管理器"，有"受信任的根证书颁发机构"列表。客户端会根据这张列表，查看解开数字证书的公钥是否在列表之内。



(17) 如果数字证书记载的网址，与你正在浏览的网址不一致，就说明这张证书可能被冒用，浏览器会发出警告。

(18) 如果这张数字证书不是由受信任的机构颁发的，浏览器会发出另一种警告。如果数字证书是可靠的，客户端就可以使用证书中的服务器公钥，对信息进行加密，然后与服务器交换加密信息。

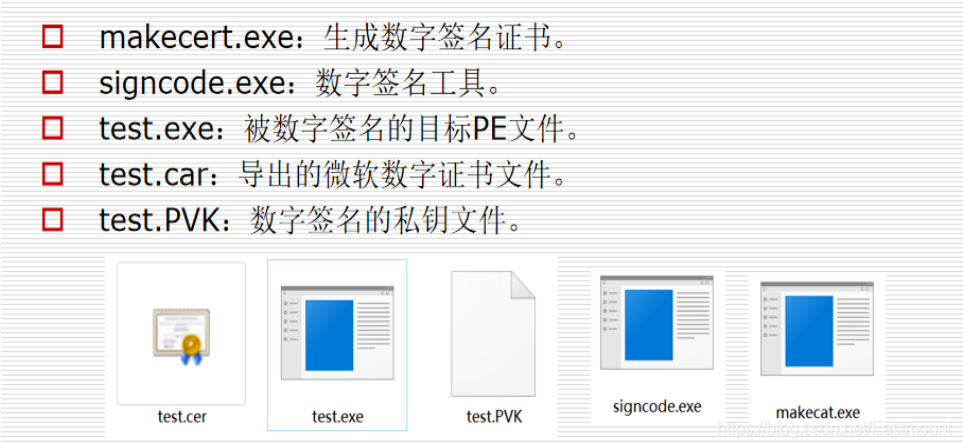




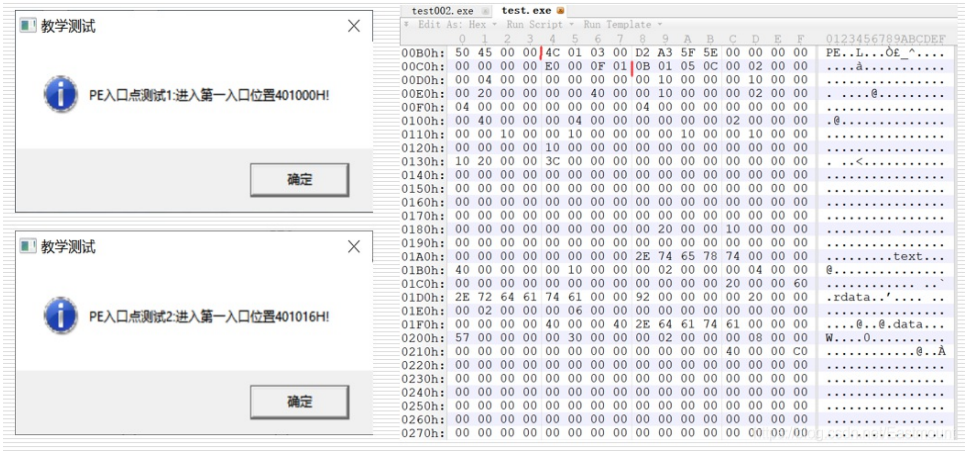
数字签名是为了保证数据完整性。通过它可以判断数据是否被篡改，私钥加密完的数据所有知道公钥的都可以解密，这样不安全。私钥加密的作用是为了确认身份，用对应的公钥解密摘要，则证明摘要来自谁，起到签名的作用。

三.Signtool签名PE文件

- 逆向分析：https://github.com/eastmountyxz/SystemSecurity-ReverseAnalysis
- 软件安全：https://github.com/eastmountyxz/Software-Security-Course

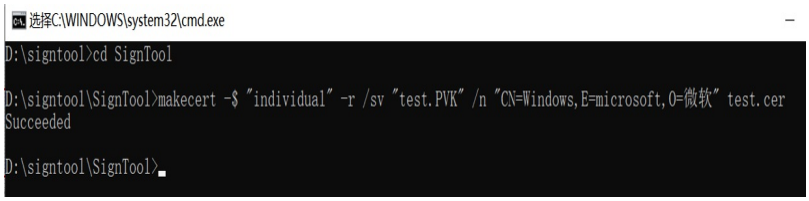


该test.exe程序后续文章也会分享，均上传至Github。

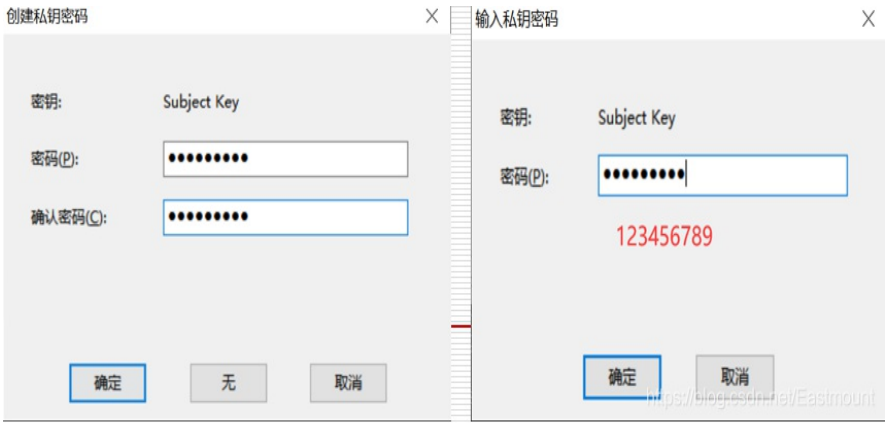


第一步，通过makecert.exe生成需要的证书，生成两个文件分别是test.cer和test.PVK。

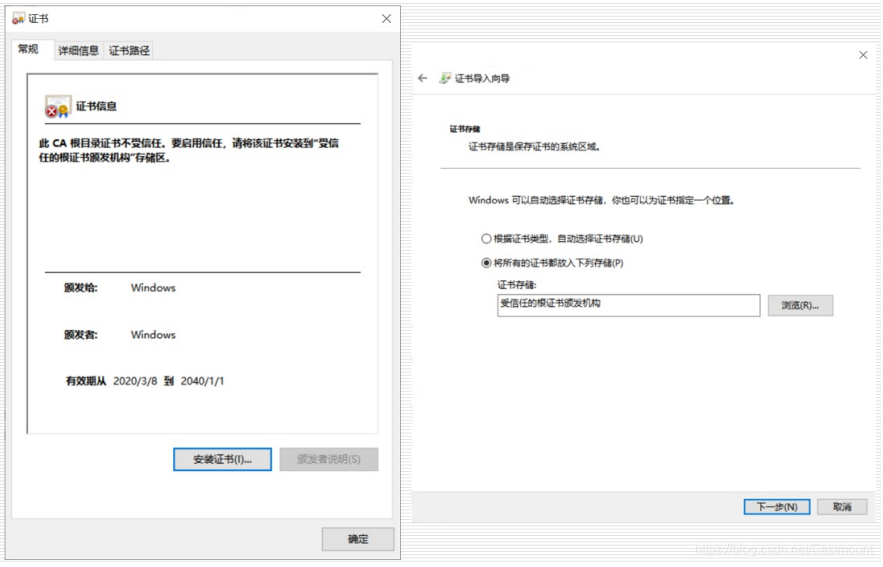
```
cd SignTool
makecert -$ "individual" -r /sv "test.PVK" /n "CN=Windows,E=microsoft,O=微软" test.cer
```



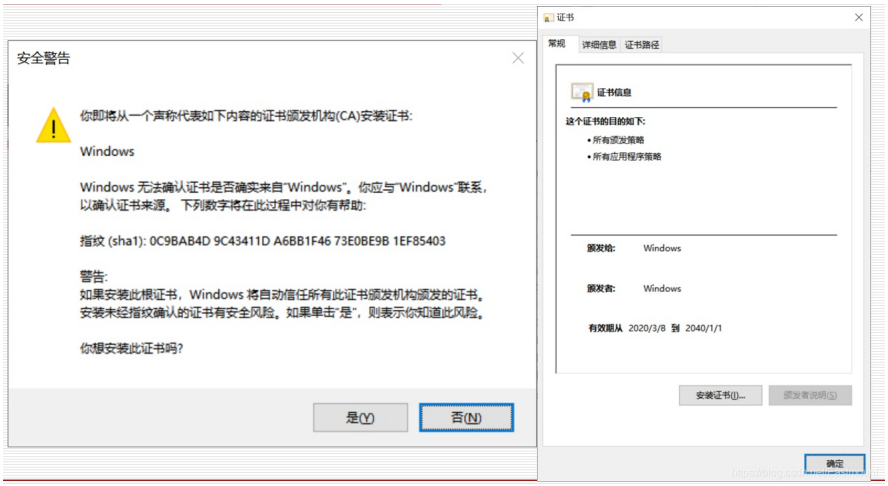
创建过程中需要输入私钥密码，这里设置为“123456789”。



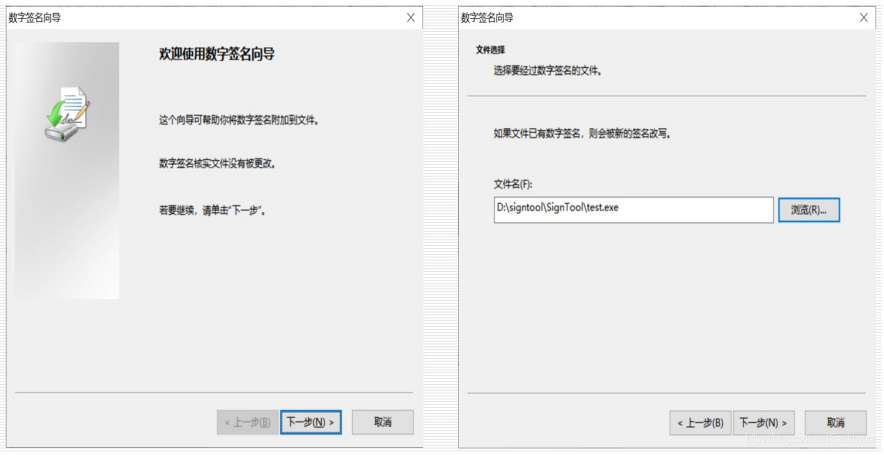
第二步，查看证书信息，如果未信任需要点击“安装证书”。



安装并信任该证书。

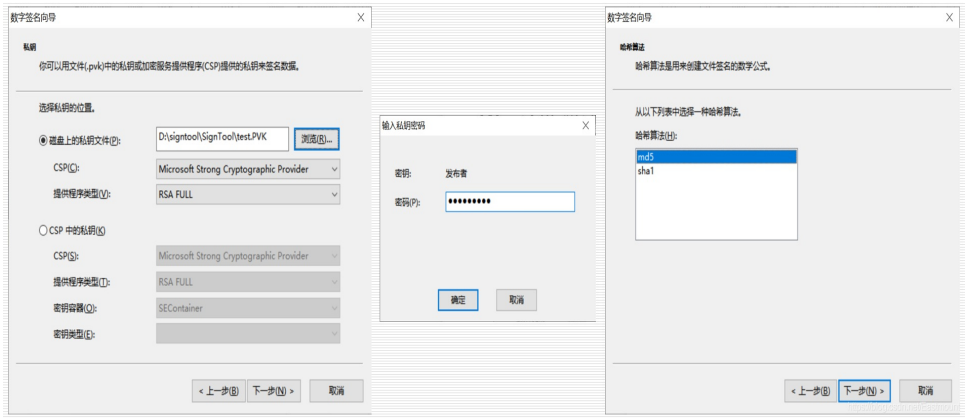


第三步，利用signcode.exe工具进行数据签名，选择需要签名的“test.exe”程序。

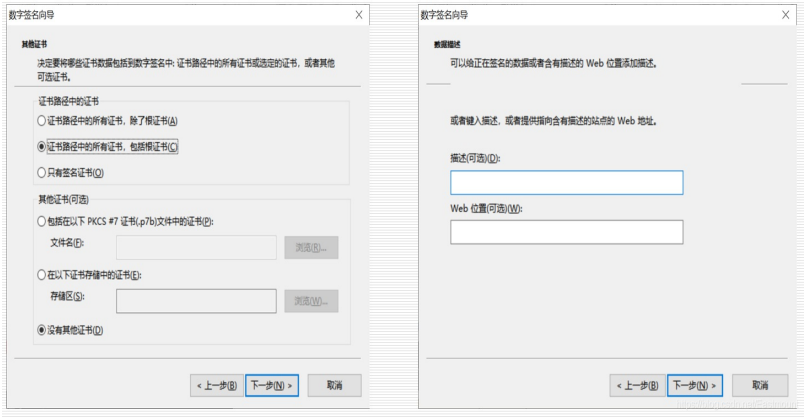


第四步，自动选择自定义选项，然后点击从文件中选择test.cer文件，test.cer文件在第一个步骤你生成的目录中，然后下一步。

第五步，点击浏览按钮，添加文件test.PVK，test.PVK文件也是在第一步生成的目录中，点击下一步，哈希算法可以选md5，也可以选sha1，点击下一步。

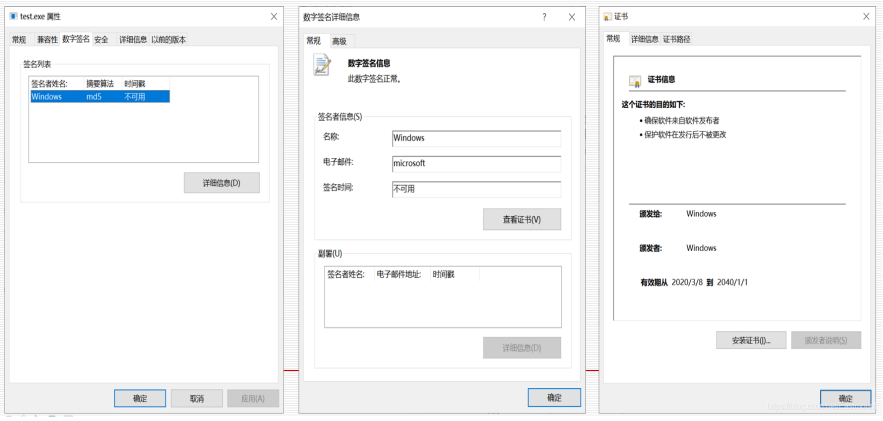


第六步，默认点击下一步，出现数据描述框，自己可以填写，也可以不填。点击下一步。

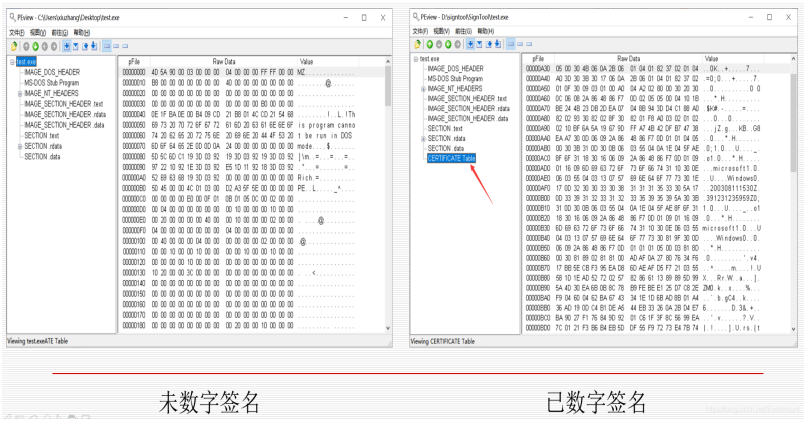


第七步，填写时间戳服务器URL：http://timestamp.wosign.com/timestamp，也可以不选添加时间戳，点击下一步，完成，弹出签名成功框。

第八步，此时test.exe文件完成数字签名，打开该exe文件属性，如下图所示，可以看到签名相关信息。注意，该数字签名正常且颁发者为Windows。

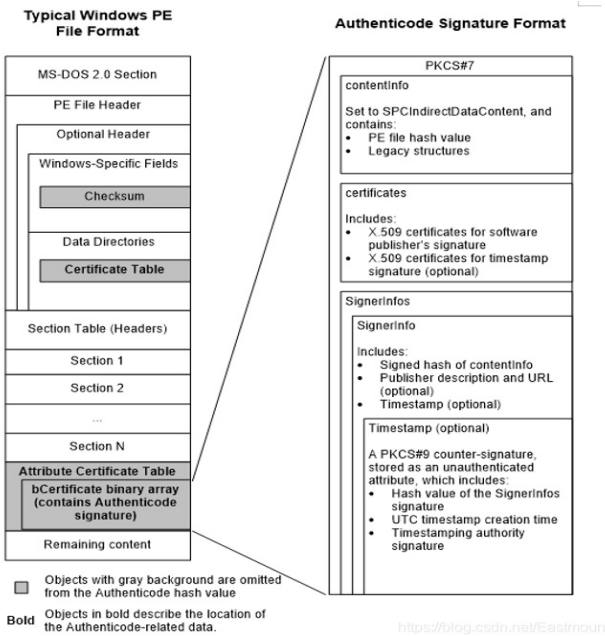


最后我们使用PEView软件打开PE文件，可以看到签名前和签名后的结构存在“CERTIFICATE Table”区别。



未数字签名　　已数字签名

下一篇文章我们将详细分析数字签名的结构。



四.总结

文章写到这里，就介绍完毕，希望文章对您有所帮助。这篇文章主要讲解：

- PE文件数字签名
- 分享阮一峰老师的博客，告诉大家什么是数字签名
- 结合SignTool工具对EXE文件进行签名

作者作为网络安全初学者的慢慢成长路吧！希望未来能更透彻撰写相关文章。同时非常感谢参考文献中的安全大佬们的文章分享，感谢小伙伴和师傅们的教导。从网络安全到系统安全，从木马病毒到后门劫持，从恶意代码到溯源分析，从渗透工具到二进制工具，还有Python安全、顶会论文、黑客比赛和漏洞分享。未知攻焉知防，人生漫漫其路远兮，作为初学者，自己真是爬着前行，感谢很多人的帮助，继续爬着，继续加油！

学安全一年，认识了很多安全大佬和朋友，希望大家一起进步。这篇文章中如果存在一些不足，还请海涵。作者作为网络安全和系统安全初学者的慢慢成长路吧！希望未来能更透彻撰写相关文章。同时非常感谢参考文献中的安全大佬们的文章分享，感谢师傅、实验室小伙伴的教导，深知自己很菜，得努力前行。编程没有捷径，逆向也没有捷径，它们都是搬砖活，少琢磨技巧，干就对了。什么时候你把攻击对手按在地上摩擦，你就赢了，也会慢慢形成了自己的安全经验和技巧。加油吧，少年希望这个路线对你有所帮助，共勉。

欢迎大家讨论，是否觉得这系列文章帮助到您！如果存在不足之处，还请海涵。任何建议都可以评论告知读者，共勉~

- 逆向分析：https://github.com/eastmountyxz/SystemSecurity-ReverseAnalysis
- 网络安全：https://github.com/eastmountyxz/NetworkSecuritySelf-study

2020年8月18新开的“娜璋AI安全之家”，主要围绕Python大数据分析、网络空间安全、人工智能、Web渗透及攻防技术进行讲解，同时分享CCF、SCI、南核北核论文的算法实现。娜璋之家会更加系统，并重构作者的所有文章，从零讲解Python和安全，写了近十年文章，真心想把自己所学所感所做分享出来，还请各位多多指教，真诚邀请您的关注！谢谢。

(By:Eastmount 2021-02-07 星期天 凌晨夜于贵阳 http://blog.csdn.net/eastmount/)

参考文献：

[1] 武大《软件安全》课程
[2] (强推) [网络安全自学篇] 四十六.微软证书漏洞CVE-2020-0601 (上)Windows验证机制及可执行文件签名复现
[3] (强推) 数字签名是什么？ - 阮一峰
[4] (强推) What is a Digital Signature? - 原始网站
[5] (强推) 对Windows 平台下PE文件数字签名的一些研究 - DoveFeng
[6] (强推) https://docs.microsoft.com/zh-cn/windows/win32/debug/pe-format
[7] (强推) 哈希 HASH·数字签名 - Phant
[8] (强推) 恶意文件分析系统中的数字签名验证 - 绿盟科技
[8] (强推) [翻译]Windows PE文件中的数字签名格式 - 看雪银雁冰大神
[9] PE文件数字签名工具 - ahuo
[10] PE文件解析-异常处理表与数字签名 - zhyulo
[11] Authenticode签名伪造——PE文件的签名伪造与签名验证劫持 - 嘶吼RoarTalk
[12] 数字签名 - CTF Wiki
[13] 数字签名算法介绍和区别 - infiniSign
[14] [求助]关于PE文件的数字签名 - 看雪论坛
[15] 区块链：数字签名是什么？ - ChinaKingKong
[16] 校验文件数字签名的合法性(VerifyPE) - ahuo
[17] 数字签名 - shinymood
[18] 恶意文件分析系统中的数字签名验证 - 百度文库
[19] 如何判断一个文件是否已经有数字签名 - CSDN论坛