A Comprehensive Analysis of Security Vulnerabilities and Attacks in Satellite Modems

Lingjing Yu
Institute of Information Engineering,
Chinese Academy of Sciences
Xingditansuo Co., Ltd
Beijing, China
yulingjing@spacesecure.cn

Jingli Hao
Xingditansuo Co., Ltd
Beijing, China
haojingli@spacesecure.cn

Jun Ma
Sinsegye (Shenzhen) Computer
System Co., LTD
Shenzhen, China
majun@sinsegye.com.cn

Yong Sun
Institute of Information Engineering,
Chinese Academy of Sciences
Beijing, China
sunyong@iie.ac.cn

Yijun Zhao
Institute of Information Engineering,
Chinese Academy of Sciences
Beijing, China
zhaoyijun@iie.ac.cn

Bo Luo
EECS and I2S,
The University of Kansas
Lawrence, KS, USA
bluo@ku.edu

Abstract

Satellite modems are critical components in satellite communication networks. Especially, they determine the entire communication regime in traditional systems where the satellites only act as transparent relays. However, unlike satellites that are usually more isolated and better protected, satellite modems are accessible and susceptible to lower-cost attacks, potentially serving as a weak link in the chain of satellite communication security. We make the first attempt to shed light on satellite modem security. We first physically disassemble commodity satellite modems and systematically examine hardware and software modules. We perform a measurement study on the satellite modems that are exposed to the Internet. We identify 16 security vulnerabilities across three attack surfaces: satellite communication interface, ground network interface, and hardware. We further introduce AirSecAnalyzer, an automated security analyzer/fuzzer for the modems' satellite communication interface. Through comprehensive analysis and extensive experiments on 9 real-world satellite modems, we report 18 novel attacks that exploit the identified vulnerabilities. Our findings are expected to contribute as a valuable foundation for future research on the security of satellite modems and satellite communication networks.

CCS Concepts

• **Security and privacy → Mobile and wireless security**.

Keywords

Satellite communication networks, satellite modems, security

ACM Reference Format:
Lingjing Yu, Jingli Hao, Jun Ma, Yong Sun, Yijun Zhao, and Bo Luo. 2024. A Comprehensive Analysis of Security Vulnerabilities and Attacks in Satellite Modems. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3658644.3670390

CCS '24, October 14–18, 2024, Salt Lake City, UT, USA.

ACM ISBN 979-8-4007-0636-3/24/10
https://doi.org/10.1145/3658644.3670390

1 Introduction

With thousands of communication satellites orbiting the Earth, satellite communication plays an increasingly important role in global connectivity, especially for underdeveloped and geographically isolated regions. Critical infrastructure sectors, including military, telecommunications, energy, utilities, and transportation, heavily rely on satellite communication systems. Satellite modems play a crucial role in satellite communication systems, enabling bidirectional communication between ground stations and satellites. This is particularly evident in the case of traditional communication satellites that utilize bent-pipe transponders, where the signal format of satellite communication is entirely determined by the satellite modems at the ground stations, while the satellites only serve as transparent signal repeaters.

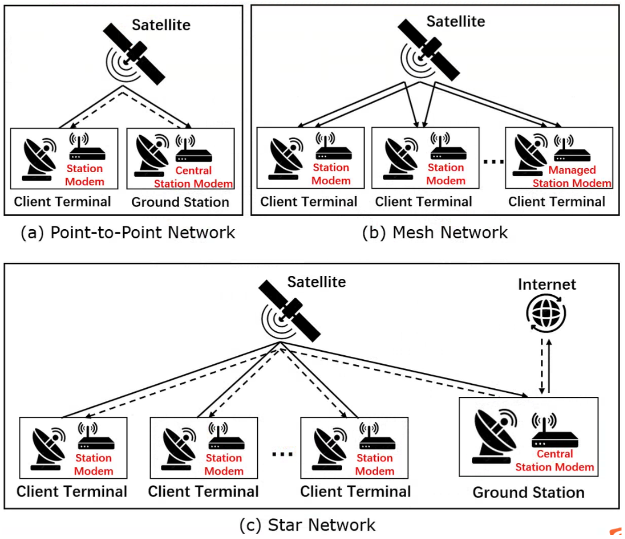
Different from traditional modems, satellite modems incorporate additional features and services to support over-the-air communication with satellites. As a result, they are not only vulnerable to traditional network attacks but also susceptible to over-the-air attacks from the satellite communication interface. This significantly expands the attack surfaces against satellite modems. Obtaining information on satellite modems is also relatively easier and less expensive compared to satellites. Moreover, the exposure of the modem's open services and other information on the Internet makes it easy for attackers to identify and access their targets.

Security issues on satellite modems encompass concerns regarding the confidentiality and integrity of data transmission and, more importantly, potential threats to the satellite communication system's overall availability. The attacker may gain access to sensitive data, such as classified government or military documents, and cause widespread outages to critical infrastructures such as energy and transportation, resulting in service disruptions or even accidents. Ultimately, such malicious attacks can severely threaten national security and public safety. For instance, a newly discovered malware wiped *SATCOM* satellite modems on February 24, 2022, affecting thousands in Ukraine and tens of thousands more across Europe [26]. In addition, a hacktivist group claimed to have successfully deleted the critical configurations on *MegaFon* modems [33], which are used in various industries that require reliable and high-speed satellite communication links, including military/defense, oil/gas, emergency services, etc.

Despite its crucial importance, there is a notable absence of research efforts dedicated to a systematic understanding of satellite modems and a comprehensive analysis of satellite modem security. To bridge this gap, we present an in-depth study of the security aspects of satellite modems. In particular, we disassemble several satellite modems from the consumer market to examine their hardware and software modules. We further conduct a comprehensive analysis to shed light on their inherent security challenges and potential vulnerabilities from three attack surfaces: the satellite communication interface, the ground network interface, and the modem hardware. Moreover, we conduct experiments with an in-house tool named AirSecAnalyzer to discover and validate attacks on a selection of representative satellite modems, aiming to provide insights into the specific threats faced by the satellite modems and their potential impacts on satellite communication networks. Finally, based on the findings of vulnerabilities and attacks, we propose security recommendations for real-world satellite modems.

The main contributions of this work are summarized as follows:
(1) We are the first to demystify the architecture, function modules, and their hardware/software implementations of commodity satellite modems, and, more importantly, the corresponding security risks within each module. We further conduct a measurement study of satellite modems that are exposed to the Internet and examine the potential security issues associated with these modems.
(2) We define three attack models corresponding to three attack surfaces in satellite modems. We are the first in the literature to conduct a comprehensive and systematic analysis of potential security vulnerabilities in satellite modems. We identify and articulate 16 vulnerabilities from different hardware/software modules.
(3) We present the first security analysis/fuzzing tool for the satellite communication interface of satellite modems. With extensive investigation and experiments, we have discovered 18 practical attacks that exploit the newly identified vulnerabilities in 9 satellite modems. This effort allows us to gain a deeper understanding of the real-world security landscape of satellite modems and to suggest potential defense strategies. All identified vulnerabilities have been responsibly disclosed to the respective vendors.

Ethical Considerations. The ultimate goal of this research is to improve the security of satellite communication systems, which has the potential to benefit a broad range of applications and users worldwide. All the experiments and attacks were performed strictly in our isolated lab environment. We did not attempt to transmit any signal to any satellite or the external Internet. The measurement study described in Section 5 only involved publicly available information. We did not perform any IP or port scanning, instead, we relied on the information provided by two search engines. We have disclosed our findings to the manufacturers of the satellite modems. For the vulnerabilities with the satellite communication interface, we made a first disclosure when we discovered the vulnerabilities, and a second disclosure when this paper was drafted. We are currently communicating with Comtech, UHP, and iDirect to discuss the vulnerabilities. We will not disclose the vulnerabilities to the public until 90 days after our last disclosure. We also hide the exact model numbers of the vulnerable devices in the paper.



(a) Point-to-Point Network

(b) Mesh Network

(c) Star Network

Figure 1: Three basic network architectures for satellite communication networks.

The rest of the paper is organized as follows: we introduce satellite communications in Section 2 and articulate modem architectures in Section 3, followed by a taxonomy of threats in Section 4. We present a measurement study of Internet-exposed satellite modems in Section 5, followed by AirSecAnalyzer and 18 novel attacks in Section 6. Finally, we discuss the defense, survey the literature, and conclude the paper in Sections 7, 8 and 9.

2 Background: Satellite Networks

Satellite Communication Networks. Communication satellites relay radio signals between modems to create a satellite communication network. Traditional satellite payloads include *regenerative transponders* and *bent pipe transponders*. The regenerative transponders are capable of demodulating and decoding signals from ground stations, followed by network reconstruction and encoding. Meanwhile, the bent pipe transponders, a.k.a. the repeaters, process signals solely at the RF level to perform actions such as frequency conversion and power amplification. They do *not* demodulate the signals or modify the signal format. Bent pipe transponders are more popular because: (1) The satellite's lifecycle can span 10 to 20 years, during which significant advancements in communication technology may occur. The use of bent-pipe transponders reduces upgrade costs, as there is no need to modify satellites. (2) The on-board processing for regenerative transponders increases power consumption. (3) Bent pipe transponders accommodate signals from different formats, providing better flexibility. Due to the prevalence of bent-pipe transponders, the signal format in satellite communication networks is determined by satellite modems, while the satellites remain uninvolved in signal processing.

Figure 1 shows the three basic satellite communication network architectures: (1) *Point-to-Point Networks.* A point-to-point network involves two stations, the client station and the central station, with

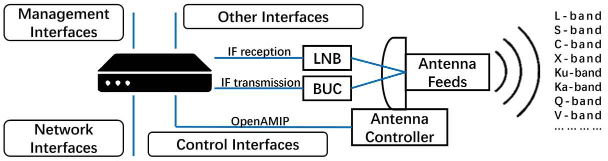


Figure 2: Interactions between the satellite modem and satellite communication antenna.

direct links between these two station modems. (2) *Mesh Network.* In mesh satellite networks, bidirectional links are established between any two stations in the network. Mesh networks may designate one or more *management stations*, which remotely manage other modems in the network. (3) *Star Networks.* In star satellite networks, stations communicate through a central station. Star networks benefit from simplified communication management. To meet specific requirements and environmental conditions, real-world networks often adopt combinations or variants of these basic structures.

Satellite Modems. The satellite modems connect to the antennas through the radio frequency (RF) interface, as shown in Figure 2. The antenna typically consists of an antenna reflector, a Block Upconverter (BUC) with a frequency upconversion power amplifier, and a Low-Noise Block downconverter (LNB). For modems with integrated antennas, functions of the BUC and LNB modules are typically integrated into dedicated chips. In data reception, the satellite signal is reflected by the antenna and directed to the LNB, which amplifies and downconverts the received signals and delivers them as intermediate frequency (IF) signals through the modem's RF input interface (RFI). In data transmission, the modem sends modulated signals through its RF output interface to the BUC. The power amplifier performs upconversion and power amplification on the signals before radiating them onto the antenna reflector. In addition, LNBs and BUCs commonly adopt the reference frequency transmitted by the modem to establish a shared reference frequency that facilitates accurate interaction in signal exchange.

- *Modem Functionalities.* Satellite modems provide essential functionalities to enable reliable and secure exchange of data in satellite communication networks: (1) modulation and demodulation, to ensure the conversion between digital data and suitable analog signals, (2) error correction, to enhance data integrity, (3) data encryption, to effectively safeguard the information from unauthorized access, and (4) manage/control carrier frequency and symbol rate, to optimize transmission parameters for efficient communication.
- *Modem Form Factors.* There exist two popular form factors of satellite modems: standalone (without antenna) and integrated (with embedded antenna and antenna control service). The standalone modems provide higher flexibility as they can pair with different antenna systems and allow convenient updates or replacements. Meanwhile, the integrated systems with reduced size and weight, e.g., the Starlink terminal, are particularly suitable for mobile and emergency communication applications.

3 Satellite Modems Demystified

3.1 Devices Disassembly and Analysis

While satellite modems are being adopted in the consumer market, limited technical details of their architecture and security features have been disclosed in the literature. To fill this gap, we purchased nine models of commodity satellite modems from four popular brands, as shown in Table 1. Note that we hide the model numbers for security considerations. They cover all three satellite network structures and all typical satellite network applications. Comtech Telecommunications Corp. and ST Engineering are considered the top 2 players in the satellite modem market [46]. Comtech's classic modems (*C1*, *C2*, *C3*) are adopted in a wide range of applications, including military, broadcasting, and maritime [29] [55]. Meanwhile, ST Engineering's iDirect *i1*, *i2*, and *i3* are widely used by satellite communication service providers in remote regions and military operations [56]. Besides the general-purpose satellite modem products, we also obtained modems for niche applications. The UHP modems (acquired by Comtech in 2021) are known for their mesh networking capabilities. Intellian *Int* is a highly-specialized integrated satellite modem system that was adopted in the International Maritime Satellite Network operated by Inmarsat [42, 43]. Given these modems' critical roles in the communication systems in various industries, our research aims to investigate the potential security vulnerabilities to ensure the safety and reliability of this critical infrastructure. Last, satellite modem security has far-reaching implications beyond commercial systems, as they are adopted in sensitive sectors like military and defense.

Table 1: Satellite modems used in this study (SA: standalone, int: integrated. mil: military, bc: broadcasting, aero: aerospace, mari: maritime, land: land mobile, ent: enterprise.). Model numbers are anonymized for security reasons.

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

We disassembled/examined the modems in the following steps.

- *Device Disassembly.* We physically disassembled the modems to expose their internal architectures. We employed visual inspection and tools to analyze the hardware modules such as the main circuit board, processors, memory, and other elements.
- *Firmware Extraction.* (1) We downloaded the firmware from the official websites for Comtech devices. (2) For iDirect modems, we extracted their firmware through the SSH management interface, (3) For Intellian *Int*, we connected to its serial interface and retrieved the firmware. (4) The first three methods were unsuccessful for UHP modems, hence, we employed chip-off extraction techniques to extract the firmware directly from physical memory chips.
- *Firmware Analysis.* Analysis of the firmware allowed us to dissect the functional modules, services, security features, and operation flow of these devices. We utilized static analysis tools (IDA Pro) to examine the binary files. Next, with firmware reverse engineering, we identified key processes and code segments within the modem system that handles satellite data. By integrating software analysis with examinations of the modems' PCB hardware, we investigated the communication mechanisms between the system and DSP modules to gain insights into the communication processes.
- *Dynamic Analysis.* We constructed network environments for the satellite modems, e.g., we configured a point-to-point network for

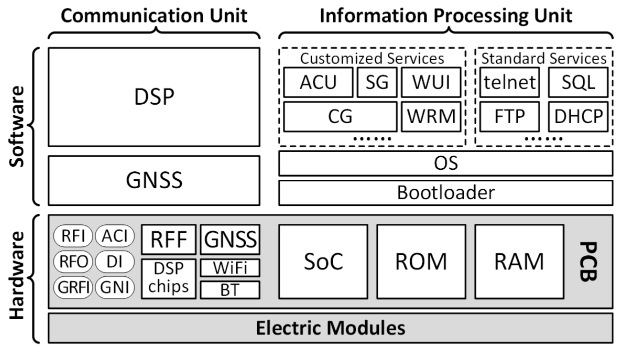


Figure 3: Function modules of a typical satellite modem.

Comtech *C2*and *C3*. We also connected the modems to our laboratory network to manage their configurations. With transmission signals close to 0dBm, we connected RF antennas in the L-band to the modems' RF interfaces. This setup enabled local short-range communication between them, bypassing the satellite transponder, i.e., no signals are transmitted to any satellite. The operational settings closely resembled real satellite communication conditions, except for signal frequency conversion and amplification by LNB and BUC. This local simulation allowed us to capture and analyze the air interface signals of the modems for L-band (1GHz to 2GHz) communication using PlutoSDR and USRP B210 software-defined radio (SDR). Signal analysis was then conducted using URH (Universal Radio Hacker) and Gnuradio software. Wireshark was employed to capture local network traffic for further analysis.

In this study, we mainly focus on the common functions inherent in contemporary satellite modems while acknowledging potential variations across different implementations. As shown in Figure 3, a typical satellite modem could be decomposed into two logical components: the communication unit and the information processing unit. We articulate the functions/services in each unit.

3.2 The Communication Unit

The communication unit captures RF signals from the antenna, handles signal modulation and demodulation, and facilitates data exchange through external interfaces such as RF input/output (RFI/RFO), antenna control interface (ACI), ground network interface (GNI) and debug interface (DI).

RF Frontend (RFF). The RFF module handles physical layer signal processing. It is typically implemented completely in hardware. RFF captures incoming RF signals through RFI, amplifies the signals, and performs frequency conversion to transform received signals into IF signals for DSP. In transmission, RFF encodes signals from DSP to a carrier signal and amplifies the modulated signal for RF output to the antenna BUC. As the gateway between the satellites and modems, attacks on RFF can interrupt the modems' signal processing capabilities in both reception and transmission.

Digital Signal Processing (DSP). The DSP module handles satellite signal processing and the conversion between digital and analog signals. It is typically hardware-based, which utilizes FPGA, DSP (Digital Signal Processor), ASIC (Application-Specific Integrated Circuit), or a combination of these technologies. Its functions include modulation/demodulation, encoding/decoding, error correction, clock synchronization, etc. Attacks on the DSP module could compromise signal integrity and degrade fundamental communication capabilities and overall performance of satellite modems.

Global Navigation Satellite System (GNSS). Some high-end integrated satellite modems, such as the Starlink terminals, contain the GNSS modules, which receive position and time information from systems like GPS, BEIDOU, and Galileo. It sends this information to antenna control (AC) to adjust antenna angles. It also supplies time and pulse-per-second (PPS) signals to both DSP and the core guard (CG) service, serving as references for time and frequency in the modem. An interfered GNSS may cause errors in antenna angle, network scheduling, and time and frequency references.

3.3 The Information Processing Unit

The information processing unit utilizes an embedded operating system, e.g., VxWorks on ARM, to handle data operations and device management. It contains the OS, Bootloader, standard services, e.g., HTTP and FTP, and customized services specifically designed for satellite modems, e.g., core guard, security guard.

Bootloader (BL). The BL verifies and loads the OS. Attacks on BL lead to service disruptions, loss of control, or further exploitations.

OS and Standard Services. The OS provides support for all upper-layer functions and services. It also integrates standard services like Telnet and SNMP. These services facilitate the modem's basic network functions, such as network protocols and remote access. Compromised OS and standard services would pose risks of data tampering, service disruptions, unauthorized access/control of modems, and potentially further exploitations.

Web User Interface (WUI). WUI provides a user-friendly, graphical interface for administrators to monitor and manage modems' features/functions, such as communication parameters, network settings, and security features. The service also provides real-time monitoring, diagnostic tools, and logs for troubleshooting. In some modems, firmware updates can be performed through WUI. Compromised WUI poses threats such as unauthorized access to critical settings and disruptions in the satellite communication system.

Core Guard (CG) Service. The CG serves as the central processor for both incoming and outgoing data. It may collaborate with services like SG for decryption and validation. Details of the data processing flow and the CG operations will be articulated in Section 3.4. Compromised CG may lead to issues such as unauthorized access, data tampering, or disruption of critical functions.

Wireless Remote Management (WRM) Service. WRM facilitates the remote management of the modems through the satellite communication interface: (1) network authentication: to authenticate the satellite modem within the communication network. (2) Fault detection and reporting: to monitor the modem for faults or anomalies, take corrective actions or alert other components, and generate reports accordingly. (3) Configuration management: to allow administrators to remotely change the settings of satellite modem(s), e.g., in a star network, the central station can broadcast configuration commands to all station modems to streamline the process, ensure uniform configurations across the network, and enhance efficiency in network management. Compromises in WRM may pose risks to the modem's functionality and data integrity, e.g., unauthorized access, tampering with critical configurations, and disruptions in satellite network communications.

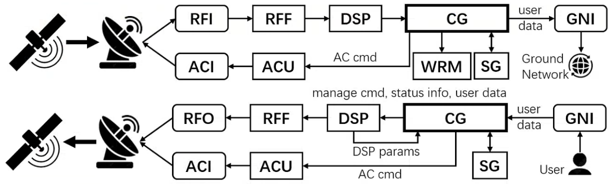


Figure 4: Data reception (top) and transmission (bottom) processes of satellite modems.

Antenna Control Unit (ACU). ACU communicates with the antenna unit with integrated protocols like openAMIP [41] to enable dynamic adjustments in azimuth, elevation, and polarization angles for optimal signal reception and transmission. Attacks on ACU may compromise antenna control and disrupt signal transmission.

Security Guard (SG). Modern satellite modems usually implement a security guard for communication security. SG provides essential security functions such as encryption/decryption, certificate management, and security policy enforcement. SG vulnerabilities can lead to a wide range of breaches, such as unauthorized access and failed encryption. Moreover, human errors of the administrators, such as neglecting or misconfiguring the SG service, introduce additional security vulnerabilities. Note that SG is considered a logic module, which may be physically implemented as embedded components in other modules/services such as CG or WRM.

3.4 Data Process Flow in Satellite Modems

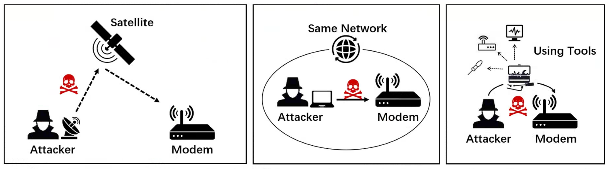
The Data Reception Process. As illustrated in Figure 4 (top), RFI receives the air signal from the antenna and processes it through the RFF and DSP modules. Air signal is eventually converted into baseband data and sent to CG, which may invoke SG for decryption and security policy validation. CG then parses and reconstructs the received data. It extracts sender and receiver information and distinguishes between management and user data segments: (1) For management data, specialized modules like WRM are invoked to process remote management commands. For instance, CG invokes ACU to handle antenna control commands, which specify control parameters for precise adjustments. ACU sends the instructions, via ACI, to the antenna for adjustments. (2) For user data, CG encapsulates it using the standard TCP/IP protocol. The encapsulated packets are then transmitted through the ground network interface (GNI) to the ground network for further distribution.

The Data Transmission Process. In the data transmission process (Figure 4 (bottom)), CG monitors network status, and retrieves parameters from modules like the DSP. When user data is received from GNI, CG may invoke SG for encryption and security policy validation. The data is encapsulated by CG, modulated, and amplified by DSP and RFF. The RF signals are eventually transmitted to the antenna via RFO. In modems with ACU, CG also invokes the ACU for antenna control during data transmission.

4 Attack Models and Vulnerabilities

4.1 The Attack Models

In this work, we assume external adversaries, who do not have any legitimate authentication or authorized access to the satellite communication system in which the target satellite modem is deployed. We consider both remote and physical attackers. They have three access mechanisms to the modems: (1) through the satellite communicating interface, (2) through the ground network interface, and (3) through hardware contact. These access mechanisms form the basis for the three attack models against satellite modems.



(a) Satellite Communication Attack (b) Ground Network Attack (c) Hardware Attack

Figure 5: Three attack models against satellite modems.

Attack Model 1: Satellite Communication Attack. As shown in Figure 5 (a), the attacker interacts with the satellite communication interface (SCI) of the modems. The attacker has basic knowledge about the communication mechanisms and protocols of the target satellite communication network. She operates within the coverage area of satellite signals. As introduced in Section 2, the widespread use of bent-pipe transparent transponders in satellite communications extends the attack range, as the attack signal could reach the target modem from other regions or even continents through a high-altitude satellite, while the target modem does not need to be connected to any ground network. The broad coverage of the satellite transponder payload allows the attacker to gather information from the satellite's downlink signal and precisely calculate the radio frequency to send attack signals to the satellites and modems. The attacker uses satellite communication equipment such as antennas to send attack signals. For certain attacks, e.g., signal localization, supplementary radio location equipment is necessary.

Attack Model 2: Ground Network Attack. Similar to conventional network attacks, the attacker attempts to access the target modem through its ground network (Figure 5 (b)). The attacker needs to have access to the same ground network as the target modem, regardless of a private network or the Internet. The attacker knows the target's IP, and potentially the type of the systems and services. She may acquire commodity modem software/hardware to explore exploitable vulnerabilities. To attack the non-publicly-exposed services, e.g., CG, the attacker needs to first penetrate the target modem through other vulnerable channels.

Attack Model 3: Hardware Attack The attacker has physical access to the modem (Figure 5 (c)), which is possible since satellite modems are often used in remote locations with low levels of physical security. Especially, modems with integrated antennas (Starlink) must be placed in open areas with direct lines of sight to the satellites. Hardware attacks may require specialized equipment. For example, signal generators are needed to forge reference signals, while signal analysis or RF measurement devices are required for attacks involving channel measurement and analysis.

4.2 Taxonomy of Satellite Modem Attacks

Attack Objectives and Impacts. In Table 2, we enumerate the attackers' objectives along with their impacts on the CIA (confidentiality, integrity, and availability) triad. The objectives are organized into four categories: (1) attacks that interfere with the *operation of the satellite network*, e.g., network degradation, DoS, compromised authentication; (2) attacks that interfere with the *operation of the*

Table 2: Taxonomy of attacks against satellite modems: attack objectives, surfaces, and impacts. Attack surface: S: satellite communication; G: ground network; H: hardware access. ✓: confirmed attacks.

ID	Attack Objective		Attack description	Surface			Impact on Security triad		
				S	G	H	Confidentiality	Integrity	Availability
O1	Satellite Network	network degradation	reducing the quality of network communication and data transmission	✓				corrupted or incomplete data transmission	may cause network congestion or disruption
O2		network DoS	deliberately interrupting network communication to cause a denial of service	✓				corrupted or incomplete data transmission	communication service becomes unavailable
O3		network authentication	accept unauthorized terminals or deny legitimate terminals to the network	✓			may expose confidential information in the network	unauthorized access compromises network integrity	denying legitimate terminals, may cause network disruption
O4	Satellite Modems	modem configuration	unauthorized access to and modification of modem configurations	✓	✓		exposure of sensitive modem and network configuration details	compromised the integrity of modem and network configuration	disruption of modem and network functioning
O5		modem authentication and access	communicate without authentication or denying legitimate communication	✓				compromised the integrity of the authentication process	prevents legitimate terminals from accessing the network
O6		modem communication degradation	reduce modem performance, decrease data transmission speed and quality	✓				corrupted or incomplete data transmission	disrupted connection from terminal, disrupted data transmission
O7		modem DoS	interrupting modem operations to cause DoS	✓	✓	✓		corrupted or incomplete data transmission	modem becomes unavailable or inaccessible to users
O8		modem privilege escalation	gaining unauthorized access and control over modem functionalities		✓	✓	exposure of information stored in the modem	compromises modem operations, inject backdoors, etc.	enables unauthorized control, impacting normal functioning
O9	Comm. Data	communication data leak	unauthorized disclosure of data-in-transit	✓			directly violates data confidentiality		
O10		user message tampering	illicit modification of user communication content	✓				undermines the integrity of communication	
O11	Meta-data	ground station location	disclosure of the geographical location of ground stations	✓			reveals sensitive location information		may expose ground stations to physical attacks or interference
O12		modem system information	disclosure of information about the modem system		✓	✓	discloses sensitive details about the modem system		

modems, e.g., compromised modem configuration or access, modem DoS; (3) attacks that explicitly focus on the data in satellite communications, e.g., unauthorized data access/tampering; and (4) attacks that attempt to learn meta-data of the satellite modems. The attack objectives are often related. For instance, any attack that compromises modem configuration (O4) could modify communication parameters to interrupt communication (O6 and O7). Likewise, a successful privilege escalation (O8) could allow the adversary to accomplish further objectives, such as O4, O6, O7.

In a typical real-world setting, a satellite modem connects a local system (a workstation or a local network) to the satellite network. An attacked or compromised modem may impact both the satellite network and the local system: (1) As shown in Table 2, attacks against the modem could impact the operations of the entire satellite communication infrastructure (O1 to O3). For example, compromised modem authentication (e.g., Attack 5 in Table 5) could allow (a significant number of) unauthorized terminals to access the network or deny the connection of legitimate terminals, posing confidentiality, integrity, and availability risks to the entire network. (2) When a modem is compromised, the confidentiality, integrity, and availability of the communication between the local system and the satellite network are all at risk (O4 to O10), which may cause severe consequences. For example, in the oil and gas industry, disrupted satellite modems could halt communication between offshore platforms and onshore control centers, leading to operational delays and safety concerns. (3) Even the metadata may carry sensitive information, which could be utilized to engineer further, more focused attacks. For example, if attackers gain metadata from unprotected satellite modems in a maritime communication system, e.g., modems on cargo ships, they could target specific ships to disrupt the supply chain and cause significant financial/safty consequences. (4) Finally, a compromised modem could be employed as a stepping stone to attack the local system or the satellites. This threat introduces a new attack surface to the local/ground systems and could bring severe consequences. We consider such attacks outside of the scope of this work as we focus on the modems. We also exclude satellites in this work since they are highly sensitive and it is impractical to test any attack on real-world satellites.

Attack Surfaces. The contact mechanisms described in the three attack models naturally constitute three attack surfaces: the satellite communicating interface (SCI), the ground network interface (GNI), and the hardware (HW).

- *Surface 1: Satellite Communicating Interface (SCI).* The SCI attacks exploit vulnerabilities within specific modules and services associated with satellite communication (RFF, DSP, CG, WRM, SG, GNSS, AC) and vulnerabilities with communication signals.
- *Surface 2: Ground Network Interface (GNI).* Traditional network attacks can compromise satellite modems through GNI, targeting the system and its associated services, including standard services (SQL, HTTP) and satellite-specific services (AC, CG, SG).
- *Surface 3: Hardware Access.* Most satellite modems were designed and manufactured without physical security concerns, resulting in unprotected hardware modules and access mechanisms.

In Table 2, we identify how each attack objective could be accomplished through attacks from one or more of the attack surfaces discussed above. Each ✓ denotes a confirmed attack path from the attack surface to the attack objective. Note that, not all such hypothetical attacks have been implemented or discovered in the real world. Indeed, before this work, only a small number of attacks were reported in the literature (discussed below), while novel attacks identified in this work are reported in Section 6.

Known Attacks. Last, we summarize the attacks against satellite modems that have been reported in the literature. In particular, we employ the newly proposed attack taxonomy to examine the attack paths, i.e., from attack surfaces to attack targets and objectives, of all the previously disclosed attacks. As shown in Table 3, while 17 attacks have been reported, the vast majority of them belong to two clusters: attacks from the ground network interface (GNI) to the OS and standard services, and attacks from GNI to the web UI. Vulnerabilities in the first cluster were found in telnet [13, 15], FTP [9], TCP [5, 7], and authentication (OS) [8, 10]. Meanwhile, web UI service vulnerabilities are mostly conventional flaws such as cross-site scripting [16], code/command injection [14, 17, 18], and information/credential leak [4, 6]. Such attacks mainly achieve objectives O4 (modify modem configuration), O7 (modem DoS), O8 (privilege escalation), and O12 (retrieve modem system information). Meanwhile, the GMR-2 cipher used in (old) Inmarsat satellite phones is found to be vulnerable [35, 45]. Finally, two hardware vulnerabilities have been identified that allow adversaries to obtain privileged access (O8) through direct hardware interaction.

Table 3: Known satellite modem attacks in the literature.

Attack Surface	Objectives	Attacks
SCI: Encryption (GMR-2)	O9	[35, 45]
GNI: OS and standard service	O4 O7 O8 O12	[5, 7–10, 13, 15]
GNI: Web UI	O4 O7 O12	[4, 6, 14, 16–18]
HW: Serial Port	O8	[11]
HW: PCB	O8	[62]

4.3 Vulnerabilities

Vulnerabilities associated with Satellite Communicating Interface (SCI). The following vulnerabilities are found in satellite communication modules (vulnerabilities 1-6 in Table 4) or satellite communication signals (vulnerabilities 7-8 in Table 4).

- *Vulnerable time and location synchronization*: Precise time synchronization may be disrupted by injected delays or jammed signals on the synchronization service. Such disruptions compromise the accuracy of timekeeping, which is crucial for the effective operation of the DSP and GNSS modules. Meanwhile, GNSS is known to be vulnerable due to the use of unencrypted channels. Interference with GNSS signals results in inaccurate antenna controls (see Section 6.2) and ineffective satellite communication.
- *Vulnerable/weak identity authentication*: Vulnerabilities in satellite identity validation could allow forged identities and enable malicious actors to join the satellite network. Moreover, a large number of unauthorized users in the network may result in network degradation or interruption. Specifically, we have identified vulnerabilities in modems such as iDirect *i1*, *i2*, etc., which could allow an attacking modem to impersonate another authorized modem in the satellite network (refer to Section 6.2 for details).
- *Vulnerable modem authentication*: For modems that already joined the satellite network, vulnerable modem/peer authentication may be exploited to impersonate the identity of other legitimate modems to tamper with normal network communications. For instance, by exploiting vulnerabilities in the EDMAC remote management function of Comtech *C2*and Comtech *C3*, we successfully impersonated an attack modem as a central station into an established network. The central station can then send arbitrary commands to other station modems and intercept all user data (Section 6.2).
- *Unencrypted traffic*: When the satellite communication is unencrypted the traffic could be intercepted or eavesdropped to leak sensitive information. Moreover, the traffic may also be illicitly modified and trigger other vulnerabilities. In particular, we have examined nine commodity satellite modems and found that all of them employed unencrypted traffic by default (Section 6.2).
- *Vulnerable encryption algorithm*: Vulnerabilities in encryption algorithms may be exploited to gain unauthorized access to sensitive data in satellite communication traffic or to inject malicious commands, jeopardizing the overall security of the satellite network. For instance, multiple security vulnerabilities were identified in the GMR-2 standard used for satellite phone encryption, allowing real-time decryption of conversation content [45].
- *Lack of command validation*: This vulnerability could be exploited to inject unauthorized commands to cause unexpected device behaviors such as misconfiguration and system/communication failure. We discovered a lack of authentication for modem identity and signal timing in Comtecch *C2*/*C3* modems. This allows attackers to perform arbitrary command injection, including modifying parameters that affect the normal communication functionality of modems, such as transmission frequency (Section 6.2).
- *Air signal jamming*: The adversary could transmit interference signals on the same frequency as the target satellite modem. Jamming can disrupt or degrade the quality of the communication signals,

Table 4: Security vulnerabilities in satellite modems.

Surf.	ID	Security Vulnerabiltities	Modules/Services
SCI	1**	Vulnerable time & sync.	DSP, GNSS
	2**	Vulnerable/weak ID auth.	SG, CG, WRM
	3**	Vulnerable modem auth.	SG, CG
	4*	Unencrypted traffic	SG
	5†	Vulnerable encryption algo.	SG
	6**	Lack of command validation	SG, CG, WRM
	7*	Air signal jamming	wireless signal, DSP
	8†	Signal localization	wireless signal
GNI	9*	Vulnerable kernel and standard service	OS, SQL, HTTP, FTP, etc.
	10**	Unprotected modem control	AC, SG, WRM, etc.
	11 †	Vulnerable GWN	Wi-Fi, BT
HW	12**	Vulnerable bootloader	BL
	13**	Insecure chips	FPGA, DSP, ASIC, SoC, ROM, RAM
	14**	System access through serial interface	console interface, debug interface
	15†	Security mechanisms bypass	PCB
	16**	Reference signal spoofing	RFI, RFO, RFF

* A vulnerability category that has been reported in the literature with new vulnerabilities or attacks identified in this study.

** A vulnerability category that is first reported in this study.

† Vulnerabilities reported in the literature.

leading to network performance degradation or interruption (please see Section 6.2 for a detailed attack).

- *Signal localization*: Due to the high transmission power in satellite communication, attackers can capture and analyze sidelobes emitted from ground stations using devices such as antennas and spectrum analyzers. Moreover, they can employ techniques such as direction finding (TDOA) to locate the position of ground stations [63] and devise subsequent attack strategies.

Vulerabilities associated with Ground Network Interface (GNI). Satellite modems may be vulnerable to traditional network attacks from GNI (9 to 11 in Table 4).

- *Vulnerable OS kernel and standard services*: Satellite modems typically employ commercial or open-source operating systems, which may have known vulnerabilities. Standard OS and network services, such as Telnet and HTTP, are common targets for adversaries. Such vulnerabilities may be exploited for sensitive data access, modem parameter tampering, or privilege escalation. We have identified multiple vulnerabilities in the standard services of the satellite modems listed in Table 1 (see Section 6.3). Last, almost all the known satellite modem vulnerabilities reported in CVEs have been found within these standard services, e.g., Telnet vulnerabilities [13, 15], FTP-related vulnerabilities [9] and Web UI vulnerabilities [4, 6, 14, 16–18]. Additionally, [5, 7, 8, 10] demonstrate the possibility of unauthorized access and arbitrary code execution.
- *Unprotected modem control*: Modem control without adequate protection may be exploited to gain unauthorized access, manipulate crucial settings, modify configurations, inject unauthorized commands, or implant vulnerabilities during firmware updates. This could lead to misconfigurations that affect the normal functionality of the system and services. In Section 6.3, we will demonstrate an exploitation of this vulnerability through command injection attacks on the AC service of Intellian *Int*.
- *Vulnerable ground wireless network (GWN)*: Some modems have Wi-Fi and Bluetooth interfaces, which introduce additional risks. Such modules are susceptible to known vulnerabilities, such as [19–21]. They may be exploited to gain access to sensitive information and potentially take control of the connected modules.

Vulnerabilities associated with Hardware. Finally, the satellite modems are also vulnerable to physical attacks against/through the hardware, i.e., vulnerabilities 12–16 in Table 4.

- *Vulnerable bootloader*: A vulnerable bootloader may be exploited to interrupt with or even take control of the boot sequence and the startup behavior of the modem, which will further enable the theft of system information or a complete takeover of the modem. See Section 6.4 for an attack that exploits this vulnerability.
- *Unprotected chips*: Unprotected chips could be exploited to extract firmware or other sensitive data. For instance, we extracted the firmware from the unprotected ROM chip of the satellite modem UHP *U1* (see details in Section 6.4).
- *Unprotected serial interface*: The serial interface, if left unprotected or improperly secured, can be exploited to gain unauthorized access to the modem's system. In [11], unauthorized privileges were gained by sending hardcoded passwords through the serial port of Cobham Aviator 700D/700E. In Section 6.4, we accessed and extracted system implementation information from Intellian *Int* by connecting to its console interface. This access allowed us to extract the modem's system firmware and obtain system privileges.
- *Bypassing security mechanisms*: By monitoring physical signals, analyzing power consumption patterns, and utilizing electromagnetic radiation or voltage injection, attackers can circumvent security mechanisms to gain access to sensitive modem system information, such as encryption keys, and even acquire system privileges. For example, Lennert successfully obtained root access to Starlink terminals through channel probing attacks [62].
- *Reference signal spoofing*: Satellite antennas are typically installed outdoors, e.g., on rooftops or hilltops at a distance from the modem. The reference frequencies of the LNB and BUC modules are often adopted from the coaxial RF cable connected to the modem (as introduced in Section 3). An illegal reference signal may be injected into the coaxial cable using a frequency source, which will result in a deviation in the reference clocks of the LNB and BUC modules. This deviation in turn leads to frequency shifts in the signals, causing communication failures. We validated this attack and provided a detailed explanation of the process in Section 6.4.

5 Internet-Exposed Satellite Modems

5.1 Satellite Modem Discovery

We first compile a list of satellite modem manufacturers and models through three sources: (1) official websites and e-commerce platforms; (2) industrial databases from sources like International Telecommunication Union (ITU) and Satellite Industry Association (SIA); (3) engagement with manufacturers at satellite communications conferences and expos. Next, we assemble queries by concatenating the manufacturers, models, and term "satellite modem", and invoke search engines Shodan (https://www.shodan.io/) and Censys (https://censys.com/) to retrieve modems exposed to the

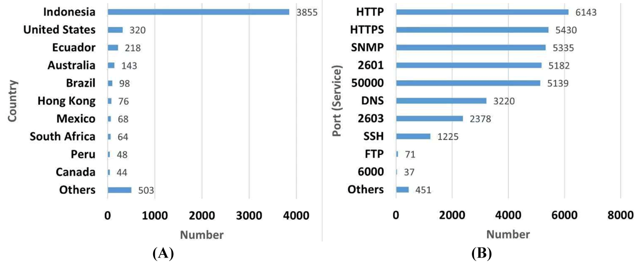


Figure 6: (A) Geographic distribution of Internet-exposed satellite modems (Others: 146 additional countries); (B) Open ports of satellite modems (Others: 15,921 additional ports).

Internet. From the results, we extract information such as open ports, services, and location (latitude, longitude, country, and city).

We initially collected 40,165 devices identified by unique IPs. We confirmed the satellite modems with two methods: (1) SNMP filtering: For IPs with open SNMP services, we retrieved SNMP data including “objectid”, “enterprise”, and “description”. The “objectid” field for satellite modems typically starts with “1.3.6.1.4.1.x”, where the mapping of x to the vendor was extracted from http://oid-info.com. The “enterprise” field may also contain the manufacturer, while the “description” field may provide model information, such as “CDM L-Band Satellite Modem.” We eliminate an IP if none of these attributes indicates a satellite modem. (2) HTTP/HTTPS filtering: For IPs with open HTTP/HTTPS ports, we crawled HTML files for keyword filtering. We identified a diverse set of confirmed satellite modems (manually confirmed by all authors). We extracted keywords/patterns from these pages (manufacturers, models, login/control interfaces) and used them to filter the remaining IPs.

We eventually confirmed 5,451 IPs of satellite modems with high precision but possibly lower recall, which is acceptable in this study. We further queried the WHOIS database to extract the “organization” and “person” fields. Named entity recognition is employed to parse the “person” field as it may contain both the names of the individual and the organization.

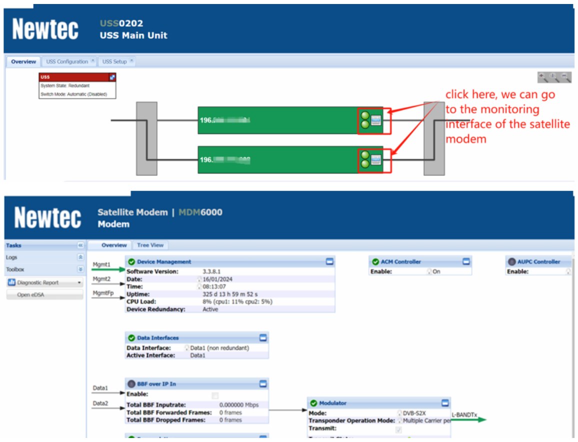
5.2 Analysis of Exposed Satellite Modems

We further examine the satellite modems exposed to the Internet to provide statistics and identify security risks.

• **Geographical distribution.** The geographical distribution of Internet-exposed satellite modems is shown in Figure 6 (A). Indonesia, the United States, and Ecuador are the top three countries with exposed modems. The high number in Indonesia may be explained by its large amount of islands and large fishermen population, who rely on satellite communication but lack awareness of security.

• **User Types.** Through whois queries, we obtained information about the IP owners of 4,808 satellite modems. Among them, only 7 IPs belonged to organizations/companies, while the rest were all individuals. This indicates that organizational owners of satellite modems may be more cautious in security, whereas individual users appear to be less attentive to the security of their modems.

• **Open ports and services.** Censys provides the open ports and services on each device. The distribution of the open ports is shown in Figure 6 (B). A significant number of the modems have open HTTP/HTTPS ports. Note that a device may support HTTP or HTTPS on multiple open ports besides 80 and 443. The exposed web services disclose information about the satellite modems and provide attackers with an evident attack surface. In manual exploration, we discovered that many of them are web-based remote management interfaces. We did not try to log in with the factory default user name and password, however, we could anticipate the default credentials being used in a significant portion of them. Moreover, we even found modems allowing access to the configuration pages without authentication, as shown in Figure 7. In particular, the highlighted buttons on the top page led to the monitor/control interface of the satellite modem (the bottom page).



System State: Redundant
Switch Mode: Automatic (Disabled)

196.[redacted]
196.[redacted]

click here, we can go to the monitoring interface of the satellite modem

Device Management
Software Version: 3.3.8.1
Date: 16/01/2024
Time: 08:13:07
Uptime: 325 d 13 h 59 m 52 s
CPU Load: 8% (cpu1: 11% cpu2: 5%)
Device Redundancy: Active

ACM Controller
Enable: On

AUPC Controller
Enable:

Data Interfaces
Data Interface: Data1 (non redundant)
Active Interface: Data1

BBF over IP In
Enable:
Total BBF Inputrate: 0.000000 Mbps
Total BBF Forwarded Frames: 0 frames
Total BBF Dropped Frames: 0 frames

Modulator
Mode: DVB-S2X
Transponder Operation Mode: Multiple Carrier per
Transmit:

Figure 7: An example of a satellite modem’s monitoring interface exposed on the Internet.

As we will demonstrate in the rest of the paper, all the Internet-exposed satellite modems and open ports (through the ground network interface) may become fruitful targets of cyber attacks against the modems and the satellite communication systems.

5.3 Auxiliary Information for the Attacker

Finally, satellite modem consumer information could be collected from the Internet and utilized in the attacks. We browsed the official websites of modem manufacturers and queried Google with keywords such as modem manufacturers, models, “contracts”, “users”, etc. As a result, we found information on satellite modems adopted by large organizations, including the ones from the military and defense industry. For example, TendersOnTime is a repository of global satellite modem tenders, contract awards, and public procurement information. News reports also disclose information about the adoption of satellite modems by military and government agencies [28, 47]. Moreover, satellite manufacturers also disclose sensitive user information on their websites [44]. The exposure of such information undoubtedly facilitates more precise and targeted attacks, including cyber, physical, and social engineering attacks.

6 Attacks against Satellite Modems

6.1 Security Analysis and Summary of Attacks

To our best knowledge, there does not exist any dedicated security analysis/testing tool for satellite modems, especially for the satellite communicating interface. In response, we developed the first efficient tool, AirSecAnalyzer, for SCI security analysis using

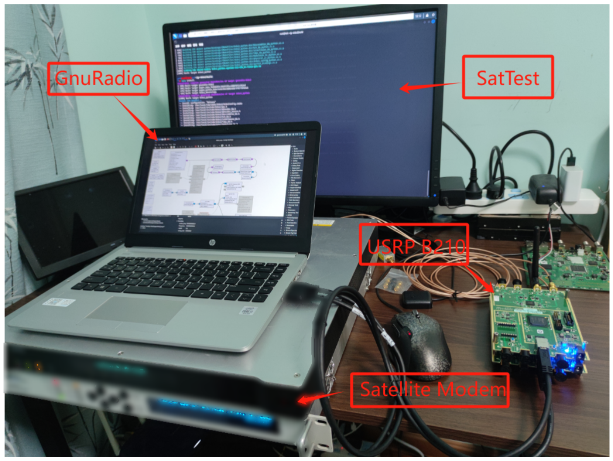


Figure 8: The hardware architecture of AirSecAnalyzer.

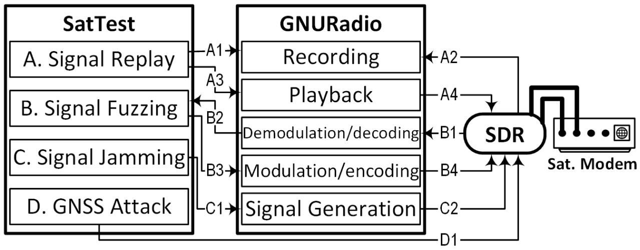


Figure 9: The functional modules of AirSecAnalyzer.

software-defined radio (SDR). In conjunction with firmware analysis and targeted attack testing on the Ground Network Interface (GNI) and Hardware (HW), we identified and validated the security issues present in the satellite modems in Table 1.

AirSecAnalyzer: Security Analysis and Testing for Satellite Communication Interface. The AirSecAnalyzer harware is shown in Figure 8. It consists of the following components: (1) the software controller and data generation module: *SatTest*; (2) the signal processing module: *GNURadio*; and (3) the SDR hardware: *USRP B210* and *PlutoSDR.* The logic structure of AirSecAnalyzer is shown in Figure 9. Here we describe the design of each module.

• **SDR Hardware.** We adopted USRP B210 (frequency of up to 6GHz and bandwidth of 56MHz) for broadband satellite signals and PlutoSDR for narrowband signals. This component handles analog-to-digital and digital-to-analog conversion processes to facilitate signal reception and transmission. It directly communicates with the satellite modem, which is being tested.

• **GNURadio Middleware.** The main signal processing module, GNURadio (https://www.gnuradio.org/) version 3.10.10.0, provides basic signal processing and communication functions, and serves as an interface between the software data generation tool (SatTest) and the SDR hardware. First, GNURadio interfaces with SDR to demodulate and decode communication signals received from the SDR before transmitting them to the software controller. Meanwhile, it receives testing data from the data generator through TCP, performs modulation on the data stream, and transmits the processed signal through the SDR interface. For generic satellite communication signals/protocols like DVB-S2 and CCSDS, GNURadio handles decoding and coding. For non-generic signals/protocols, GNURadio performs modulation and demodulation for common signals such as BPSK, QPSK, and 8-PSK. Additionally, GNURadio is also responsible for recording and replaying signals. It is also capable of generating interference/jamming signals based on the parameters set by the software controller.

• **The Software Controller and Data Generator (SatTest).** An upstream software, SatTest, is developed to implement the test cases. It mainly provides three sets of basic functions: (1) to control the functions of GNURadio, (2) to process data received from GNURadio, and (3) to generate data and send it to GNURadio. The advanced security tests are further built on top of these functions. SatTest also provides a user interface for selecting security tests and examining the results. Here we describe four typical tests that are currently implemented in SatTest.

(A) *Signal Replay*: This test is built based on two basic functions: signal recording and signal transmission. As shown in Figure 9, SatTest first invokes GNURadio (A1) to capture and store signals received from the satellite modem (A2). In a simple replay attack, such signals are not demodulated or decoded. (A3) SatTest then invokes GNURadio's playback function, which (A4) transmits the stored signals to the modem through SDR. In an advanced attack, the signal is demodulated, decoded, and saved locally. The data file could be modified before it is sent back to the satellite modem.

(B) *Signal Fuzzing*: (B1) SatTest invokes GNURadio to capture communication data through SDR and demodulate and decode such data. (B2) The data is further transmitted to SatTest, which generates fuzzing signals. SatTest utilizes two fuzzing strategies: random fuzzing and heuristic fuzzing. For random fuzzing, SatTest randomly modifies received data. For heuristic fuzzing, it identifies patterns in the data (e.g., repeated values) and modifies them accordingly (e.g., changing them to values that deviate from the established pattern, such as XORing). It also dissects the packets and modifies the header attributes based on pre-defined heuristics, e.g., enumerating all possible values, or testing the extreme or illegal values. (B3) The modified data is sent to GNURadio for encoding and modulation, and (B4) subsequently sent to the modem through SDR.

(C) *Signal Jamming*: (C1) SatTest employs GNURadio to set parameters for the jamming signals (such as frequency, power, bandwidth, etc.). (C2) GNURadio's signal generation module then follows these parameters to generate the jamming signals that are transmitted through SDR.

(D) *GNSS Attack*: (D1) SatTest employs GPS-SDR-SIM [48] to generate false GNSS location and time information, and directly transmits the false information through SDR.

Last, the modular design of AirSecAnalyzer provides flexibility and extensibility, i.e., we could conveniently utilize SatTest's basic data processing functions to develop new tests/attacks and invoke the corresponding modules in GNURadio to send them to the SDR/modem. While we continuously add new functions to SatTest and share them with the community, we also support and welcome external contributors. AirSecAnalyzer is available at: https://anonymous.4open.science/r/AirSecAnalyzer-5C77/README.md

Firmware Analysis. As introduced in Section 3.1, we have downloaded/extracted the firmware of all the satellite modems we purchased. We first scrutinized the codebase to identify areas where user inputs or external interactions could potentially influence

Table 5: Attacks against satellite modems discovered in this study. Vul. ID: vulnerability in Table 4; Outcome: attack objective in Table 2.

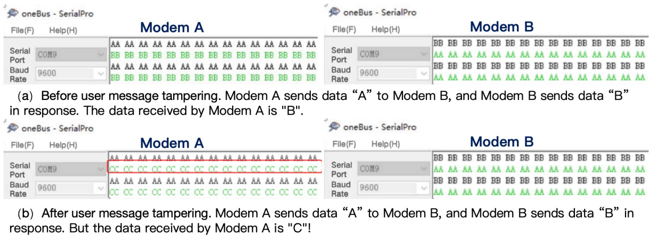
ID	Attack/Threats	Vul. IDs	Outcome	Modems
1	Comm. data theft	4	O9	all
2	User message tampering/spoofing	2+4	O10	*C2 C3*
3	Command tampering	2+4+6	O4	*C2 C3*
4	Unauthorized tampering of network structure	2+3+4+6	O5	*C2 C3*
5	Identity spoofing	2+4	O1 O2 O3 O9	*i1 i2 i3*
6	GNSS attack	1	O6 O7	*Int*
7	Random crash at fuzzing	unknown	O7	*C2 C3*
8	Air signal jamming	7	O1 O2 O6 O7	all
9	AC command injection	10	O4 O7 O12	*Int*
10	XSS	9	O4 O7 O12	*C1 Int*
11	Web command injection	9	O4 O12	*Int*
12	Unauthorized web operation	9	O4 O7 O12	*C1 Int*
13	SQL injection	9	O4 O12	*Int*
14	Arbitrary write	9	O7	*C1*
15	System information theft	12+14, 13	O12	*Int*
16	Device control	12+14	O8	*Int*
17	Firmware extraction	12+14, 13	O12	*Int U1 U2*
18	Reference signal spoofing	16	O7	all

the behavior of the device. In particular, we examined how external inputs, such as user commands or configurations, propagate through the code and impact crucial functionalities. Subsequently, we conducted an in-depth audit of the firmware’s codebase to locate functions that are commonly associated with security vulnerabilities, such as buffer overflows. The emphasis was on understanding how these functions interacted with (improperly handled) user inputs and external data. Additionally, the scrutiny extended to the broader data processing logic within the firmware, aiming to discover potential security threats in the code supporting the modem’s control logic. Last, we examined the literature to retrieve known vulnerabilities in the software and hardware components/modules adopted in satellite modems, e.g., the web server.

With the integration of multiple techniques, including air interface testing, firmware analysis, historical vulnerability research, and hardware interface analysis, we successfully identified new vulnerabilities in the satellite modems listed in Table 1 and crafted several impactful attacks that exploit these vulnerabilities. A summary of the attacks is presented in Table 5. It also associates each attack with the exploited vulnerabilities in Table 4 and attack objectives/outcomes in Table 2. These attacks span across all three attack surfaces (SCI, GNI, and HW). We provide details of the validated attacks in this section. Note that we intentionally omitted some very specific details, such as the exact values of the parameters, to prevent potential attackers from directly utilizing our findings.

6.2 Attacks against SCI

Attacks 1 to 8 in Table 5 all target the satellite communication interface, which is a satellite-modem-specific component. They could even attack satellite modems that are not connected to the ground network. Attacks 6 and 8 require proximity to the satellite modem, while the others could be launched from remote.



Serial Port: COM9
Baud Rate: 9600

```
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
BB BB BB BB BB BB BB BB BB BB BB BB BB BB BB
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
BB BB BB BB BB BB BB BB BB BB BB BB BB BB BB
```

```
BB BB BB BB BB BB BB BB BB BB BB BB BB BB BB
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
BB BB BB BB BB BB BB BB BB BB BB BB BB BB BB
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
```

(a) Before user message tampering. Modem A sends data “A” to Modem B, and Modem B sends data “B” in response. The data received by Modem A is "B".

```
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
CC CC CC CC CC CC CC CC CC CC CC CC CC CC CC
```

```
BB BB BB BB BB BB BB BB BB BB BB BB BB BB BB
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
BB BB BB BB BB BB BB BB BB BB BB BB BB BB BB
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
```

(b) After user message tampering. Modem A sends data “A” to Modem B, and Modem B sends data “B” in response. But the data received by Modem A is "C"!

Figure 10: User message tampering attacks.

1. Communication data theft. We systematically examined the signal encryption features of all the satellite modems we have acquired and discovered that, despite their capability to support signal encryption, all modems have this feature *turned off* by default. In particular, the encryption function in Comtech’s modems is an add-on feature that has extra cost. This default configuration, coupled with a business model where users need to pay extra for encryption, undoubtedly increases the risk that users may neglect the signal encryption feature, which makes the satellite communication signals more susceptible to attacks against confidentiality.

2. User message tampering/spoofing. Modems with missing or vulnerable authentication are susceptible to message tampering attacks in the absence of traffic encryption. We established a local simulated communication environment based on two Comtech *C3* modems, referred to as A and B. As shown in Figure 10 (top), A sends data packets `0xAA` to B, while B replies with `0xBB`. We utilized AirSecAnalyzer to transmit data with identical communication parameters (frequency, modulation, and rate) but with higher power to tamper the communication from B to A. As shown, data B sent by modem B was altered to `0xCC`.

3. Command tampering attack. The command tampering attack exploits three vulnerabilities in the target satellite modem: unencrypted satellite communication, lack of identity authentication, and lack of command validation. The EDMAC/EDMAC2 protocol, widely used in Comtech modems (WRM), allows the remote management of the modem, such as setting the signal frequency. We analyzed the protocol and discovered a lack of authentication of modem identity and signal timing in Comtech *C2* and *C3*.

To validate this vulnerability, we experimented with three Comtech *C2* modems: one configured as the central station (A), one as the station modem (B), and one as the attacker station (C). Initially, we established an over-the-air communication network between A and B. We used A to send a management command to B to modify its transmission frequency. Simultaneously, we captured the communication signal using AirSecAnalyzer. Next, we configured C as the central station modem and B as the station modem, and restored B’s parameters. We then replayed the captured management command signal from C using AirSecAnalyzer. The replay attack successfully modified B’s transmission frequency. The successful attack confirmed that the EDMAC/EDMAC2 remote management protocol (and its implementation) did not authenticate the identity of the sender modem or the signal timing. To further demonstrate that EDMAC/EDMAC2 also lacked authentication for the receiving modem’s identity, we reconfigured A as the central station modem and C as the station modem. Using the AirSecAnalyzer, we replayed the previously captured signal from A to C, and successfully modified the transmission frequency parameter of C.

4. Unauthorized tampering of network structure. We further exploited network authentication vulnerabilities to tamper with the architecture of the satellite communication network: we first employed A as the central station modem and B as the station modem to establish communication between A and B. We then sent commands via AirSecAnalyzer to modify B's communication parameters, e.g., frequency and bandwidth, to match those of C, which is the central station modem of another network. We then successfully pinged B from a computer connected to C, to confirm that a link between B and C was established. That is, we hijacked B from A's network to C's network. Neither B or C attempted to authenticate the identity of the other party in the communication.

Attacks 3 and 4 exploit the vulnerability in the WRM service EDMAC/EDMAC2, which lacks authentication for signal timing and sender/receiver identity. This vulnerability affects all satellite modems utilizing the EDMAC/EDMAC2 protocol, potentially including all Comtech modems. Attackers may remotely exploit this set of vulnerabilities (2, 3, 4, 6 in Table 4) through over-the-air satellite links to severely tamper with the satellite communication network, e.g., hijack a station or force a station off the network.

5. Identity spoofing. Through reverse engineering of iDirect modems' firmware, we identified a vulnerability that may allow identity spoofing in the CG service named Falcon. In particular, iDirect satellite communication systems utilize a unique identifier for terminal modems known as the "DID" number. We reverse-engineered the Falcon service and recovered the calculation formula for the DID number, which is derived from a unique serial number printed on each modem (due to security considerations, we refrain from providing the specific calculation formula in this document). The attacker could maliciously alter the DID generation function in Falcon on her modem to generate any arbitrary DID for the modem, thereby spoofing any identity. There are several mechanisms for the attacker to learn the DID of a specific modem to launch a targeted attack. For instance, the iDirect X series uses unencrypted communication by default, hence, the attacker can intercept the unencrypted over-the-air communication to learn the DID of the target modem/station as well as its communication parameters. The attacker may also obtain the serial number of a target modem through social engineering and then derive the DID.

6. GNSS attack. GNSS Spoofing is a highly unique attack against satellite modems. Some satellite modems rely on GNSS to determine their locations and then calculate the relative position of the satellites, so that they set their antennas to the correct angle for best signal reception. Fake GNSS signal will trick the modem into believing it is in a different location, and misalign its antenna to a wrong direction, causing weak signals and communication disruptions. We successfully manipulated the antenna parameters in a GNSS attack. In particular, we used AirSecAnalyzer to broadcast fake GPS parameters near the Intellian *Int* modem. From its management interface, we observed that it picked up the signal and changed its location. We also observed that the satellite communication antenna connected to the modem started to deviate from the correct direction, and the deviation grew with the increase of the position error. This discrepancy is attributed to the GNSS spoofing causing the antenna to erroneously believe it is in a different location.

7. Random crash at fuzzing. We used AirSecAnalyzer to fuzz the satellite communication interface of all the modems. For Comtech modems, we observed that both Comtech *C2* and *C3* consistently experienced random system crashes, which always happened within 10 minutes after fuzzing started. We speculate that the crashes may be caused by flaws in the functions that handle the transport layer protocol. First, physical layer errors could lead to communication failures, however, they are unlikely to cause device freezes or crashes. Meanwhile, the fuzzing test that triggered the crash did not involve the transmission of the actual payload (user data), hence, the crash is unlikely caused by user data processing. Therefore, we suspect that the observed crashes may be attributed to logical bugs in package dissection. However, we were unable to pinpoint the exact location of these issues due to the lack of identification of relevant functions in firmware reverse engineering, and the lack of a memory dump at the crash. Nevertheless, this finding suggests that attackers could potentially disrupt the functionality of these two modems by sending meaningless/empty packets.

8. Air signal jamming. In AirSecAnalyzer, we construct a simple signal generation process in GNURadio, which utilizes SDR to generate random noise at maximum power. The generated noise, transmitted through a 3dBi antenna within proximity of our modems, successfully interfered with the experiment modem systems, disrupting the system's normal communication. More complex jamming strategies may be implemented to improve attack efficiency, however, our experiment confirms the viability of this attack.

6.3 Attacks against GNI

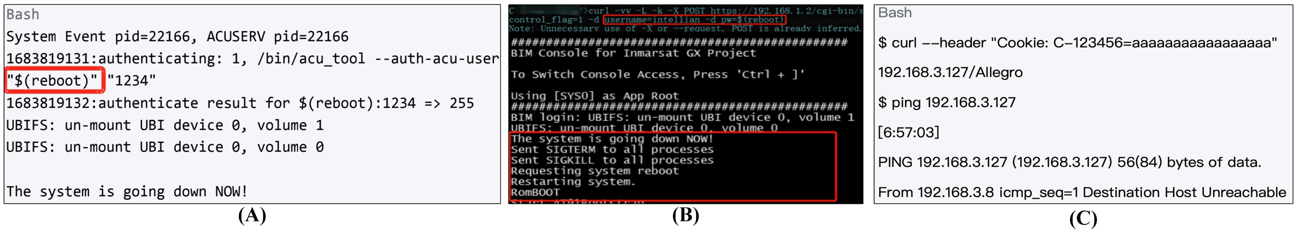
Attacks 9 to 14 in Table 5 target the ground network interface. They could be launched using conventional network attack mechanisms. Attack 9 exploits a satellite-modem-specific vulnerability, while the others all exploit vulnerabilities in standard services.

9. Antenna control (AC) command injection. In the audit of the AC service of Intellian *Int* , we conducted a comprehensive analysis of its codebase. We noticed that the *make_acu_auth_command -> escape_expand()* function only filters out symbols such as "\", leading us to believe that command injection could occur using "$()". To validate this observation, we accessed the device's AC service through port X (we will provide the specific port number after the manufacturer patches the vulnerability). Next, we followed the on-screen instructions to enter "$(reboot)" as the username and a random string as the password. As demonstrated in Figure 11 (A), this input triggered the entire satellite modem system to reboot.

This attack instance indicates that the AC service does not effectively sanitize (risky) parameters in pre-processing the commands. This vulnerability opens the door for attackers to inject arbitrary commands on the modem through the AC service, allowing them to manipulate parameters or disrupt the operation of the satellite modem. We also noticed that the Intellian *Int* modems are actively used in the International Maritime Satellite network operated by Inmarsat [42, 43]. This information creates opportunities for adversaries to launch targeted attacks on Inmarsat.

10. Cross-site scripting (XSS). We identified XSS vulnerabilities in the standard HTTP/HTTPS services (web-based administration interface) in both Comtech *C1* and Intellian *Int* modems.

For Comtech *C1*, if the HTTP/HTTPS request contains parameters undefined on the server, it throws an error and returns the



```
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!
```

(A)

```
C [redacted]>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
```

(B)

```
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
```

(C)

Figure 11: Examples of satellite modem attacks: (A) AC command injection; (B) Web command injection; (C) arbitrary write.

undefined parameters in HTML. The web server does not properly sanitize the returned parameters, hence, user input will be directly displayed, leading to XSS vulnerabilities. An attacker could craft a malicious HTTP/HTTPS request that contains undefined parameters with malicious content, i.e., adversarial client-side script. When a victim user opens the link, the injected script will be executed on the user side. We validated this attack by injecting a simple alert script and confirmed its execution on the victim client.

For Intellian *Int* , we discovered that */cgi-bin/setagent.cgi?type=3* provided an HTML interface to configure server variables. This interface does not sanitize or validate user input so that it could be exploited to inject JavaScript code into the variable values, thus creating an XSS vulnerability for almost all variables configurable through this CGI. To validate this vulnerability, we modified the SYS_IP parameter to include client-side scripts. Subsequently, we observed the successful injection of scripts in the network settings interface. Note that this attack could only be performed by an authenticated user who is authorized to execute the CGI.

The aforementioned attack demonstration confirms that by injecting malicious scripts into a user's web browser, attackers can execute malicious operations when the user is interacting with infected websites. This vulnerability can lead to information disclosure, account hijacking, or other security vulnerabilities.

11. Web command injection. In the firmware of Intellian *Int* , we observed that *setagent.cgi* was invoked through lighttpd requests [2] to handle user login. Further investigation of the processing logic of the username and password parameters in *setagent.cgi* revealed that if the username is present in the system's user file, the password is directly used as a parameter to generate and execute a command line to invoke the system function. In case the password contains a command line, it results in a command injection attack.

To validate this vulnerability, we entered *$(reboot)* as the password, which successfully triggered a system reboot, as demonstrated in Figure 11 (B). This vulnerability could lead to unauthorized access, data disclosure, or system disruption.

12. Unauthorized web operation. In the evaluation of the web interfaces of Comtech *C1* and Intellian *Int*, we observed that many functionalities can be accessed without the need for the Authorization and Cookie fields in the HTTP requests. We utilized Burp Suite to test each form submission. A request to *C1* successfully rebooted the device even after removing the Authorization field from the HTTP header. Additionally, in the form submission interfaces of *C1* and *Int*, it was possible to modify administrator credentials, access lists, and satellite modem control parameters without authentication (by removing the Authorization or Cookie fields from the HTTP request). Consequently, unauthorized attackers can perform actions such as device reboot and device configuration modification to disrupt the normal operation of the devices.

13. SQL injection. The Intellian *Int* modem is found to be vulnerable to an SQL injection exploit, sharing a similar mechanism with the unauthorized web operation attack. The attacker can inject arbitrary SQL queries into the modem's SQL operations without any authorization. This vulnerability poses a significant risk, potentially leading to the unauthorized disclosure and tampering of parameters stored in the satellite modem's database.

14. Arbitrary write. In the firmware of Comtech *C1*, we identified strings related to RomPager (v. 4.10), a commercial web server widely adopted by embedded devices. RomPager (versions 4.34 and lower) has been associated with a significant vulnerability known as Misfortune Cookie [12], which can lead to memory errors by manipulating the cookie value in an HTTP packet.

According to the RomPager 4.34 exploitdb script, constructing the cookie field in the HTTP header as: *"Cookie: C" + str(num) + "=" + "B" * n + data + ";"* triggers a memory vulnerability. We further examined the firmware and found that the cookie in the format *Cn=yyy* is handled as follows: the system multiplies int *n* by 0x28, adds a base address, and uses the result address to store *yyy*. Consequently, if the system does not validate *n*, it may write *yyy* to any arbitrary address. In our experiments, we found that triggering this vulnerability requires a sufficiently large negative integer *n*. As shown in Figure 11 (C), we exploited this vulnerability with string "*Cookie: C-123456=aaaaaaaaaaaaaaaa*" and successfully crashed the TCP stack of the RTOS, so that the device became unreachable.

6.4 Attacks against Hardware

Attacks 15 to 18 in Table 5 target modem hardware. They assume a stronger attack model that the adversary has physical access to the modem. This is possible for modems located in remote stations.

15. System information theft: We discovered that the Intellian *Int*'s console port is interactive and unprotected, which allowed us to get the information printed by the bootloader (BL) from power-on to initialization. From this initialization log, we identified AT91Bootstrap as the first-level bootloader. AT91Bootstrap, serving as the bootloader for Microchip Technology's AT91 series chips, initializes hardware and memory, and then downloads the main program from a specified storage medium to memory for booting. We identified four storage chips (EEPROM, Nand Flash, and 2× SPI Flash). By analyzing the roles of each storage chip based on hardware and U-Boot startup logs, we found that the Nand Flash stores the kernel and file system, two SPI Flash chips mainly store bootstrap and bootloader, while EEPROM is speculated to hold parameters like network card addresses. This analysis indicates that the initialization information printed by BL exposes the underlying technical details of the satellite modem. Additionally, we observed that the system uses U-Boot as the second-level bootloader, with access to the U-Boot command line through the console port.

16. Device control. As described above, we accessed the U-Boot command line of Intellian *Int* through its console port. We further utilized *setenv* command to inject *init=/bin/sh*, to force the kernel to boot directly into root shell, and took control of the modem. In this process, we exploited a vulnerability in U-Boot that lacked effective permission management, enabling us to escalate the privileges.

17. Firmware extraction. We obtained the firmware of Intellian *Int*, UHP *U1* and *U2* through hardware access. As mentioned earlier, we gained shell access to Intellian *Int* through its BL vulnerability. To extract the firmware, we configured and enabled the ground network interface through the shell access. Subsequently, utilizing SecureCRT's scripting functionality for automated file transfer, we established a TFTP server to receive files. The firmware was then transferred in batches, files were concatenated, and we ultimately obtained the device's firmware. For UHP *U1* and *U2* modems, we extracted the firmware from the flashrom chip by desoldering it from the modem's mainboard and placing it into a programmer socket. The firmware extraction process was completed using a Raspberry Pi. The extracted firmware will enable the adversaries to further examine the code base to discover further vulnerabilities.

18. Reference signal spoofing. In this attack, the adversary can inject an adversarial reference frequency signal generated by a frequency source into the exposed coaxial RF cable. The injected reference slightly deviates from the correct reference to disrupt the modem operation without being detected. However, executing this attack requires a complete satellite communication system for real data reception and transmission, along with the necessary satellite communication licenses and permissions. Consequently, we did not physically carry out this attack. Nevertheless, the product documentation provided by LNB manufacturers [1, 3, 22] explicitly specifies the external reference frequencies required for their LNB products, providing substantial evidence that attackers could exploit vulnerabilities through reference signal injection.

7 Mitigation and Defense

To enhance satellite modem security, a multifaceted approach is critical, which consists of robust authentication, proper encryption practices, firmware management, network configurations, physical security, comprehensive monitoring, and awareness programs. In particular, we recommend the following defense mechanisms: (1) *Authentication and Access Control*: Implementing strong authentication measures is essential. As shown in Section 6, weak/vulnerable authentication is the root cause of several attacks against the SCI. We recommend multi-factor authentication as well as regularly review and update access policies, taking into account potential threats obtained from publicly available information. (2) *Encryption practices*: End-to-end and link encryptions should be properly deployed across communication interfaces to safeguard data in transit. Update encryption protocols and algorithms to address vulnerabilities exposed through public information. Employ industry-standard encryption methods and stringent key management practices. (3) *OS and firmware management*: Prioritize routine updates for OS and firmware to patch vulnerabilities. Utilize public information for proactive vulnerability management. Establish streamlined processes for users to receive and apply updates promptly, minimizing exposure to known threats. (4) *Secure the embedded services*: The security of the embedded services is often neglected by both the device vendors and the end users. Services should be hidden from the external network unless absolutely necessary. The embedded services should always be patched up-to-date. The modem vendors should provide a convenient means for the users to update add-on services. (5) *Network isolation and firewall*: Enhance security through network isolation and careful firewall configurations. Isolate modems within secure networks to limit lateral movement opportunities. Regularly audit and update firewall rules based on emerging threats and insights from public information to maintain effective perimeter defenses. (6) *Physical security measures*: Limit physical access to modem facilities and hardware and implement robust surveillance and access controls. Regularly conduct security audits to ensure physical security remains resilient to evolving threats. (7) *Comprehensive Monitoring and Logging*: Build a robust monitoring infrastructure to detect and respond to security events effectively. Configure logging systems to capture relevant security data and anomalies. Implement real-time alerts for suspicious activities, integrating insights from public information into monitoring processes. (8) *Security Awareness and Training*: Address the impact of publicly available information on social engineering attacks in comprehensive security awareness programs. Regularly update training programs to include evolving threats and attack vectors. Foster a culture of security awareness among users, manufacturers, and other stakeholders, promoting proactive security practices. (9) *Regular Security Assessments*: Integrate insights from public information into routine security assessments. Conduct regular vulnerability scans, penetration testing, and risk assessments to identify and address potential weaknesses. Establish a feedback loop for continuous improvement based on assessment findings, ensuring a proactive security posture.

8 Related Work

The literature on satellite communication network security collectively addresses a spectrum of challenges in the overarching system [23, 27, 50, 51, 60] or with the satellites [52–54, 61]. Existing research on satellite modems primarily focuses on technical improvements or specific functionalities, while little effort has been devoted to security and privacy. [32, 64] provided analyses and discussions of the implementations of satellite modems. [31, 37, 38, 40, 49, 57, 58, 65] examined the software and hardware architecture of their modems. Others studied particular aspects, such as modulation and demodulation algorithms [24, 25, 30, 34, 36, 39, 59].

Security analyses of satellite modems primarily targeted on the exploitation of specific vulnerabilities [4–11, 13–18]. While they contributed valuable insights into the security practice, these efforts primarily focused on isolated instances, lacking a systematic and comprehensive view of the broader spectrum of security issues in satellite modems. Moreover, the vulnerabilities were mostly discovered in the standard services (e.g., SQL) and web UI [4–10, 13–18], with limited coverage on the hardware [11, 62] and the encryption algorithm [35, 45], while the most unique features of satellite modems and satellite communications are largely neglected.

9 Conclusion

In this paper, we present the first comprehensive security analysis of satellite communication modems. We first disassemble nine commodity satellite modems from four vendors and thoroughly examine their hardware and software components. We explore satellite models that are exposed to the Internet and discuss the risks. We further propose three attack models against three main attack surfaces in satellite modems and provide a comprehensive security analysis of vulnerabilities in each attack surface. We conduct empirical experiments on real-world satellite modems, which demonstrate how practical attacks are enabled by such vulnerabilities. Finally, armed with our findings, we provide actionable security recommendations for satellite communication modems.

References

[1] [n. d.]. KU-Band PLL LNB MODEL. https://www.stepelectronics.com.au/wp-content/uploads/2020/10/NJRC-Ku-PLL-LNB-Ext_NJR2934E_35E_36E_37E_39E_rev07.pdf

[2] [n. d.]. lighttpd open-source web server. Available at: https://www.lighttpd.net/.

[3] [n. d.]. Orbital 5400X Off-the-Shelf External Reference Ku-Band LNB. https://orbitalresearch.net/wp-content/uploads/2019/12/Orbital-5400X-Off-the-Shelf-External-Reference-Ku-Band-LNB-web-1912.pdf

[4] 2013. CVE-2013-6034. https://nvd.nist.gov/vuln/detail/CVE-2013-6034

[5] 2013. CVE-2013-6035. https://nvd.nist.gov/vuln/detail/CVE-2013-6035

[6] 2014. CVE-2014-0326. https://nvd.nist.gov/vuln/detail/CVE-2014-0326

[7] 2014. CVE-2014-0327. https://nvd.nist.gov/vuln/detail/CVE-2014-0327

[8] 2014. CVE-2014-2942. https://nvd.nist.gov/vuln/detail/CVE-2014-2942

[9] 2014. CVE-2014-2950. https://nvd.nist.gov/vuln/detail/CVE-2014-2950

[10] 2014. CVE-2014-2951. https://nvd.nist.gov/vuln/detail/CVE-2014-2951

[11] 2014. CVE-2014-2964. https://nvd.nist.gov/vuln/detail/CVE-2014-2964

[12] 2015. CVE-2015-9222. https://nvd.nist.gov/vuln/detail/CVE-2015-9222

[13] 2016. CVE-2016-9495. https://nvd.nist.gov/vuln/detail/CVE-2016-9495

[14] 2016. CVE-2016-9496. https://nvd.nist.gov/vuln/detail/CVE-2016-9496

[15] 2016. CVE-2016-9497. https://nvd.nist.gov/vuln/detail/CVE-2016-9497

[16] 2018. CVE-2018-19391. https://nvd.nist.gov/vuln/detail/CVE-2018-19391

[17] 2018. CVE-2018-19392. https://nvd.nist.gov/vuln/detail/CVE-2018-19392

[18] 2019. CVE-2019-15652. https://nvd.nist.gov/vuln/detail/CVE-2019-15652

[19] 2020. CVE-2020-12351. https://nvd.nist.gov/vuln/detail/CVE-2020-12351

[20] 2020. CVE-2020-24587. https://nvd.nist.gov/vuln/detail/CVE-2020-24587

[21] 2020. CVE-2020-24588. https://nvd.nist.gov/vuln/detail/CVE-2020-24588

[22] LNB QUAD-BAND EXT REF 1000XU-2. [n. d.]. KU-Band PLL LNB MODEL. https://cdn.shopify.com/s/files/1/1094/0100/files/1000xu_2_lnb.pdf?14577775421144751663

[23] Ijaz Ahmad et al. 2022. Security of Satellite-Terrestrial Communications: Challenges and Potential Solutions. *IEEE Access* 10 (2022), 96038–96052.

[24] RD Allan, JR Bramwell, DA Saunders, and M Tomlinson. 1988. A high performance satellite data modem using real-time digital signal processing techniques. *Journal of the Institution of Electronic and Radio Engineers* 58, 3 (1988), 117–124.

[25] S. Benedetto, R. Garello, G. Montorsi, C. Berrou, C. Douillard, D. Giancristofaro, A. Ginesi, L. Giugno, and M. Luise. 2005. MHOMS: high-speed ACM modem for satellite applications. *IEEE Wireless Communications* 12, 2 (2005), 66–77.

[26] bleepingcomputer. 2022. Viasat confirms satellite modems were wiped with AcidRain malware. https://www.bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/

[27] Matthew Bradbury et al. 2020. Identifying attack surfaces in the evolving space industry using reference architectures. In *2020 IEEE Aerospace Conference*. IEEE.

[28] breakingdefense. 2023. Comtech's Army SATCOM modem win opens door to cross-service sales. https://breakingdefense.com/2023/10/comtechs-army-satcom-modem-win-opens-door-to-cross-service-sales/

[29] businesswire. 2020. Comtech Receives Satellite Modem Order. Available at: https://www.businesswire.com/news/home/20201022005364/en.

[30] Enrico Casini, R De Gaudenzi, and Alberto Ginesi. 2004. DVB-S2 modem algorithms design and performance over typical satellite channels. *International journal of satellite communications and networking* 22, 3 (2004), 281–318.

[31] Osman Ceylan, Alican Caglar, Halim Bahadir Tugrel, Hasan Onur Cakar, Ahmet Oguz Kislal, Kaan Kula, and Hasan Bulent Yagci. 2016. Small Satellites Rock A Software-Defined Radio Modem and Ground Station Design for Cube Satellite Communication. *IEEE Microwave Magazine* 17, 3 (2016), 26–33.

[32] D. Chakraborty and C. Wolejsza. 1983. A Survey of Modem Design and Performance in Digital Satellite Communications. *IEEE Journal on Selected Areas in Communications* 1, 1 (1983), 5–20.

[33] cyble. 2023. Hacktivists Targeting Satellite and Space Industry. https://cyble.com/blog/ghostsec-targeting-satellite-receivers/

[34] E. Del Re, A. Fanfani, S. Morosi, and L. S. Ronga. 2014. Robust modem design for satellite communications in emergency scenarios. In *ASMS/SPSC*.

[35] Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, and Thorsten Holz. 2012. Don't trust satellite phones: A security analysis of two satphone standards. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 128–142.

[36] Alessio Fanfani, Simone Morosi, Luca Ronga, and Enrico Del Re. 2018. Frequency recovery techniques for TM/TC satellite modem in critical scenarios. *International Journal of Satellite Communications and Networking* 36, 2 (2018).

[37] Rajeev Gopal. 2018. Resilient Satellite Communications with Autonomous Multi-Modem Adapter. In *IEEE MILCOM*.

[38] WP3 GROUP. 2001. DSP-based CDMA satellite modem: CNIT/ASI project. In *Software Radio: Technologies and Services*. Springer.

[39] Yanpeng Guo and K. Feher. 1995. A new FQPSK modem/radio architecture for PCS and mobile satellite communications. *IEEE Journal on Selected Areas in Communications* 13, 2 (1995), 345–353.

[40] C. Heegard, J. Heller, and A. Viterbi. 1978. A Microprocessor-Based PSK Modem for Packet Transmission Over Satellite Channels. *IEEE Trans. Comm.* 26, 5 (1978).

[41] iDIRECT. [n. d.]. openAMIP. https://www.idirect.net/products/openamip/

[42] intelliantech. [n. d.]. Introducing the all new GX terminals for the Inmarsat Fleet Xpress service. https://www.intelliantech.com/en/products/inmarsat-gx-maritime-terminals/#

[43] intelliantech. 2020. Inmarsat Partner focus: Intellian Technologies. https://www.inmarsat.com/en/insights/government/2020/inmarsat-partner-focus-intellian-technologies.html

[44] intelliantech. 2023. case study of providing solutions. https://www.intelliantech.com/en/news/case-study#

[45] Jingmei Liu, Linsen Zhao, and Jingwei Liu. 2017. A real-time attack on the GMR-2 encryption algorithm in satellite phones. *China Communications* 14, 11 (2017).

[46] Markets and Markets. 2021. Satellite Modem Companies - Comtech Telecommunications Corp. (US) and ST Engineering (Singapore) are the Key Players. Available at: https://www.marketsandmarkets.com/ResearchInsight/satellite-modem-market.asp.

[47] meritalk. 2023. DISA Awards 16 Satellite-Based Services Contracts. https://www.meritalk.com/articles/disa-awards-16-satellite-based-services-contracts/

[48] osqzss. [n. d.]. Software-Defined GPS Signal SimulatorL. https://github.com/osqzss/gps-sdr-sim

[49] H.I. Paul. 2002. Multi-carrier network-centric satellite communications modem design. In *MILCOM*.

[50] James Pavur et al. 2019. Secrets in the sky: on privacy and infrastructure security in dvb-s satellite broadband. In *ACM WiSec*.

[51] Jordan Plotnek and Jill Slay. 2022. New Dawn for Space Security. In *International Conference on Cyber Warfare and Security*, Vol. 17.

[52] Swapnil Sayan Saha et al. 2019. Ensuring cybersecure telemetry and telecommand in small satellites: Recent trends and empirical propositions. *IEEE Aerospace and Electronic Systems Magazine* 34, 8 (2019), 34–49.

[53] Edd Salkield et al. 2023. Firefly: Spoofing Earth Observation Satellite Data through Radio Overshadowing. *arXiv* (2023).

[54] Edd Salkield et al. 2023. Satellite Spoofing from A to Z: On the Requirements of Satellite Downlink Overshadowing Attacks. In *ACM WiSec*.

[55] satmagazine. 2010. Comtech provides dSCPC bandwidth management of the space segment. Available at: http://www.satmagazine.com/story.php?number=1881861986.

[56] Skybrokers. 2017. Skybrokers supported Teleport clients as well as Satellite Services Service providers with iDirect's new X3, X5 and X7-series. Available at: https://sky-brokers.com/supplier/idirect-technologies-inc/.

[57] F. Takahata, M. Yasunaga, Y. Hirata, T. Ohsawa, and J. Namiki. 1987. A PSK Group Modem for Satellite Communications. *IEEE ISAC* 5, 4 (1987).

[58] K. Tanabe, Y. Sagawa, K. Kobayashi, K. Ohata, and M. Ueba. 2002. An Architecture of Group MODEM with Timesharing Processing for Satellite Communication Networks. In *Joint Conference on Satellite Communications*. 125–130.

[59] Moysis Tsamsakizoglou. 2012. Radiation tolerant satellite communication modem.

[60] Vijay Varadharajan and Neeraj Suri. 2022. Security Challenges When Space Merges with Cyberspace. *arXiv preprint arXiv:2207.10798* (2022).

[61] Johannes Willbold et al. 2023. Space Odyssey: An Experimental Software Security Analysis of Satellites. In *IEEE Symposium on Security and Privacy*.

[62] Lennert Wouters. 2022. Glitched on Earth by Humans: A Black-Box Security Evaluation of the SpaceX Starlink User Terminal. Black Hat USA, Las Vegas, US.

[63] Peng Wu, Shaojing Su, Zhen Zuo, Xiaojun Guo, Bei Sun, and Xudong Wen. 2019. Time difference of arrival (TDoA) localization combining weighted least squares and firefly algorithm. *Sensors* 19, 11 (2019), 2554.

[64] Fuqin Xiong. 1994. Modem techniques in satellite communications. *IEEE Communications Magazine* 32, 8 (1994), 84–98. https://doi.org/10.1109/35.299842

[65] Shengkang Zhang, Xueyun Wang, Haifeng Wang, Hongbo Wang, Yuan Yuan, and Keming Feng. 2015. A new modem for two way satellite time and frequency transfer. In *IEEE EFTF/IFCS*.