

IOT安全三十六计

@安恒海特实验室

· whoami

- 安恒安全研究院海特实验室
- 关注智能硬件安全、IOT安全、二进制漏洞挖掘



Agenda

- 瞒天过海
- 无中生有
 - 反间计
- GeekPwn分享

· 漏洞实例分享

一、瞒天过海

— 本指光天化日之下不让天知道就过了大海。形容极大的欺骗和谎言，什么样的欺骗手段都使得出来。

— 逻辑漏洞 && 命令注入 → RCE

· 漏洞实例分享

1、后台命令注入

.text:0040ADBA	BLX	memset
.text:0040ADBE	LDR	R3, [R6]
.text:0040ADC0	MOV.W	R1, #0x100 ; maxlen
.text:0040ADC4	LDR	R2, =aMountTNfsSSSOI ; "mount -t nfs %s:%s %s -o intr,timeo=3,
.text:0040ADC6	ADD	R0, SP, #0x120+s ; s
.text:0040ADC8	STR	R3, [SP,#0x120+var_11C]
.text:0040ADCA	LDR	R3, [R5]
.text:0040ADCC	STR	R3, [SP,#0x120+var_120]
.text:0040ADCE	LDR	R3, [R7]
.text:0040ADD0	BLX	snprintf

```

if ( v3 >= 0 )
{
    if ( !v3 )
    {
        execl("/bin/sh", "sh", "-c", v15, 0);
        perror("vfork2");
        exit(127);
    }
}

```

exec家族: `execve()`、`execl()`、`execvp()`... `system()`、
`popen()`

· 漏洞实例分享

2、逻辑漏洞

strstr()的trick

strstr()函数的定义:

The C library function **char *strstr(const char *haystack, const char *needle)** function finds the first occurrence of the substring **needle** in the string **haystack**. The terminating **'\0'** characters are not compared.

· 漏洞实例分享

2、逻辑漏洞

```
kingdomdeMacBook-Pro:tmp kingdom$ cat 002.c
```

```
#include <stdio.h>
#include <string.h>
```

```
int main()
```

```
{
```

```
    printf("%p\n", strstr(
    return 0;
```

```
}
```

```
kingdomdeMacBook-Pro:tmp king
```

```
0x0
```

```
kingdomdeMacBook-Pro:tmp king
```

```
kingdomdeMacBook-Pro:tmp kingdom$ cat 001.c
```

```
#include <stdio.h>
```

```
#include <string.h>
```

```
int main()
```

```
{
```

```
    printf("%p\n", strstr("aaa", ""));
```

```
    return 0;
```

```
}
```

```
kingdomdeMacBook-Pro:tmp kingdom$ ./001
```

```
0x102712fa4
```

· 漏洞实例分享

2、逻辑

千里之

int a

{

}

```
kingdomdeMacBook-Pro:tmp kingdom$ cat 003.c
```

```
#include <stdio.h>
```

```
#include <string.h>
```

```
int main()
```

```
{
```

```
    printf("%p\n", strstr("", ""));
```

```
    return 0;
```

```
}
```

```
kingdomdeMacBook-Pro:tmp kingdom$ ./003
```

```
0x103bebf4
```

```
kingdomdeMacBook-Pro:tmp kingdom$
```

```
...
```


· 漏洞实例分享

二、无中生有

- 本指本来没有却硬说有。现形容凭空捏造。
- 安装内核模块bypass安全措施。

· 漏洞实例分享

1、Squashfs

- Squashfs

SquashFS 也是一个只读的文件系统，它可以将整个文件系统压缩在一起，存放在某个设备，某个分区或者普通的文件中。

- 文件系统不可写

- /var/tmp可写：tftp上传

· 漏洞实例分享

2、智能设备文件系统加密

- 自定义的enc文件系统

```
ash: ./x: Success
/var/tmp # ash

BusyBox v1.18.4 (2017-01-20 15:07:12 CST) built for armv7l
Revision: 23493
Enter 'help' for a list of built-in commands.

/var/tmp # ./x
ash: ./x: Read-only file system
/var/tmp # ./x
ash: ./x: Success
/var/tmp # █
```


· 漏洞实例分享

2、智能设备文件系统加密

- 改造已有的ko模块实现任意代码执行。

```
/var/tmp # insmod ./fake.ko
```

```
10:49:38|You have been pwned! This is a fake module
```



· 漏洞实例分享

三、反间计

- 原指使敌人的间谍为我所用，或使敌人获取假情报而有利于我的计策。后指用计谋离间敌人引起内讧。
- 利用厂商预留的后门或调试接口。

漏洞实例分享

— 2013年D-link后门

— 在user-agent中与特殊字符串比较成功就可以bypass认证界面

```

nop
addiu $a1, (aGraphic - 0x470000) + "graphic/"
sw $v0, 0x100+var_490($sp)
lc $t9, strstr
nop
jalr $t9 ; strstr
nop
lw $gp, 0x3B8+saved_gp($sp)
nop
lc $a1, 0x470000
nop
addiu $a1, (aPublic - 0x470000) + "public/"
lw $v0, end
li $v1, 1

```

```

lw $a0, 0x00($t0)
lc $t9, stricmp
nop
jalr $t9 ; stricmp
nop
lw $gp, 0x3B8+saved_gp($sp)
nop
lc $a1, 0x470000
nop
addiu $a1, (aXr1set_readt_0 - 0x470000) + "xmlset_readt00000128840yht1do"
lw $v0, end
li $v1, 1

```

```

lw $a0, 0x00($t0)
lc $t9, strcmp
nop
jalr $t9 ; strcmp
nop
lw $gp, 0x3B8+saved_gp($sp)
beqz $v0, end
li $v1, 1

```

```

lw $a0, 0x00($t0)
lw $a1, 0xE0($t0)
lc $t9, check_login
nop
jalr $t9 ; check_login
nop
lw $gp, 0x3B8+saved_gp($sp)
move $a0, $a0
addiu $a1, $sp, 0x100+var_2A0
lw $v0, end
li $v1, 1

```


· 漏洞实例分享

— 某智能设备调试接口

PORT	STATE	SERVICE	VERSION
554/tcp	open	rtsp	
5555/tcp	open	freeciv?	

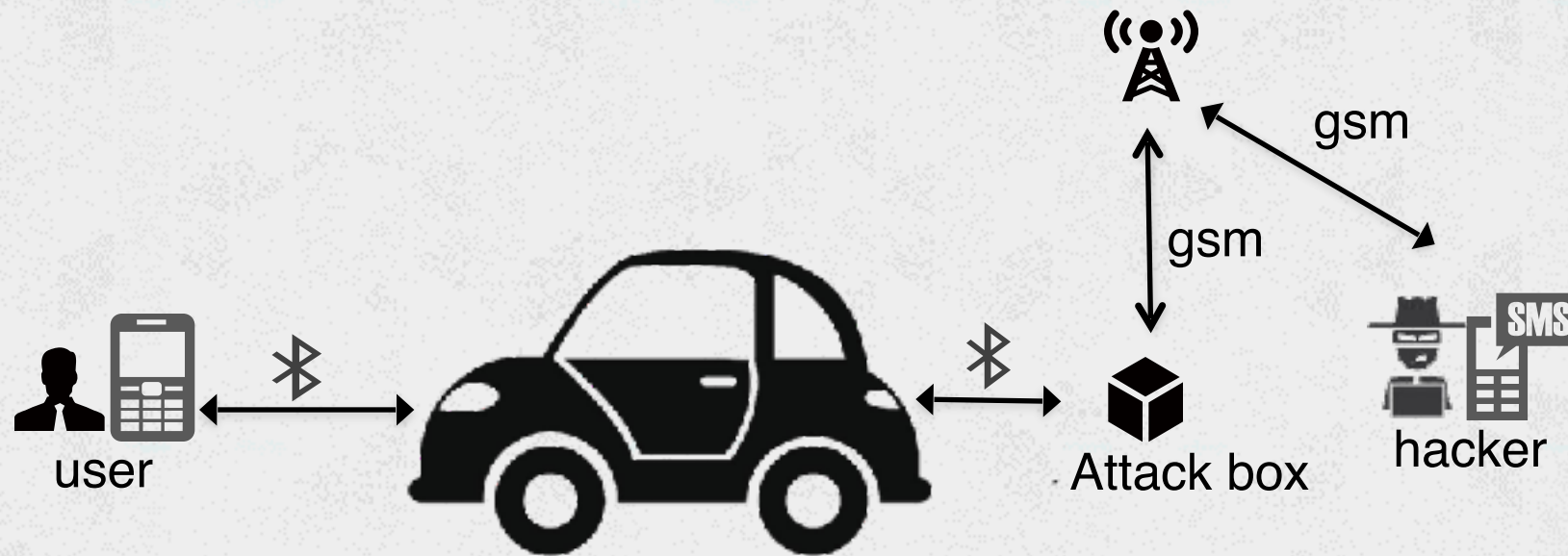
Adb调试接口

```
root@kali:~# adb connect 10.42.0.58
connected to 10.42.0.58:5555
root@kali:~# adb shell
shell@r2_cht_cr:/ $
```

· GeekPwn分享



· GeekPwn分享



Q&A

Thank You~