

# Security Challenges in Modern Space and Satellite Systems

Johannes Willbold

## Abstract

Space systems have become a vital part of modern technology and a backbone of critical infrastructure by offering telecommunications, Earth observation, global navigation, and scientific research services. Their widespread application has been fueled by a stark increase in the number of satellites in Earth's orbit, which is in turn attributed to a new era of space exploitation — the *New Space* era. This era has been defined through affordable small satellites, increasingly ambitious missions, and falling launch costs that enable democratized space access. However, as these systems have become ubiquitous, they have become more attractive to attackers aiming to disrupt their services, as witnessed in several conflicts around the world. Usually, mounting security criticality and exposure prompts increasing research efforts, but space security research has historically been slow and focused on their telecommunications aspect.

Therefore, in this work, we advance the overall state of research around the security of space systems in three main contributions that each explore a novel aspect that has not been subject to public research before. First, we present the first systematic security analysis of real-world satellites to explore the security issues associated with onboard software, where we find significant vulnerabilities in all satellites. We categorize our results based on a new threat taxonomy and challenge our results using a survey among professional satellite developers. Second, we investigate the complete absence of exploit mitigation techniques on satellites. To rule out issues with the underlying ecosystems, we first conduct a comprehensive survey of flight computers. We identify cosmic radiation as a potential source of issues and propose the first fully binary-agnostic fault-injection approach, which we use to measure the impact of cosmic radiation on binary hardening techniques. We find that stack canaries degrade reliability beyond their code-size impact, whereas other techniques, such as control-flow integrity, have no significant effect. Third, we study the security issues associated with Very Small Aperture Terminals (VSATs) used for satellite-based internet connectivity. We conduct a security analysis of two VSAT systems, focusing on the command-and-control layer, where we identify several critical vulnerabilities. We then categorize our findings in a threat model and expose several insecure VSAT design patterns.

## Zusammenfassung

Weltraumssysteme sind zu einem essenziellen Teil moderner Technologie und zu einem Rückgrat kritischer Infrastruktur geworden durch ihre Fähigkeit, Telekommunikation, Erdbeobachtung, globale Navigation, und wissenschaftliche Erkundung anzubieten. Ihre weite Verbreitung wurde durch die steigende Zahl von Satelliten im Erdorbit befeuert, welche im Gegenzug dem Einläuten einer neuen Ära der Weltraumerkundung zuzuschreiben ist — der *New Space* Ära. Diese Ära wurde durch kostengünstige Kleinsatelliten, zunehmend ambitionierte Missionen und fallende Startkosten definiert, welche in Summe deinen breiteren Weltraumzugang ermöglichen. Mit der Allgegenwart dieser Systeme steigt dabei auch deren Attraktivität für Angreifer, welche darauf abzielen, ihre Dienste zu unterbrechen, wie es bereits in mehreren Konflikten weltweit zu beobachten war. Für gewöhnlich führen wachsende Sicherheitsbedeutsamkeit und erhöhte Aufmerksamkeit zu einem gesteigerten Interesse an der Forschung. Doch die Forschung im Bereich

der Sicherheit von Weltraumsystemen ist historisch langsam und konzentriert sich vor allem auf Telekommunikationsaspekte.

Aus diesem Grund treibt diese Arbeit den aktuellen Forschungsstand um die Sicherheit des Weltraumsystems durch drei Hauptbeiträge, welche jeweils einen bis jetzt nicht öffentlich untersuchten Aspekt beleuchten, voran. Zuerst präsentieren wir die erste systematische Sicherheitsanalyse von realen Satelliten, um die Sicherheitsprobleme, welche in der Kontrollsoftware auftreten können, genauer zu untersuchen. Dabei stellen wir mehrere signifikante Schwachstellen in allen untersuchten Satelliten fest. Wir kategorisieren diese Ergebnisse basierend auf einer neuen Bedrohungstaxonomie und überprüfen diese mit einer Umfrage unter professionellen Satellitenentwicklern.

Als Zweites untersuchen wir die vollständige Abwesenheit von Techniken, welche Exploits auf Satelliten verhindern. Um Probleme im zu Grunde liegenden Ökosystem auszuschließen, habe ich dazu eine umfassende Bestandsaufnahme von Flugcomputern durchgeführt. Dabei haben wir kosmische Strahlung als potenzielle Ursache ausgemacht und schlagen zur genaueren Untersuchung den ersten vollständig programagnostischen Fault-Injection-Ansatz vor, welchen wir verwenden, um den Einfluss kosmischer Strahlung auf Exploitverhinderungstechniken zu messen. Dabei stellen wir fest, dass Stack-Canaries die Zuverlässigkeit des Programms stärker beeinträchtigen als deren Zuwachs des Gesamtcodes erklären lässt, während andere Techniken wie Control-Flow-Integrität keinen signifikanten Einfluss haben.

Drittens untersuchen wir die Sicherheitsprobleme im Zusammenhang mit Very Small Aperture Terminals (VSATs), die für satellitengestützte Internetanbindung verwendet werden. Dazu führen wir eine Sicherheitsanalyse zweier VSAT-Systeme durch, wobei wir uns auf die Command-and-Control-Ebene fokussieren und dabei mehrere kritische Schwachstellen identifizieren. Im Anschluss ordnen wir unsere Ergebnisse in ein neu entwickeltes Bedrohungmodell für VSAT-Systeme ein und zeigen dabei mehrere unsichere Designmuster auf.