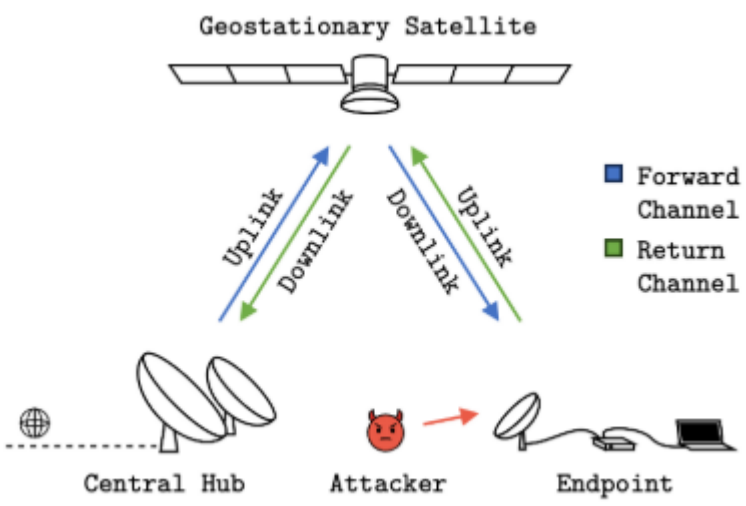
2025-03-06汇报

指南撰写

卫星地面站

卫星通信系统

- **中央集线器**——卫星与地面通信系统的中继器，配有大型蝶形天线(`天线系统`)，用于向卫星收发信号
- **卫星**——互通中央集线器与端点的数据，不执行任何数据处理/路由/身份验证，可定位在静止轨道GEO，中轨道MEO与低轨道LEO
- **端点**——与卫星通信，将接收的数据传达到接收方(下行链路)，或通过卫星传输数据至中央集线器(上行链路)



终端系统VSAT=>双向数据传输[Usenix_2024_VAST]

- **室外单元ODU**`射频前端`——高增益碟形天线(向地球同步卫星发送和接收信号)、收发器
- **室内单元IDU**——室外机与用户网络之间的接口，包括**调制解调器**`固件`(调制输出信号进行传出、解调输入信号进行接收)、**网络接口**`网络协议`(以太网、WiFi等，连接用户本地网络)

卫星地面通信系统API

卫星地面通信系统 API 主要用于地面站、卫星网络管理系统、用户终端及云端数据平台之间的信息交互，涵盖数据传输、遥测控制、用户身份验证、卫星任务调度等功能。主要包括以下几类 API：

- **控制 API**——用于地面站对卫星姿态、轨道、遥测等数据进行管理和控制，如远程指令发送
- **数据 API**——负责卫星遥测数据、气象数据、图像数据等的上传和下载，支持 HTTP、MQTT、gRPC 等通信协议
- **身份认证 API**——用于终端用户与卫星服务之间的身份验证，通常采用 OAuth、JWT 令牌等认证方式
- **远程访问 API**——允许运维人员对卫星地面站及网络基础设施进行远程操作

API运行架构与连接方式

- **数据交互流程**——卫星通过高频无线电波（如 S 频段、X 频段、Ka 频段）与地面站通信，地面站 API 负责数据解码、存储，并通过 HTTP(S) 或 WebSocket 将数据传输至应用系统
- **认证与授权**——基于 PKI（公钥基础设施）进行身份验证，通过 HMAC（哈希消息认证码）或基于 OAuth 2.0 的 JWT 令牌对 API 请求进行验证
- **远程管理**——地面站 API 允许运维人员远程访问系统，执行固件更新、日志分析、故障排除等任务

拟写指南——基于大模型的智能化卫星地面通信系统API漏洞挖掘与渗透攻击关键技术

主要研究内容

- **卫星地面通信系统智能化部署**——对系统**脆弱性**进行分析发现，包括**API端点暴露、固件安全风险及协议级漏洞**等
- **卫星地面通信系统API漏洞挖掘技术**——对**API固件、多种传输协议、身份认证逻辑**等关键环节存在的漏洞进行自动化检测与精准识别
- **基于大模型的渗透攻击关键技术**——智能化攻击路径生成、模拟现实攻击者的行为模式，提高**渗透测试**的自动化与精准性