ISCAS 中国科学院软件研究所学术年会'2023
暨计算机科学国家重点实验室开放周
学术论文

x86指令架构可打印shellcode的最小信息冗余度生成算法

Least Information Redundancy Algorithm of Printable Shellcode Encoding for x86

周园丁 指导老师：张阳，程亮
E-mail：yuanding2021@iscas.ac.cn

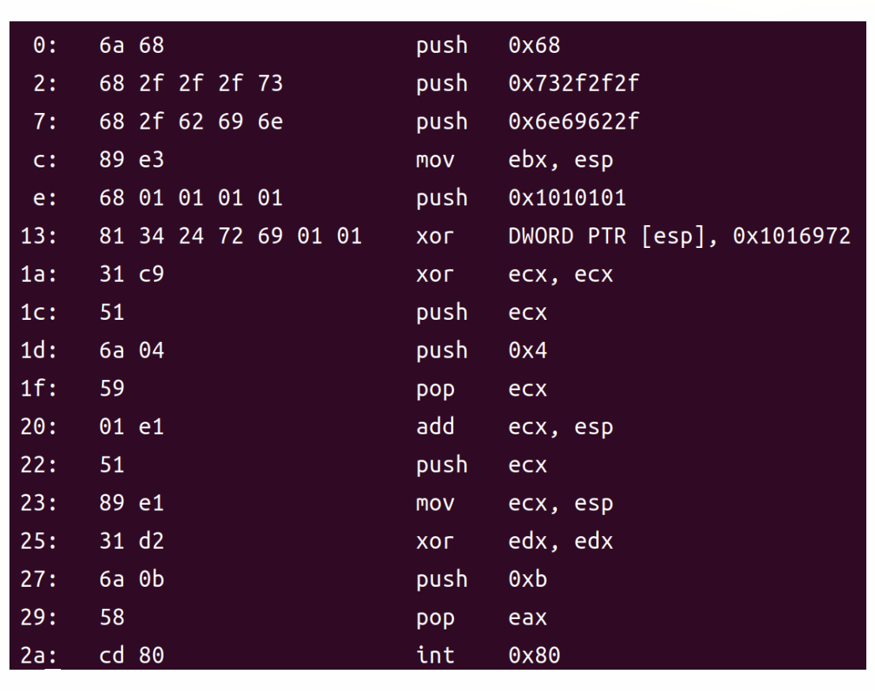
研究背景

实际漏洞利用中，未处理的shellcode的使用受到限制，例如在字符串中表示结尾的0字节不能出现在shellcode中。在浏览器内核、网络协议的漏洞利用中，可打印的ASCII字符更容易嵌入到正常数据流中并被程序接受，因此往往需要将shellcode编码或加密为只含可打印字符的形式，但这常常会增加整个shellcode的体积。我们提出了理论上信息冗余度最小的编码算法，并实现了对应的工具Lycan，极大地改进了编码效率，减少了shellcode的尺寸。

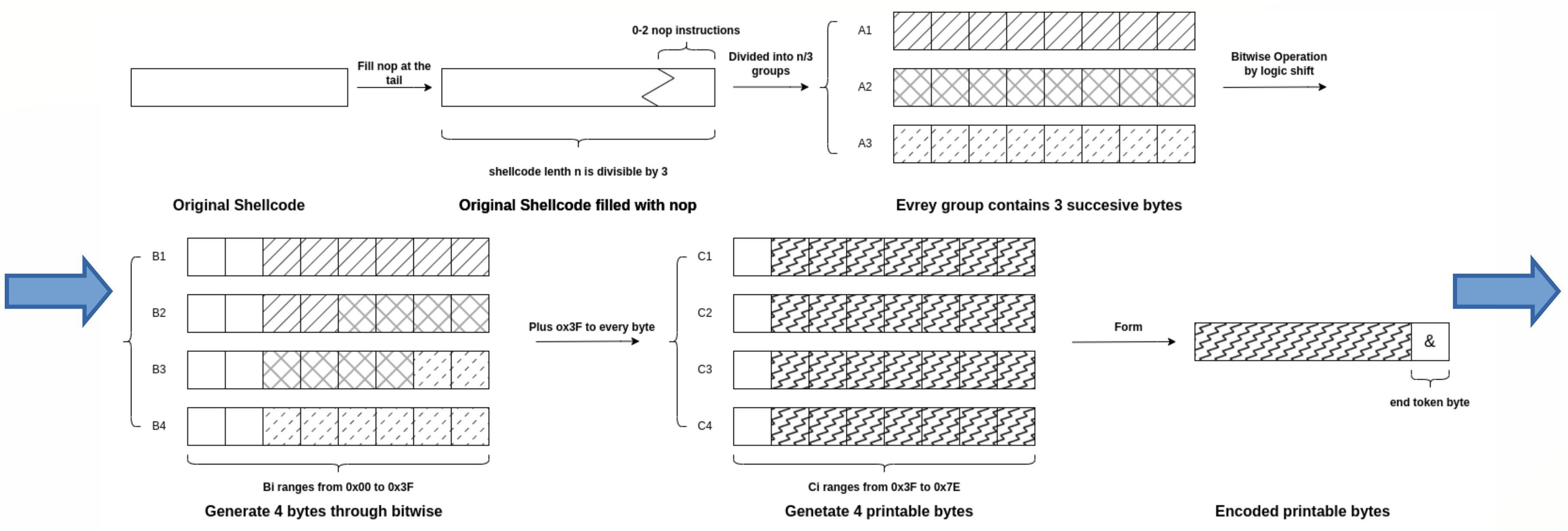
本文创新

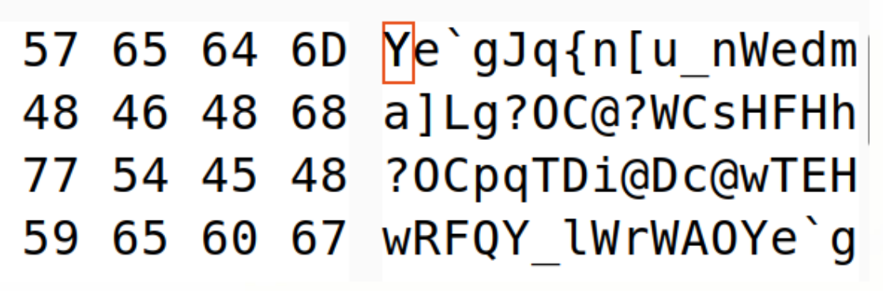
本文证明了可打印shellcode编码算法的理论最低信息冗余度为0.25（每字节最多使用6比特用于编码），而目前可打印shellcode 编码算法均未达到最低信息冗余度。本文提出了信息冗余度为理论最低的可打印shellcode编码算法，编码过程将每3个连续的字节编码为4个字节，并且实现了对应的工具Lycan。Lycan由能在运行时解码的decoder以及编码后的shellcode组成。解码完成后，控制流跳转至原本的shellcode。

实验流程



```
 0:   6a 68                   push   0x68
 2:   68 2f 2f 2f 73          push   0x732f2f2f
 7:   68 2f 62 69 6e          push   0x6e69622f
 c:   89 e3                   mov    ebx, esp
 e:   68 01 01 01 01          push   0x1010101
13:   81 34 24 72 69 01 01    xor    DWORD PTR [esp], 0x1016972
1a:   31 c9                   xor    ecx, ecx
1c:   51                      push   ecx
1d:   6a 04                   push   0x4
1f:   59                      pop    ecx
20:   01 e1                   add    ecx, esp
22:   51                      push   ecx
23:   89 e1                   mov    ecx, esp
25:   31 d2                   xor    edx, edx
27:   6a 0b                   push   0xb
29:   58                      pop    eax
2a:   cd 80                   int    0x80
```





```
57 65 64 6D Ye`gJq{n[u_nWedm
48 46 48 68 a]Lg?OC@?WCsHFHh
77 54 45 48 ?OCpqTDi@Dc@wTEH
59 65 60 67 wRFQY_lWrWAOYe`g
```

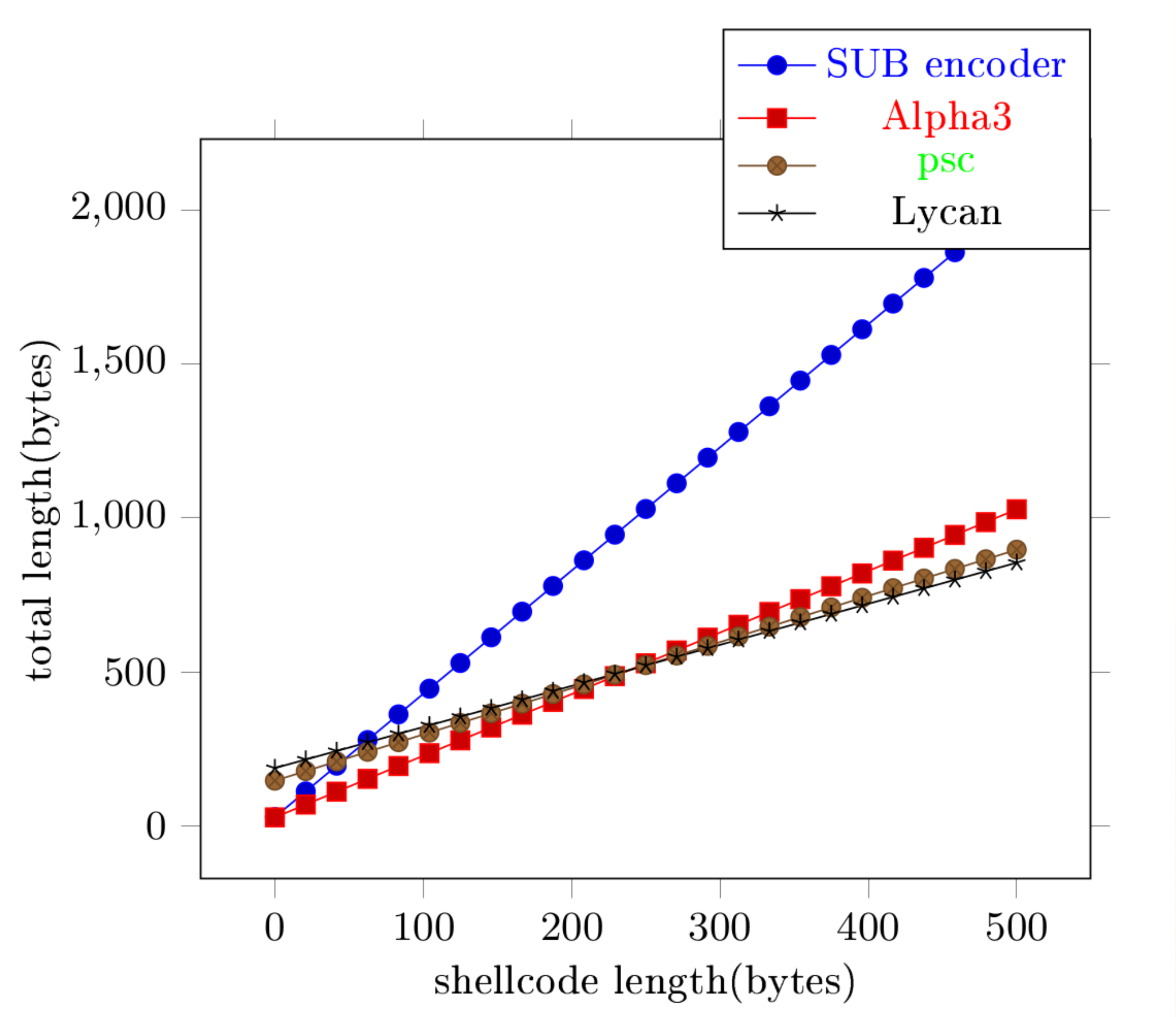
未编码的
shellcode

编码过程

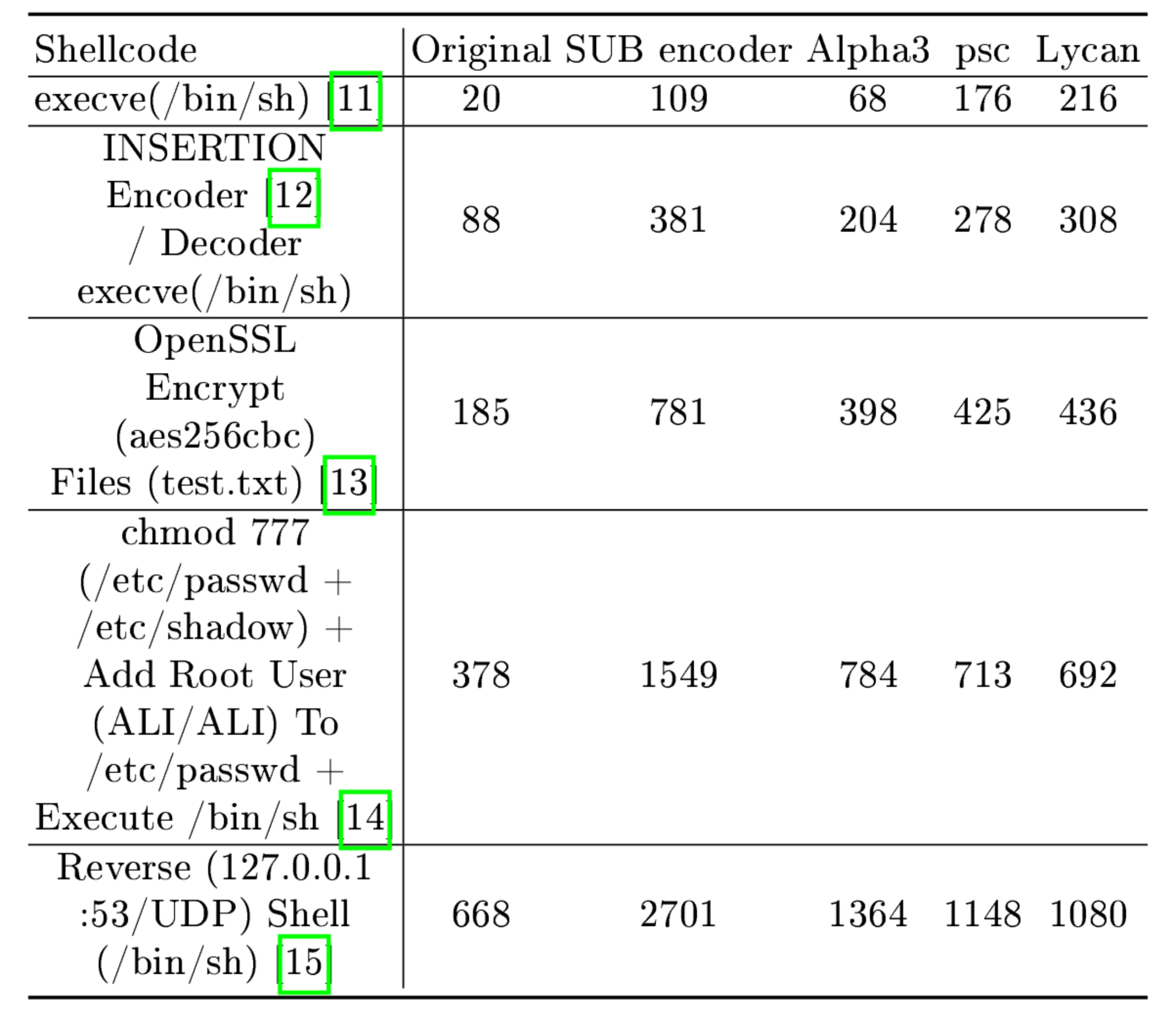
编码后的可打印
shellcode

原始的shellcode被编码为只包含可打印字符的shellcode，并且在执行时会被解码为原始的shellcode，完成后跳转到shellcode中执行

实验效果



与Metasploit中的SUB encoder、Alpha3相比，Lycan极大减少了编码后的shellcode信息冗余度



Shellcode	Original	SUB encoder	Alpha3	psc	Lycan
execve(/bin/sh) [11]	20	109	68	176	216
INSERTION Encoder [12] / Decoder execve(/bin/sh)	88	381	204	278	308
OpenSSL Encrypt (aes256cbc) Files (test.txt) [13]	185	781	398	425	436
chmod 777 (/etc/passwd + /etc/shadow) + Add Root User (ALI/ALI) To /etc/passwd + Execute /bin/sh [14]	378	1549	784	713	692
Reverse (127.0.0.1 :53/UDP) Shell (/bin/sh) [15]	668	2701	1364	1148	1080

与不同可打印shellcode编码工具的在真实shellcode相比，Lycan算法极大地减少了编码后的shellcode尺寸