International Cyber Security Center of Excellence INCS-CoE

SECURITY CHALLENGES FOR SPACE SYSTEMS

Image created by ChatGPT

On Wednesday, December 11, 2024, INCS-CoE held an on-line seminar on security challenges for space systems. Three speakers presented their ongoing research: Ali Abbasi (CISPA Helmholtz Center for Information Security, Germany), Ioana Boureanu (University of Surrey, UK) and James Pavur (State Department, US) – see biographies at the end of this note. These talks focussed mainly on satellite technology and the challenges that arise for systems operating in such challenging environments.

Ali Abbasi spoke about the proliferation of actors in the construction and operation of Low Earth Orbit (LEO) satellites. He spoke about technical challenges, regulatory and industry issues and some design challenges. As satellites revolutionize global communication and Earth observation, their rapid growth has outpaced efforts to secure them. He discussed the evolving cybersecurity landscape of satellite systems, examining vulnerabilities from legacy design flaws to sophisticated attack vectors. He analyzed the architecture of LEO satellite subsystems, using case studies and demonstrations to reveal how weaknesses in components like COM and CDHS can be exploited. Beyond technical challenges, he discussed the broader issues of insufficient security standards, limited access to satellite systems for researchers, and fragmented regulatory efforts.

Ioana Boureanu presented some aspects of the formal verification of a protocol used in message authentication in Global Navigation Satellite Systems (GNSS), notably the European Galileo system. A recent version of the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol was adopted as part of the Open Service Navigation Message Authentication (OSNMA) inside the Galileo system , the European Global Satellite Navigation System (GNSS) Service, in 2024, but this has not been formally verified with computer-aided tools beforehand. She reported on work to formally verify these versions of the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol, using symbolic/Dolev-Yao verification tools (the Tamarin prover) — looking to understand what the challenges and solutions are.

James Pavur presented several avenues for academic and applied security research in space that go beyond traditional communications topics. By viewing space missions holistically, he identified promising sub-fields in the space security domain that have received relatively little research attention, such as space domain awareness and launch operations. He hoped to inspire those interested in security research to consider new avenues for the cyber defense of space missions.

The talks covered important topics ranging from the ground systems, through communications between ground and space-based platforms, the platforms themselves and policy and operations. Some of the key research challenges which emerged during the seminar Included:

1. To what extent are traditional security approaches applicable to space systems which have to hardened to operate in the harsh space environment? It is known that deployed systems often suffer from basic security vulnerabilities such as lack of memory safety, weak encryption and authentication and operating system vulnerabilities.

2. As the sector evolves and both ground stations and platforms are offered as a service, how can properties of systems owned by others be verified?

3. Are "secure-by-design" approaches applicable to space systems? -- what are the appropriate design methodologies to ensure that systems are as secure as possible.

4. What are the appropriate standards and enforcement mechanism for these systems? It is important that such standards and regulations should provide security without stifling innovation.

5. Space systems share some features with Internet of Things and Industrial Control Systems; what can be learnt from the experience of protecting these systems?

6. Formal methods have proved their worth in the verification of components such as message authentication protocols (eg TESLA); can formal methods be used more broadly in verifying security properties of the various components in space systems?

More information about the individual presentations and the resulting research questions may be found on the INCS-CoE website (incs-coe.org) or by contacting the speakers. We encourage the community to start conversations which might lead to the solutions of some of these challenges.

Aanjhan Ranganathan will be chairing Space Sec 2025 (co-located with a top tier security conference NDSS in San Diego) in February 2025. More details: https://spacesec.info

Speakers

Dr Ali Abbasi, CISPA Helmholtz Center for Information Security, Germany

Ali Abbasi is a faculty at CISPA Helmholtz Center for Information Security, Saarbrücken, Germany. His research interests include embedded systems security, security of mission-critical real-time systems, and secure space and automotive systems. He leads the Embedded Security group at CISPA, which develops and implements new methods to protect embedded systems against various classes of attacks on both the hardware and firmware.

Prof Ioana Boureanu, University of Surrey, Centre for Cyber Security, UK

Ioana Boureanu is Professor of Secure Systems at University of Surrey and Director of Surrey Centre for Cyber Security. Her research focuses on (automatic) analysis of security using mainly logic-based formalisms, as well as on provable security and applied cryptography. Before joining Surrey, she worked as a researcher and professor in Switzerland, as well as a cryptography consultant in industry.

James Pavur, United States Department of State's Office

James Pavur is a Senior Advisor and Presidential Innovation Fellow at the United States Department of State's Office of the Special Envoy for Critical and Emerging Technology. In this role, he focuses on the technical dimensions of AI technologies and their relationship to foreign affairs. Previous roles include leading an infrastructure and security team at a digital engineering startup and working for the Pentagon's Defense Digital Service and Chief Digital and Artificial Intelligence Office. He holds a DPhil from Oxford University's Department of Computer Science, courtesy of a Rhodes Scholarship, where his research focused on space systems security. He also holds a Bachelor of Science in Foreign Service from Georgetown University's Walsh School of Foreign Service. Beyond academia, James has delivered multiple briefings at the DEFCON and Blackhat hacking conferences and his research has been covered by several popular press outlets.