

Proceedings

**SpaceSec 2023**

**Workshop on  
Security of Space and  
Satellite Systems**

February 27, 2023  
San Diego, CA, USA

*Published by the*





---

**Internet Society**  
**11710 Plaza America Drive**  
**Suite 400**  
**Reston, VA 20190**

---

Copyright © 2023 by the Internet Society.  
All rights reserved.

This volume is published as a collective work. The Internet Society owns the copyright for this publication and the copyrights to the individual papers are retained by their respective author[s].

Address your correspondence to: NDSS Program Manager, Internet Society, 11710 Plaza America Drive, Suite 400, Reston, VA 20190 USA, tel. +1 703 439 2120, fax +1 703 326 9881, [ndss@elists.isoc.org](mailto:ndss@elists.isoc.org).

*The papers included here comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interest of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors or the Internet Society.*

ISBN Number (Digital Format) 1-891562-89-4

*Additional copies may be ordered from:*



**Internet Society**  
11710 Plaza America Drive  
Suite 400  
Reston, VA 20190  
tel +1 703.439.2120  
fax +1 703.326.9881  
<http://www.internetsociety.org>

## **Table of Contents**

### **Message from the Program Co-Chairs Program Committee Co-Chairs Program Committee**

### **Threat Modelling**

Cybersecurity of COSPAS-SARSAT and EPIRB: threat and attacker models, exploits, future research

*Andrei Costin, Hannu Turtiainen, Syed Khandkher, Timo Hämäläinen*

Position Paper: Space System Threat Models Must Account for Satellite Sensor Spoofing

*Benjamin Cyr, Yan Long, Takeshi Sugawara, Kevin Fu*

### **Link Segment Security**

Death By A Thousand COTS: Disrupting Satellite Communications using Low Earth Orbit Constellations

*Frederick Rawlins, Richard Baker, Ivan Martinovic*

CLExtract: Recovering Highly Corrupted DVB/GSE Satellite Stream with Contrastive Learning

*Minghao Lin, Minghao Cheng, Dongsheng Luo, Yueqi Chen*

Firefly: Spoofing Earth Observation Satellite Data through Radio Overshadowing

*Edd Salkield, Sebastian Köhler, Simon Birnbach, Richard Baker, Martin Strohmeier, Ivan Martinovic*

Towards Protecting Billions and Billions of Bits on the Interplanetary Internet

*Stephen Herwig*

### **Space Segment Security**

A Case Study on Fuzzing Satellite Firmware

*Tobias Scharnowski, Felix Buchmann, Simon Wörner, Thorsten Holz*

The Vulnerabilities Less Exploited: Cyberattacks on End-of-Life Satellites

*Frank Lee, Gregory Falco*

### **Test Beds**

Towards a Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, Drone (SAAMD) technologies and communications

*Andrei Costin, Hannu Turtiainen, Syed Khandkher, Timo Hämäläinen*

QPEP in the Real World: A Testbed for Secure Satellite Communication Performance

*Julian Huwyler, James Pavur, Giorgio Tresoldi, Martin Strohmeier*

## **Message from the Program Co-Chairs**

Greetings from the First Workshop on the Security of Space and Satellite Systems (SpaceSec23)!

This year marks the inauguration of our workshop on Earth. We are excited to be the first workshop to cover this topic in the security community, and to discuss the challenges and opportunities in securing the fast-growing space and satellite ecosystem. With the increasing reliance on space-based technology for communication, navigation, and observation, it is imperative that we improve the security of these systems against potential impacts from terrestrial and space-born threats.

With 19 submissions and 10 accepted papers, our first edition of SpaceSec was an interstellar success. Not only did we have over 60 attendees join us in person, but we also had over 15 virtual attendees who tuned in from all corners of the galaxy Earth! We want to thank all participants for their contribution in exciting discussions after each of the talks and even after the workshop. Especially for emerging research fields such as ours, discussions and new collaborations are vital to kickstart new research, which we think our workshop achieved in many ways.

In particular, we want to thank our outstanding keynote speaker, James Pavur, for his excellent insights on the open challenges and opportunities for new researchers in the field. He provided an excellent overview of the field – not only for newcomers. We are sure that people took notes, and we are already thrilled to see next year's papers investigating some of these directions.

Finally, we thank our outstanding technical program committee listed below for their work. After receiving far more submissions than we could have hoped for, the burden was on our reviewers to provide at least three reviews per paper.

As co-chairs, we are honored to have led this first interstellar workshop on the security of space and satellite systems. We are now looking towards the future and planning the next steps of our mission to explore the security of the final frontier.

**Martin Strohmeier and Johannes Willbold**  
**Program Committee Co-Chairs, SpaceSec 2023**

## **Program Committee Co-Chairs**

Martin Strohmeier, *Cyber-Defence Campus, armasuisse W+T (Switzerland)*  
Johannes Willbold, *Ruhr University Bochum (Germany)*

## **Program Committee**

Aanjhan Ranganathan, *Northeastern University (US)*  
Ali Abbasi, *CISPA (Germany)*  
Brandon Bailey, *Aerospace Corp (US)*  
Christina Pöpper, *NYU Abu Dhabi (UAE)*  
Gregory Falco, *Johns Hopkins University (US)*  
Harshad Sathaye, *Northeastern University (US)*  
Ivan Martinovic, *University of Oxford (UK)*  
James Pavur, *Defense Digital Service, Department of Defense (US)*  
Knut Eckstein, *European Space Agency (Europe)*  
Thorsten Holz, *CISPA (Germany)*  
Verena Zimmermann, *ETH Zurich (Switzerland)*  
Vincent Lenders, *Cyber-Defence Campus, armasuisse W+T (Switzerland)*