一种PE文件RSA验证加密算法

朱根标[1]，　张凤鸣[1]，　王金干[1]，　陈华勇[2]

(1. 空军工程大学工程学院，陕西西安 710038；2. 重庆市95696部队，重庆 401329)

摘　要：研究了非对称RsA加密算法及PE文件结构，基于Derome的RSA密钥快速生成方法，提出了利用高级语言ASM编写嵌入RSA验证DLL和直接修改PE文件来加密Win32平台下的PE可执行文件的方法。该方法避免了耗时的Euclidear算法，可并行处理，同时在PE文件验证时嵌入了DLL来实现，具有很好的安全强度。

关键词：RSA；PE文件结构；DLL嵌入；验证加密；数据安全

中图分类号：TP3　　**文献标识码**：A　　**文章编号**：1009-3516(2005)04-0067-03

非对称密码术RSA算法不仅可以作为加密算法使用，而且可以用作数字签名和密钥分配与管理[1]。RSA的实现要求大整数运算，计算量比较大且较复杂，而且要求额外的DLL提供支持。本文探讨一种私钥快速生成方法及直接操作PE的方法，实现了在原来PE文件基础上直接实现RSA验证功能而且不要附带DLL的方法。

1　非对称RSA及密钥快速生成方法

1.1　非对称RSA

RSA采用一对密钥，即公钥和私钥，从公钥难于推出私钥，反之亦然，此难度是基于大数分解。利用RSA加密软件的流程如下：①随机生成一对公钥 e 和私钥 d；②软件作者实现一个注册机。注册机的工作就是把输入 M 用私钥 d 加密，生成的密文 C 作为软件的注册码。密文 $C = (M \hat{} d) \bmod N$ 并满足 ed mod s = 1。式中 s 是 N 的欧拉函数[2]。③软件根据用户输入的注册码得到密文，然后用公钥 d 对密文进行解密，得到明文 M'，如果明文和输入相同(即满足 $M' = M$)，则说明注册码正确，否则就是非法的注册码。破解者可以通过跟踪软件得到公钥 e，但无法得到私钥 d。明文 $M' = (C \hat{} e) \bmod d$。

1.2　密钥快速生成方法

由 ed mod s = 1 表明存在一正整数 j，使 $de - js = 1$。

由Derome方法1Derome方法[3]，RSA的私钥可按下式求得 $d = 1 + j[s/e] + [j(s \bmod e)] \bmod (e-1)$。式中，$j = (-s^{\phi(e)-1}) \bmod e$。

容易证明，上式求得的私钥满足 ed mod s = 1，并且只要给出公钥，就可以使(X)简单地计算出相应的私钥。于是，避免了用Euclidean算法[4]来求解私钥 e。

快速生成方法的步骤：①利用唯一因子分解定理将公开密钥 e 用 n 个子公开密钥表示 $e = e_1^{\alpha_1} e_2^{\alpha_2} \cdots e_n^{\alpha_n}$，式中 n 个子公开密钥 $e_1, e_2, \cdots, e_n$ 是 n 个素数；a_1，a_2，…，a_n 是 n 个正整数；②按 $d = 1 + j[s/e] + [j(s \bmod e)] \bmod (e-1)$ 计算 $d_1, d_2, \cdots, d_n$。d_i 是与子公开密钥 e_i 对应的子私钥；③按下式计算私钥 $d = \prod_{i=1}^{n} d_i^{\alpha_i} \bmod s$。

由于 e 已经被分解成个独立的 e_i，所以 $e_i d_i = 1 (\bmod s)$ 可借助于并行处理来实现[5]。

收稿日期：2004-11-30
基金项目：国防预研基金项目和空军工程大学工程学院优秀博士论文基金资助
作者简介：朱根标(1975-)，男，浙江兰溪人，博士生，主要从事信息安全和复杂系统仿真等研究；
张凤鸣(1963-)男，重庆梁平人，教授，博士生导师，主要从事系统工程研究.

2 PE 文件 RSA 验证加密方法

PE(Portable Executable)文件是 Windows 95/NT 操作系统主流的可执行文件格式,WIN32SDK 的头文件 WINNT. H 中详细定义了 PE 文件格式,它由 DOS Sub、PE 文件头、块表、块、辅助信息块等部分组成,典型的 PE 文件结构见文献[6]。

使用 RSA 加密 PE 文件结构包含三部分工作:完成 RSA 大数运算、实现 RSA 验证代码、修改 PE 文件结构使得 PE 文件执行时先运行验证代码。

加密 PE 文件并让 RSA 验证代码运行,最好用汇编语言实现,但是 RSA 必须用到大数运算(RSA1024 是 1024 位的大整数),用汇编语言编写基本不可能,若采用高级语言编写,则相对容易得多。所以可以用高级语言将 RSA 大数运算的代码编译成 DLL,这样在加到 PE 文件中的汇编代码中可以装入该 DLL,并执行相应的大数运算函数来达到 RSA 验证的功能。

每个处理过的 PE 文件在运行时,需要保证存在执行 RSA 验证的 DLL。具体的方法是将该 DLL 当成数据增加到新的 PE 文件中,由 RSA 验证的 ASM 代码找到这些数据,生成临时 DLL,并在验证完成后删除该临时 DLL。

RSA 验证的流程:①保存原 PE 执行现场;②寻找 PE 尾部的 DLL 数据;③生成临时 DLL 文件并装载;④ RSA 验证得到输出信息 M';⑤ 比较输入信息 M,如果 $M = M'$,则跳转到步骤 6; ⑥ 删除临时 DLL 文件、恢复原 PE 执行现场并切换到程序的 OEP(Original Entry Point),继续执行; ⑦删除临时 DLL 文件并退出。

这部分代码必须由 ASM 编写,并编译成二进制码,其中的重定位和 API 地址等需要在这段代码中完成,以保证代码添加到 PE 文件中后可以直接执行。

修改 PE 文件的流程:①在 PE 结构的最后加入一个 Section,其大小为实现 RSA 验证的 ASM 编译所生成的二进制代码的大小加入 RSA 验证 DLL 的文件大小;② 在新加的 Section 中加入实现 RSA 验证的二进制代码;并在后面加入 DLL 文件;③保存原 PE 的 OEP(original entry point),修改 PE 的 entry point 到新增加 Section 的开始 RVA(relative virtual address);④ 修改 PE 文件头中相关内容以使新的 PE 文件符合 PE 文件结构要求。图 1 ~ 图 4 是 PE 文件在加密前后的比较。

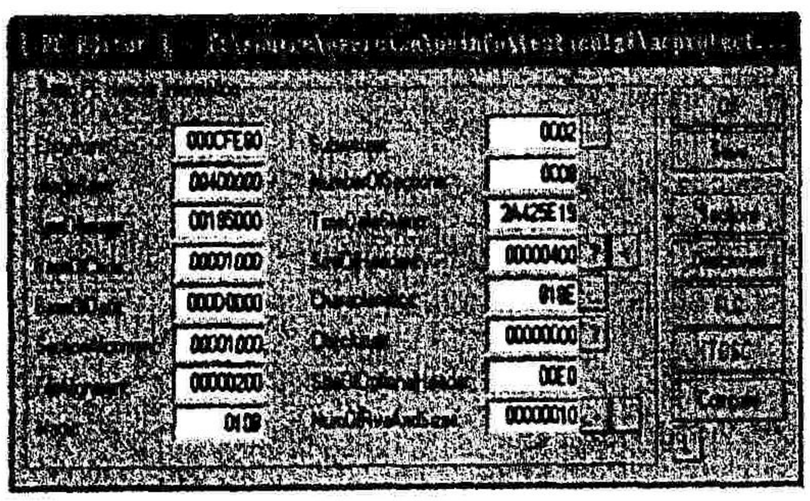

图 1 加密前的 PE 文件头

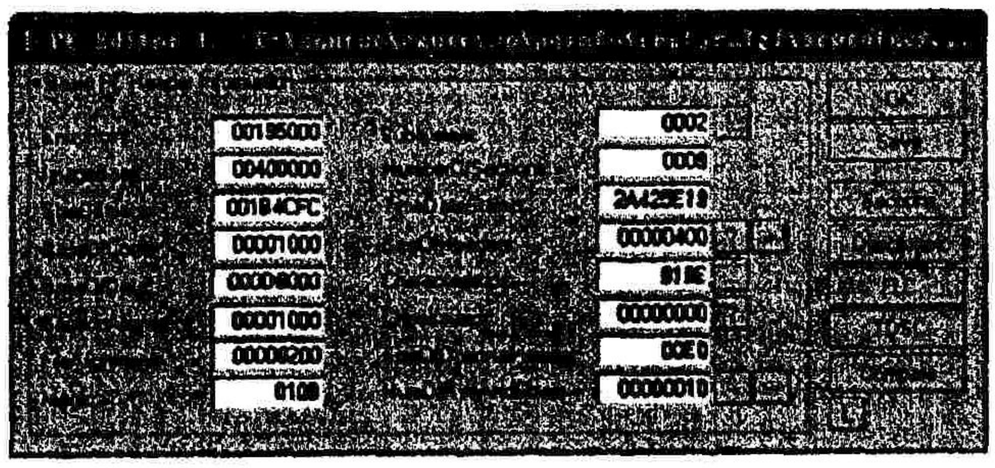

图 2 加密后的 PE 文件头

发生变化的参数有 EntryPoint、SizeOfImage、NumberOfSection。加密后 Section 表增加 perplex 节,Voffset 就是 Entry Point 程序入口地址。Perplex 中包含验证处理的可执行码和作为数据存储的 RSA 验证的 DLL。

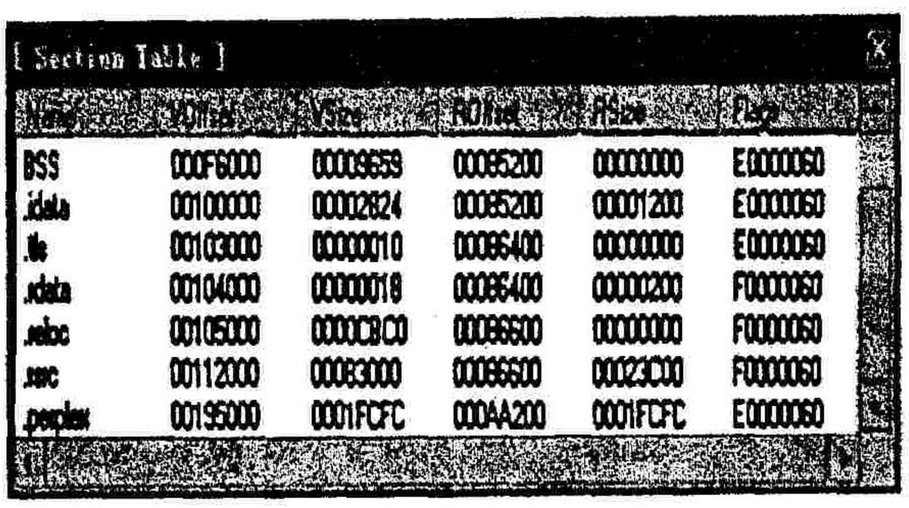

图 3 加密前的 Section 表

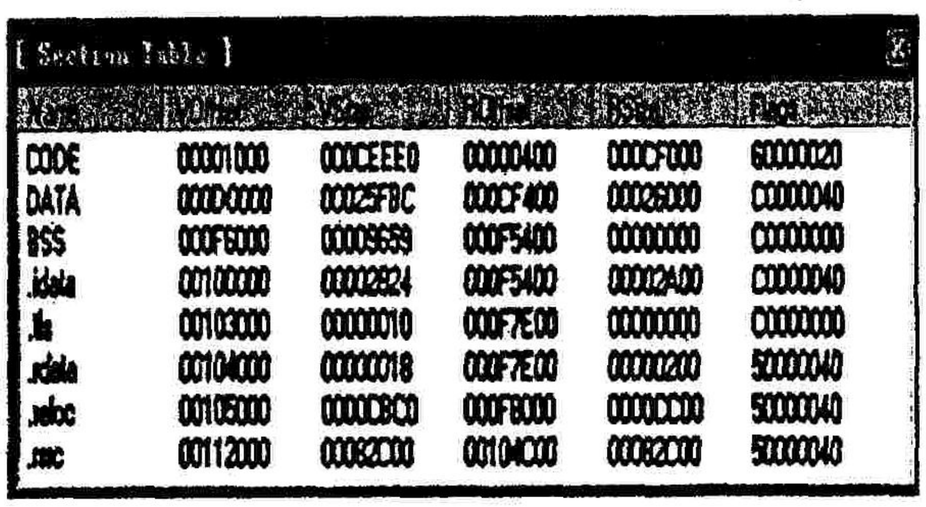

图 4 加密后的 Section 表

3　试验结果

在P4计算机上用DELPHI实现了RSA认证加密算,其加密结果见表1。

明文	密文	明文	密文
20766963746F7279	CE2E97EC7B99F7	20737563656564	E5455DDE0543A0DD
7465737464174641	B39BF3C4F26D47A4	3364657374657374	CAB3B836F62078B

在P4计算机上,本文提出的RSA算法可达到1.326002 Mbps,一般的RSA仅达到0.326391Mbps。在采用相同密码长度(1 024 bit),本文的算法更安全[7]。

4　结束语

本文针对汇编语言难以实现RSA算法大整数运算的特点及实现时要求额外的DLL提供支持这一缺点,基于Derome方法,介绍了一种RSA密钥快速生成方法,采用利用高级语言ASM编译的可执行代码和RSA验证DLL结合修改PE文件的方法可以对现有的Win32的PE文件实现RSA1024甚至RSA2048的验证工作。在不要求软件作者做任何修改的情况下直接给PE可执行文件加上RSA验证功能,而且不要求附带DLL文件,实现对PE文件进行加密并取得了很好的安全强度。此算法在美国最权威的安全测试网上进行测试,以五星级(最高级别)的记录名列第一。

参考文献:

[1] Rivest T L, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public Key Cryptosystem [J]. Communications of the ACM,1978,(21):120 - 126.

[2] 施荣华. 一种针对RSA的冗余二进制算法[J]. 计算机科学技术学报,1996,11(4):416 - 420.

[3] Derome M F A. Generating RSA Keys Without the Euclid Algorithm[J]. Electron Lett, 1993, 29(1):19 - 21.

[4] Knuth D E. Seminumberical Algerithims - the Art of Computer Programming[M]. Reading:Addison - Wesley,1981.

[5] 施荣华,胡湘陵. 一种针对RSA密码系统密钥的快速生成方法[J]. 电子科技大学学报,1999,(4):461 - 462

[6] Pie trek M. Windows95 System Programming Secrets[M]. Hoboken: IDG Books Worldwide, 1995.

[7] 赵全习, 陈西宏, 冯有前. 利用IDEA算法之MA——结构的对合置换[J]. 空军工程大学学报(自然科学版),2001,2(3):48 - 52.

(编辑:姚树峰)

A Validating and Encrypting Algorithm for PE File Based on RSA

ZHU Gen - biao1 , ZHANG Feng - ruing1 , WANG Jin - gan1 , CHEN Hua - yong2

(1. The Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710038, China; 2. PLA Unit 95696 in Chong Qing, Chong Qing 401329, China)

Abstract:This paper analyzes non - symmetrical RSA encrypting algorithm and PE file format, based on RSA fast key generating method of Derome, proposes a method of validating DIL by utilizing advanced language ASM to compile embedded RSA and encrypting PE executable file under Win32 platform by directly modifying PE file. This method is free from the time consuming Euclidean algorithm, can be implemented by parallel processing, and has a robust safety in practice.

Key words:RSA; PE file format; embedded DIL; validating and encrypting; data security