Satellite Systems (SATCOM) Security

Nov 19, 2022

DSCI 519
Chenglin Jiang, Rhiston Yu

Overview

- Satellites play an increasingly significant role in today’s technology, from providing telecommunication services, to enabling logistics and navigation through GPS, to 5g backhauls and Internet of Things, and to the intelligence gathering conducted by nation states
- Security has been left behind with the widespread deployment and use of satellites
- As more satellites are deployed, more satellites must be protected
- Most satellites rely upon security through obscurity
- Current approaches to securing satellites isn’t fundamentally different from securing any other system
  - Same traditional IT “best practices” apply

Current Approaches

- Security through obscurity
- Defense in depth approach
- Industry “best practices”
  - Joint CISA/FBI Advisory
  - Mitigation Strategies:
    - Use secure methods for authentication.
    - Enforce principle of least privilege.
    - Review trust relationships.
    - Implement encryption.
    - Ensure robust patching and system configuration audits.
    - Monitor logs for suspicious activity.
    - Ensure incident response, resilience, and continuity of operations plans are in place.

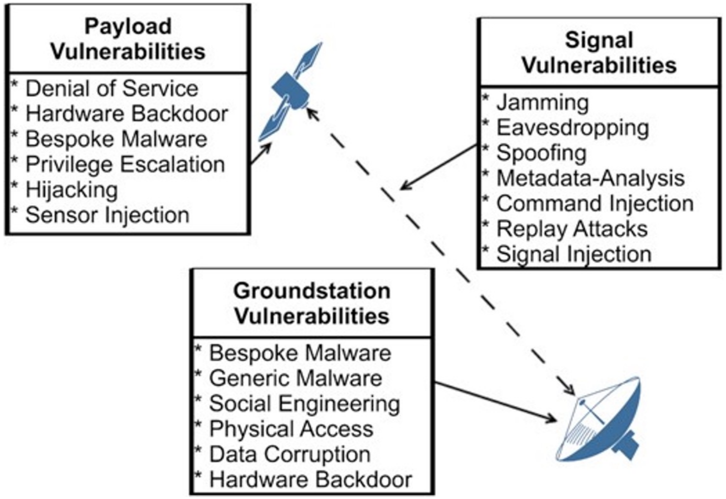
Unique Technical Security Challenges

- Most satellites were launched 10-15 years ago and have an average lifespan of about 10 years
- Satellites are not designed with security in mind
    - Compute-constrained devices with limited resources and have significant security/performance trade-offs
        - Security was not a requirement when most satellites were launched
    - Industry “best practices” is not enough or may not even work
    - How do you roll out patches and updates to satellites that were not designed to receive them?
- High number of system entry points and attack vectors
    - Difficult to trace and mitigate cyber attacks

SATCOM Attacks

Example of attacks:

- Subversion of ground system capabilities by utilizing the ground system to maliciously interact with a satellite
- Communications hacking on TT&C systems via command link injection, replay attacks, or electronic attacks like jamming and spoofing
- Malicious features embedded during hardware development, including hardware-based trojans
- Design vulnerability exploitation, where designed-in features of the system are used for malicious purposes, i.e., direct memory writes to a satellite
- Software weaknesses and vulnerabilities exploitation
- Insider threats



Payload Vulnerabilities

* Denial of Service
* Hardware Backdoor
* Bespoke Malware
* Privilege Escalation
* Hijacking
* Sensor Injection

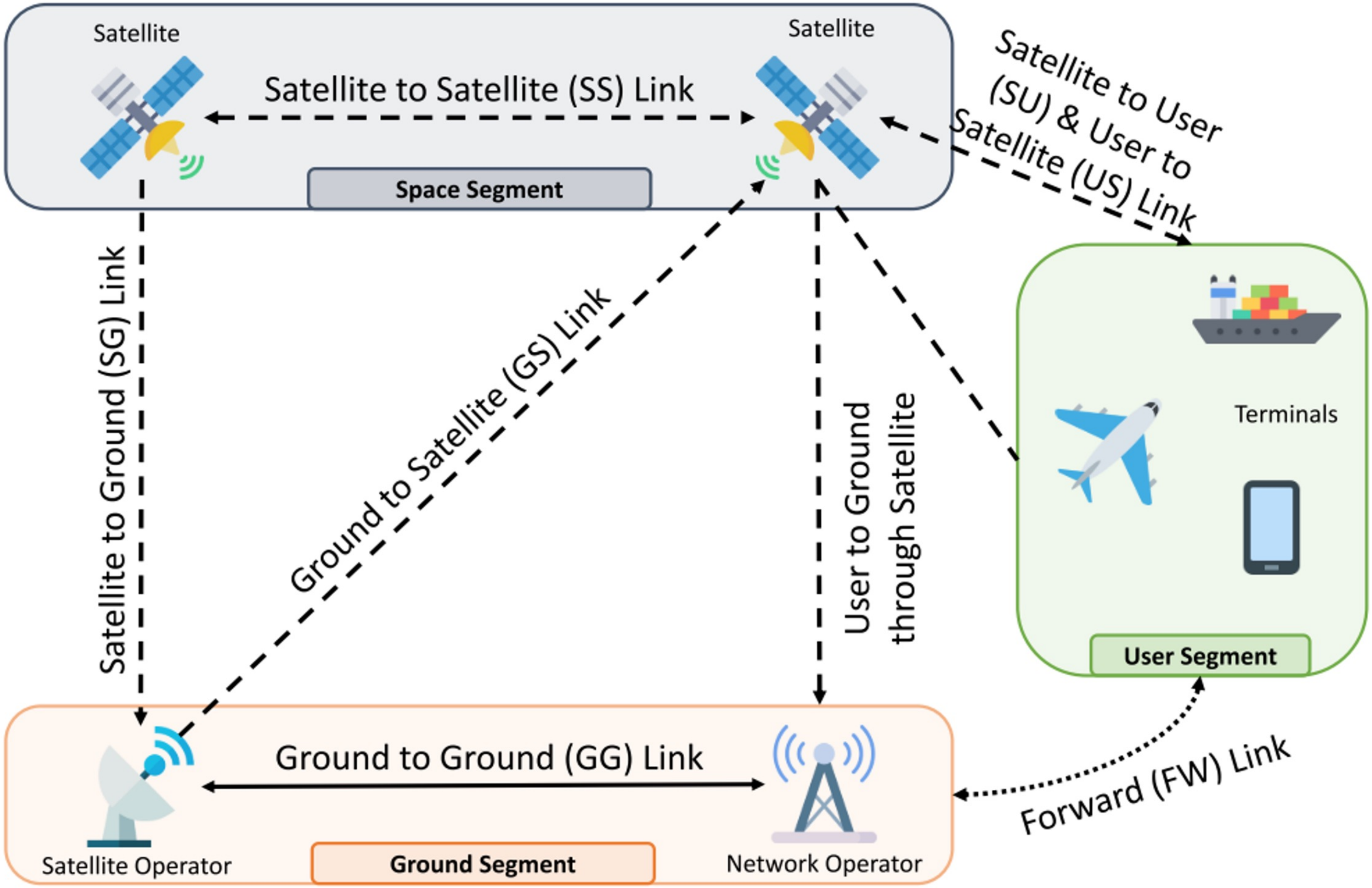
Signal Vulnerabilities

* Jamming
* Eavesdropping
* Spoofing
* Metadata-Analysis
* Command Injection
* Replay Attacks
* Signal Injection

Groundstation Vulnerabilities

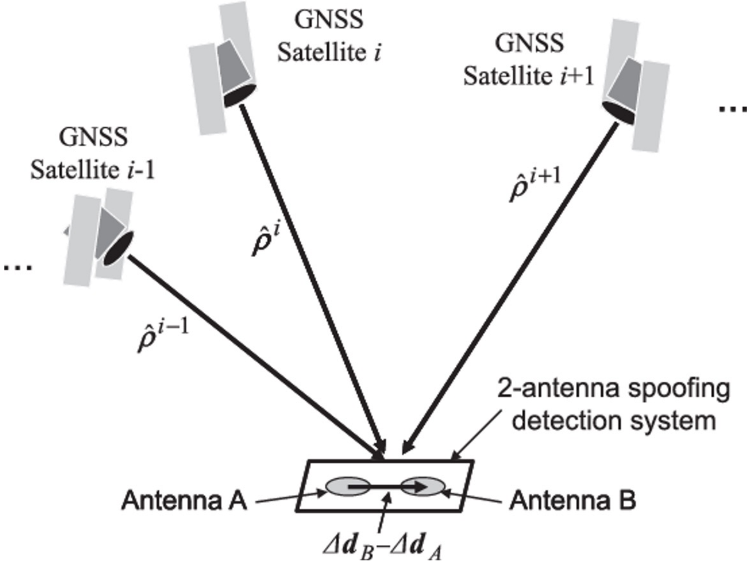
* Bespoke Malware
* Generic Malware
* Social Engineering
* Physical Access
* Data Corruption
* Hardware Backdoor

SATCOM Architecture


Satellite
Satellite
Satellite to Satellite (SS) Link
Space Segment
Satellite to User (SU) & User to Satellite (US) Link
Satellite to Ground (SG) Link
Ground to Satellite (GS) Link
User to Ground through Satellite
Terminals
User Segment
Ground to Ground (GG) Link
Forward (FW) Link
Satellite Operator
Ground Segment
Network Operator

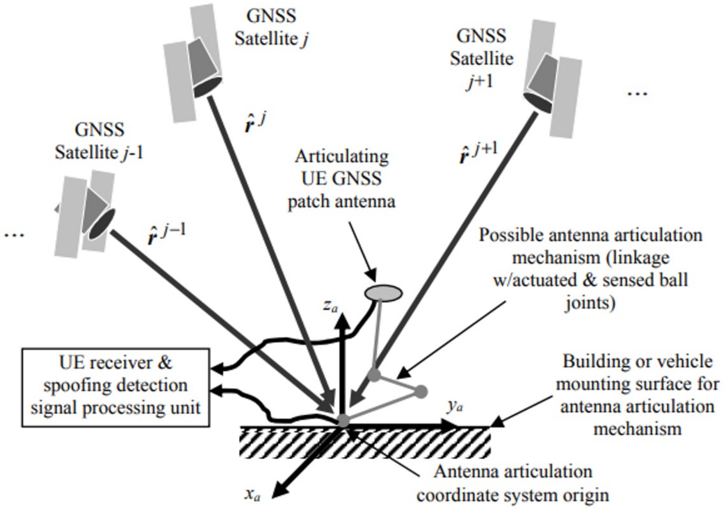
Defending Against Signal Attacks: GNSS Anti-Spoofing

- Spoofing Detection
  - Use of Physical-layer information
  - Multiple Receiving Antennas
  - Ad-Hoc Network Infrastructures



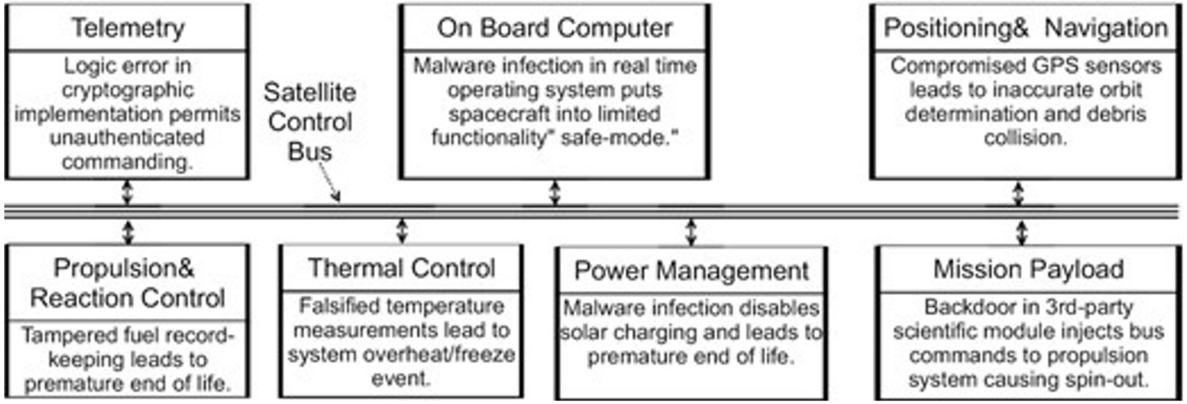
Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data

- The method uses a short segment of beat carrier-phase time histories that are collected while the receiver's single antenna is undergoing a known, high frequency motion profile, typically one pre-programmed into an antenna articulation system
- The spoofing detection algorithm correlates high-pass-filtered versions of the known motion component with high-pass-filtered versions of the carrier phase variations. True signals produce a specific correlation pattern, and spoofed signals produce a recognizably different correlation pattern if the spoofer transmits its false signals from a single antenna.


GNSS Satellite j
GNSS Satellite j+1
...
GNSS Satellite j-1
...
$\hat{r}^{j}$
$\hat{r}^{j+1}$
$\hat{r}^{j-1}$
Articulating UE GNSS patch antenna
Possible antenna articulation mechanism (linkage w/actuated & sensed ball joints)
z_a
y_a
x_a
UE receiver & spoofing detection signal processing unit
Building or vehicle mounting surface for antenna articulation mechanism
Antenna articulation coordinate system origin

Satellite Payload Security

- Four general attack surfaces: input systems like sensors and RF antennae, output systems (i.e. telemetry transmitters), internal communications (internal network/Spacewire buses), and the underlying flight computer that integrates all the components
- Current defense against payload attacks
  - RF encryption and specialized groundstation hardware mitigate the risk of malicious attackers
  - However, if these boundary protections are overcome, lateral movement aboard the spacecraft and privilege escalation is extremely easy
- Example satellite architecture with compromise scenarios for onboard sub-system:



Telemetry

Logic error in cryptographic implementation permits unauthenticated commanding.

Satellite Control Bus

On Board Computer

Malware infection in real time operating system puts spacecraft into limited functionality" safe-mode."

Positioning& Navigation

Compromised GPS sensors leads to inaccurate orbit determination and debris collision.

Propulsion& Reaction Control

Tampered fuel record-keeping leads to premature end of life.

Thermal Control

Falsified temperature measurements lead to system overheat/freeze event.

Power Management

Malware infection disables solar charging and leads to premature end of life.

Mission Payload

Backdoor in 3rd-party scientific module injects bus commands to propulsion system causing spin-out.

Satellite Payload Security (Cont'd)

- Suggested mitigations against payload hijacking
  - Frequent, automatic re-imaging of satellite software
    - Store a verified secure copy of the satellite operating system on a trusted platform module (TPM)
    - Could limit the amount of time an attacker to abuse the system
    - Downsides? Cannot patch other vulnerabilities
- Limited bandwidth, data-storage, and compute capabilities of satellites means that it is uneconomical and difficult to implement proposed defenses against payload attacks
- More research is needed

References

1. Berning, Jack. “What Hackers Can Teach Us About Satellite Security.” *Freethink*, 8 July 2021, https://www.freethink.com/series/coded/satellite-security.
2. Corporation, The Aerospace. “Protecting Space Systems from Cyber Attack.” *Medium*, Medium, 10 May 2022, https://aerospacecorp.medium.com/protecting-space-systems-from-cyber-attack-3db773aff368.
3. “GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data .” *Cornell University*, https://gps.mae.cornell.edu/Paper_F5_8_ION_GNSS_2013b.pdf.
4. Pavur, James, and Ivan Martinovic. “Building a Launchpad for Satellite Cyber-Security Research: Lessons from 60 Years of Spaceflight.” *Academic.oup.com*, 20 June 2022, https://academic.oup.com/cybersecurity/article/8/1/tyac008/6611670.
5. Stremlau, Thorsten. “The Vulnerability of Satellite Communications.” *Security Magazine RSS*, Security Magazine, 25 Feb. 2021, https://www.securitymagazine.com/articles/94689-the-vulnerability-of-satellite-communications.
6. “Strengthening Cybersecurity of SATCOM Network Providers and Customers: Alert(AA22-076A).” *CISA*, 17 Mar. 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-076a.
7. Tedeschi, Pietro, et al. “Satellite-Based Communications Security: A Survey of Threats, Solutions, and Research Challenges.” ArXiv.org, 29 July 2022, https://arxiv.org/abs/2112.11324.
8. L. Heng, D. B. Work and G. X. Gao, "GPS Signal Authentication From Cooperative Peers," in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 4, pp. 1794-1805, Aug. 2015, doi: 10.1109/TITS.2014.2372000.