文章编号:1001 - 9081(2009)S1 - 0077 - 03

DES 差分特征的分析与搜索

顾海文,祝跃飞,康 绯,师国栋
(信息工程大学 信息工程学院,郑州 450002)
(guhaiwen95@sohu.com)

摘 要:通过对已有的 DES 各轮的差分特征进行分析,发现了现有的 DES 高概率差分特征存在的特有现象,利用这些特点对以前的差分特征搜索算法进行改进,设计出了新的 DES 差分特征的搜索算法。经过程序实现,新的算法不仅能够找到现有的所有差分特征,还找到了一个目前没有的五轮特征,该特征的概率比现有的五轮特征的最大概率大。新搜索算法比原来的算法快。

关键词:分组密码;迭代;差分特征
中图分类号: TP309 **文献标志码**:A

Analysis and search of differential characters

GU Hai-wen, ZHU Yue-fei, KANG fei, SHI Guo-dong
(*Institute of Information Engineering, Information Engineering University, Zhengzhou Henan* 450002, *China*)

Abstract: By analyzing DES' s existing differential characters, the traits were found. Based on those traits a new search algorithm was designed. The new algorithm could not only find all differential characters in existence, but also find a five rounds differential character whose probability is higher. And the new algorithm was faster than the old ones.

Key words: cryptosystems; iterated; differential characters

0 引言

1990 年,Eli Biham 和 Adi Shamir 针对数据加密算法(Data Encryption Standard,DES)提出了差分密码分析[1]。它是迄今已知的攻击迭代分组密码体制最有效的方法之一。

1994 年 Matsui 提出了 DES 概率线性关系式的算法[2],由于寻找差分特征于线性关系式在本质上是很类似的东西,所以该算法经过部分改变也同样适用于对 DES 的高概率差分特征的搜索。1995 年 K. Ohta 等人提出了 Matsui 的搜索算法中存在的两个问题[7],在原搜索算法基础上提出了改进方法。张焕国等人对循环轮特征进行了一些分析[4],并给出了一个限制输入权重的差分搜索算法。

这些算法的都是以穷举为基础,通过对搜索条件的限制在一定程度上降低了特征搜索的复杂度,但是对于高轮的差分特征,由于还是在整个差分空间中搜索,加上搜索轮数太高,搜索的运算量会成指数级递增。本文通过对 DES 各轮差分攻击所使用的特征进行分析,发现了其中的规律,并给出了寻找这种具有固定结构的差分特征的算法,这种算法减少了需要搜索的轮数,降低了特征搜索的复杂度。

1 差分密码分析方法简介

差分分析针对 DES 在低轮上的攻击是非常成功的。在此先给出几个基本概念和引理。

定义 1[5] r 轮特征 Ω 是一个差分序列 $a_0,a_1,\cdots,a_r$,其中 a_0 是明文对 Y_0 和 Y_0^* 的差分,$a_i(1 \leqslant i \leqslant r)$ 是第 i 轮输出 Y_i 和 Y_i^* 的差分。R 轮特征 $\Omega = a_0,a_1,\cdots,a_r$ 的概率 p^Q 是指在子密钥 $K_1,K_2,\cdots,K_r$ 独立、均匀随机时,明文对 Y_0 和 Y_0^* 的差分为 a_0 的条件下,第 i 轮($1 \leqslant i \leqslant r$)输出 Y_i 和 Y_i^* 的差分为 a_i 的概率。

引理 1[4] 在明文、密钥独立均匀随机下,r 轮特征的概率等于单轮特征概率的乘积。

定义 2[4] r 轮特征 $\Omega_r = a_0,a_1,\cdots,a_r$ 称之为循环轮特征,是指如果 $a_0 = a_r$,r 为该循环轮特征的周期。

定理 1[4] 设周期为 r 的循环轮特征 $\Omega = a_0,a_1,\cdots,a_r$ 的概率为 p^Q,a_r 经过 DES 的扩展置换后含有 m 个非零项,则利用该轮特征对 DES 可以作 $k \times r + 2$ 轮差分分析,能够得到全部 S 盒的子密钥,作 $k \times r + 3$ 轮分析时只能得到 k 个 S 盒的子密钥,其分析概率为 p^Q 的 k 次方。

2 DES 差分特征

2.1 DES 差分特征分析

我们先分析一下目前对 DES 的降低轮的[1]攻击和全十六轮的攻击[5]中使用的差分特征:

四轮攻击使用的是两个三轮差分特征[1]:

概率为 1

(20 00 00 00,00 00 00 00) - (20 00 00 00,00 00 00 00)

概率为 1

(02 22 22 22,00 00 00 00) - (02 22 22 22,00 00 00 00)

六轮攻击使用的是两个三轮差分特征[1]:

概率为 0.062 5

(40 08 00 00,04 00 00 00) - (04 00 00 00,00 00 00 00) - (00 00 00 00,04 00 00 00) - (40 08 00 00,04 00 00 00)

概率为 0.062 5

(00 20 00 08,00 00 04 00) - (00 00 04 00,00 00 00 00) -

收稿日期:2008 - 12 - 07;修回日期:2009 - 03 - 07。 基金项目:国家 863 计划项目(2007AA01Z471)。

作者简介:顾海文(1985 -),女,江苏如皋人,硕士研究生,主要研究方向:网络密码、计算机网络; 祝跃飞(1962 -),男,浙江杭州人,教授,博士生导师,主要研究方向:网络密码、计算机网络; 康绯(1972 -),女,副教授,主要研究方向:网络密码、计算机网络; 师国栋(1984 -),男,河南周口人,硕士研究生,主要研究方向:网络密码、计算机网络。

(00 00 00 00,00 00 04 00) - (00 20 00 08,00 00 04 00)

八轮攻击使用的是一个五轮差分特征[1]：

概率为9.5367E-5

(40 5c 00 00,04 00 00 00) - (04 00 00 00,00 54 00 00) - (00 54 00 00,00 00 00 00) - (00 00 00 00,00 54 00 00) - (00 54 00 00,04 00 00 00) - (40 5c 00 00,04 00 00 00)

十五轮和十六轮的攻击使用的是同一个差分特征[6]：

概率为4.2724E-3

(00 00 00 00,19 60 00 00) - (19 60 00 00,00 00 00 00) - (00 00 00 00,19 60 00 00)

容易发现在十五轮和十六轮攻击时使用的特征是循环轮特征。循环轮特征有个好处,就是在多轮的高概率差分难以搜索时,可以用低轮的差分特征进行循环扩展(如十五轮和十六轮的攻击)。

循环轮思想的根本就是由少轮的差分特征拼接出多轮的差分特征,随着密码算法的设计越来越复杂,高概率差分特征越来越难搜索到,这种思想将得到广泛的应用。这种思想在最小活动S盒的估计[7]上也可以进行应用,将很有可能得到突破。

在降低轮的攻击中使用的特征都有两个特点:1)中间一轮的输入差分为0;2)特征前半部分和后半部分存在对称关系。将会在2.2节证明这两个特点的可利用性。用这两个特点,就可以将奇数轮的高概率特征搜索降低一半的复杂度。

2.2 DES差分特征自动搜索算法

利用差分对DES进行攻击,关键在于找到一个高概率差分特征。

基于2.1节对DES攻击使用的差分特征的特点分析,我们设计了一个DES的特征搜索算法。

假设 假设特征的中间一轮的输入差分为0,即若特征为一个$2r+1$轮特征,则约定第$r+1$的输入为0,若循环特征为一个$2r$轮特征,则约定第$r+1$轮的输入为0。

定理2 两轮的循环特征概率最大的必为图1或图2所示的两种结构。

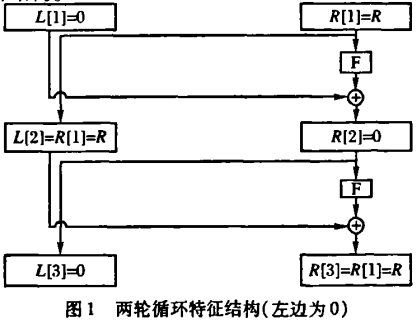


图1 两轮循环特征结构(左边为0)

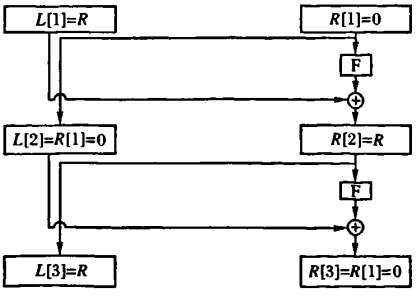


图2 两轮循环特征结构(右边为0)

证明 假设特征$(a,b)-(c,d)-(e,f)$是一个两轮的循环特征。

根据循环特征的定义,那么该特征等价于特征$(a,b)-(c,d)-(a,b)$。

根据DES的加密结构可知$c=b$并且$d=a$,所以该特征又可写成$(a,b)-(b,a)-(a,b)$。

而该特征的概率为$p(x=b,y=0)\times p(x=a,y=0)$。

若b不等于0且a也不等于0,

那么$p(x=b,y=0)<1$且$p(x=a,y=0)<1$,

而$p(x=0,y=0)=1$,

那么$p(x=b,y=0)\times p(x=a,y=0)<p(x=a,y=0)\times p(x=a,y=0)$且$p(x=b,y=0)\times p(x=a,y=0)<p(x=b,y=0)\times p(x=a,y=0)$。

显而易见,图1和图2的两种结构是等价的。

证毕

定理3 根据假设,偶数轮的循环差分特征必为图1所示结构的循环。

证明 设要搜索的是$2r$轮的循环差分特征,

由假设知$R[r+1]=0$,令$L[r+1]=R$

那么:

$R[r+2]=L[r+1]\oplus F(R[r+1])=R$

$L[r+2]=R[r+1]=0$

$R[r]=L[r+1]=R$

$L[r]=F(R[r])\oplus R[r+1]=F(R)$

由定义2,得到$L[r]=0$

同上推理,可以看出,特征将会是$(0,R)-(R,0)-(0,R)$的循环,概率则为特征$(0,R)-(R,0)-(0,R)$的概率的r次方。

证毕

在这种情况下可知,偶数轮的循环轮特征及其概率是很容易得到的。

由偶数轮的循环结果再加一轮或减一轮就可以轻易得到奇数轮的差分特征,但是这个差分特征不一定是概率最高的。

定理4 根据假设,那么$2r+1$轮的高概率循环轮特征必为图3所示的结构,该特征的概率则为一半差分特征(以图3所示的虚线为分界)概率的平方。

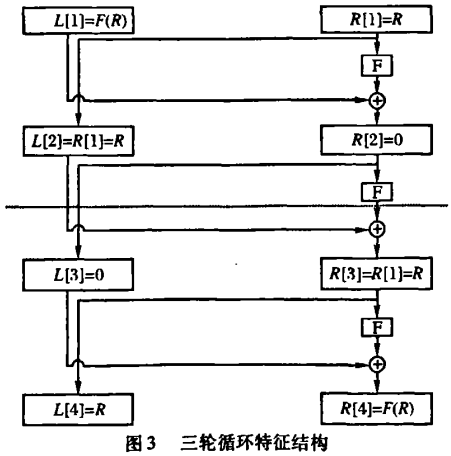


图3 三轮循环特征结构

证明 设要搜索的是$2r+1$轮的差分特征

由假设知,$R[r+1]=0$,令$L[r+1]=R$,

则$R[r+2]=R$,$L[r+2]=0$。

由于 DES 密码是对称的,它的加解密的结构是一致的,所以特征1-2-3-4的概率和特征4-3-2-1的概率是相等的[3],把这个$2r+1$轮的差分特征从中间一分为二(如图3虚线所示),那么上面一半的差分可以为下面一半的差分的反顺序差分。

由图3可知:

图3所示差分特征的概率 = 一半差分特征的概率^2 × 差分特征$(0,R)-(R,0)$的概率。

因为差分特征$(R,0),(0,R)$的概率为1,

所以图3所示差分特征的概率 = 一半差分特征的概率^2。

证毕

那么在搜索过程中,只要搜索符合结构的上半部分或者下半部分就可以了。下面的算法给出的是下半部分的搜索算法。根据约定$L[0]=0$,可以在算法中直接应用。

算法详细过程:

$X[i]$代表第i轮F函数的输入差分,$Y[i]$代表第i轮F函数的输出差分,$p[i]$代表搜索过程中第i轮的概率,$B[i]$代表已知的i轮的,$B0$代表目前已搜索到的最大的差分概率,$L[i]$和$R[i]$中存放的是目前搜索到的概率最大的差分。

算法1　$2r+1$轮循环轮特征的下半部分的搜索算法(即r轮):

1) 对任意输入差分$X[1]$和输出差分$Y[1]$,令$p[1]=(X[1],Y[1])$,

如果$p[0]\times B[r-1]>=B0$,则执行第2)步。

程序结束。

2) 对任意输出差分$Y[2]$,令$X[2]=Y[1]$,$p[2]=(X[2],Y[2])$,

如果$p[1]\times p[2]\times B[r-2]>=B0$,则执行第3)步。

返回到上轮程序。

i: 对任意输出差分$Y[i](2<i<r)$,令$X[i]=X[i-2]\hat{}Y[i-1]$,$p[i]=(X[i],Y[i])$,

如果$p[1]\times p[2]\times\cdots\times p[i]\times B[r-i]>=B0$,则执行$i+1$步。

返回到上轮程序。

r: $X[r]=X[r-2]\hat{}Y[r-3]$,$p[r]=\max(X[r],Y[r])$

如果$p[1]\times p[2]\times\cdots\times p[r]>=B0$,

那么令:

$B0=p[1]\times p[2]\times\cdots\times p[r]$

$L[1]=0$

$R[0]=X[0]$

$L[i]=R[i-1]$

$R[i]=X[i]$

打印$L[i]$和$R[i]$和$B0$至 *.txt 中。

返回到上轮程序。

搜索结果:存放在 *.txt 中。

由定理4,将这个差分特征根据图3的结构向上扩展一倍,就是想要的$2r+1$轮的循环差分特征了,概率为$B0$的平方。

将搜索结果减一轮就可以得到偶数轮的高概率差分了。

该算法是以 Matsui 提出的算法[2]为基础进行了改进,由于该算法只用求一半的差分特征,所以大大减少了搜索算法的运算量。该算法的思想进行适当改变也可用于其他的密码算法。

2.3　结果分析

根据算法一易见,奇数轮的特征搜索其实只是搜索了原来 Matsui 提出的算法的一半,速度的提高是显而易见的。

在其他条件完全相同的情况下,三轮的运行时间等于原来的算法一轮的运行时间,五轮的运行时间等于原来的算法两轮的运行时间。

搜索具体结果如下(文献[1]中有的结果不再列出):

二轮的循环差分特征概率最大的有两个,概率均为4.2724E-3。

特征一:(00 00 00 00,1B 60 00 00) - (1B 60 00 00,00 00 00 00) - (00 00 00 00,1B 60 00 00)。

攻击中所用的三轮的差分特征是 DES 唯一的两个概率最大的三轮差分特征,稍小一点的概率为0.04785。

特征二:(00 10 00 01,00 00 00 60) - (00 00 00 60,00 00 00 00) - (00 00 00 00,00 00 00 60) - (00 00 00 60,00 10 00 01)。

特征三:(40 00 40 10,02 00 00 00) - (02 00 00 00,00 00 00 00) - (00 00 00 00,02 00 00 00) - (02 00 00 00,40 00 40 10)。

特征四:(00 00 40 10,06 00 00 00) - (06 00 00 00,00 00 00 00) - (00 00 00 00,06 00 00 00) - (06 00 00 00,00 00 40 10)。

特征五:(00 80 82 00,60 00 00 00) - (60 00 00 00,00 00 00 00) - (00 00 00 00,60 00 00 00) - (60 00 00 00,00 80 82 00)。

由文献[1]可知五轮最好的差分概率为率为9.5367E-5,找到了一个概率比他大的差分,概率为1.0514E-004。

特征六:(40 00 46 D0,02 00 00 00) - (02 00 00 00,00 00 06 C0) - (00 00 06 C0,00 00 00 00) - (00 00 00 00,00 00 06 C0) - (00 00 06 C0,02 00 00 00) - (02 00 00 00,40 00 46 D0)。

还有一个概率相同的特征,概率为9.5367E-005。

特征七:(40 3c 00 00,04 00 00 00) - (04 00 00 00,00 34 00 00) - (00 34 00 00,00 00 00 00) - (00 00 00 00,00 34 00 00) - (00 34 00 00,04 00 00 00) - (40 3c 00 00,04 00 00 00)。

为了验证结果的正确性,对以特征七和特征六两个差分特征分别生成了10组10^6个随机数对,加密后的差分结果数据如表1所示。

表1　特征七和特征六的验证结果

组号	特征七	特征六
1	86	105
2	97	111
3	95	103
4	97	106
5	82	104
6	92	109
7	100	113
8	90	109
9	94	108
10	96	107
平均值	93	107

根据表1中的数据,可以判断算法一得到的结果都是正确的。

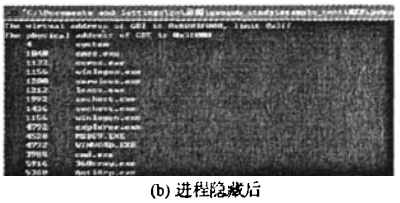
(下转第88页)

基址是0x8003f000限长是0x3ff,处于系统内核空间,受系统保护用户不能直接对其进行相关的读写操作。从Windows 2000开始,系统提供了\Device\PhysicalMemory对象,但是该对象的安全描述符规定只有SYSTEM可以使用,普通用户和管理员都没有权限使用,我们通过NtOpenSection、GetSecurityInfo、SetEntriesInAcl、SetSecurityInfo等函数给这个对象添加另一个ACL,使对其拥有完全的读写权限,从而可以对任意物理内存进行读写。最后把GDT表的物理地址(线性地址在0x80000000和0xA0000000之间的话,其物理地址就是线性地址的值与0x1FFFF000相与的结果)通过该对象映射到我们进程空间并添加相应的调用门。

通过调用该调用门,就可以使用户程序的特权级由ring 3到ring 0的提升,就可以实现对用户态空间和内核空间的任意访问,我们先获得进程控制块链表的表头PsActiveProcessHead,它可以用搜索代码的方法来取,也可以简单的用kd得到它的地址,然后遍历进程控制块链表,找到需要隐藏的进程控制块,把它从进程双向链表中摘除下来,就可以达到进程的隐藏目的。

通过段寄存器FS指向的数据结构我们可以找到当前线程的TEB,再由TEB指向的数据结构可以找到当前进程的KPEB,在KPEB结构偏移0x12c处存放的就是当前进程的Token了,我们用SYSTEM进程的Token替换当前进程的Token,就可以使当前进程拥有了SYSTEM权限。实验结果如图5所示。

(a) 进程隐藏前



(b) 进程隐藏后

图5 实验结果

由图5可以看出,通过该方法我们自己进程my_rootkit.exe已经被隐藏,达到了进程隐藏的目的。我们再在当前进程中通过shell函数运行regedit.exe打开注册表编辑器,因为[HKEY_LOCAL_MACHINE\SAM\SAM]注册表项默认只有System权限可以进行查看和修改,通过验证表明我们可以展开该注册表项,说明regedit.exe是以System权限运行的。从而证明我们自己进程也拥有了System权限。在实验中我们还通过NtCreateSymbolicLinkObject函数创建符号连接对象,间接地使用\Device\PhysicalMemory对象,从而躲过大部分软件对ZwOpenSection函数的监控,实验结果表明该方法可以有效地躲过360安全卫士、卡巴斯基、冰刃、诺顿等杀毒软件。

4 结语

基于调用门的进程隐藏技术可以使用户程序通过安装调用门来实现程序特权级由ring 3到ring 0的提升,从而可以达到对系统内核空间的任意访问,如修改进程链表和进程访问令牌等,该方法不需要通过加载驱动的方式,也不需要调用以被监控的一些敏感系统接口函数,因此隐蔽性更好,更难被发现。除了以上的应用外,调用门在Rootkit方面还有很广的应用,如直接修改SSDT表、IDT表,直接操作端口等,在控制方面也有很广泛的应用。

参考文献:

[1] DENNING D E. Information Warfare and Security[M]. Boston: Addison Wesley, 2001.

[2] 齐琪. Windows下EPA技术的研究与改进[M]. 湖北:华中科技大学, 2006.

[3] 王建华, 张焕生, 侯丽坤. Windows核心编程[M]. 北京:机械工业出版社, 2001.

[4] LEVINE J G, GRIZZARD J B, HUTTO P W, *et al*. A methodology to characterize kernel level rootkit exploits that overwrite the system call table[C]// Proceeding of IEEE. SoutheastCon: IEEE, 2004: 25-31.

[5] 尤晋元, 史美林. Windows操作系统原理[M]. 北京:机械工业出版社, 2001.

[6] 冯万利. 基于内核入侵的木马设计与实现[J]. 微计算机信息, 2006, 22(18): 120-122.

[7] 姜新, 汪秉文, 瞿坦. Linux核心模式下的用户进程研究[J]. 计算机工程与应用, 2004, 40(4): 118-120.

[8] 赵炯. Linux内核完全剖析[M]. 北京:机械工业出版社, 2006.

[9] 张银奎. 软件调试[M]. 北京:电子工业出版社, 2008.

(上接第79页)

3 结语

本文详细分析了DES各轮差分攻击使用的特征,研究了这些特征的共同特点和结构,根据这些特点和结构提出了一个DES的差分特征搜索算法,降低了搜索的复杂度和时间,在2.3节中列举出了搜索结果,除了DES常用的高概率差分特征,还搜索到了别的较好的特征,五轮的特征也搜索到了一个比常用特征概率大的特征。

参考文献:

[1] BIHAM E, SHAMIR A. Diferential cryptanalysis of DES — Like cryptosystems [J]. Journal of Cryptology, 1990, 4(1): 3-72.

[2] MATSUI M. On Correlation between the order of S-boxes and the strength of DES[C]// Advances in Cryptology Eurocrypto'94. Perugia, Italy: [s. n.], 1994: 356-375.

[3] OHTA K, MOTIAL S, AOKI K. Improving the searching algorithm for the best linear expression [EB/OL]. [2008-10-10]. http://dsns. csie. nctu. edu. tw/research/crypto/HTML/PDF/C95/157. PDF.

[4] 张焕国, 冯秀涛, 覃中平, 等. 演化密码与DES的演化研究[J]. 计算机学报, 2003, 26(12): 1678-1684.

[5] 李贞, 吕述望, 王永传. 差分分析中的特征概率计算问题研究[J]. 电子与信息学报, 2003, 25(8): 1108-1113.

[6] BIHAM E, SHAMIR A. Differential cryptanalysis of full 16-round DES [C]// Advances in Cryptology — Crypto'92, LNCS 740. Berlin: Springer-Verlag, 1993: 487-496.

[7] 曾祥勇, 张焕国, 刘合国. 高级加密标准的差分特征[J]. 武汉大学学报: 2004, 50(1): 60-64.

[8] 李超, 沈静. Camellia的差分和线性迭代特征[J]. 电子学报: 2005, 33(8), 1345-1348.

[9] 冯登国. 密码分析学[M]. 北京, 清华大学出版社, 2000: 15-32.