nccgroup

Jun 03, 2020 14:10 BST

Securing the next frontier in space technology in collaboration with the University of Surrey

In a review of over 70 past satellite security incidents, experts at the University of Surrey and NCC Group have revealed significant cyber security risks to future satellite control and communication systems.

This analysis of emerging and enabling technologies outlines challenges and research objectives for the future of space technology. This includes the need for standardised security processes from the outset of a mission, reliable and up-to-date software, tamper-resistant hardware-based protection measures, and more robust security protocols for satellite positioning and intersatellite

communications.

The upcoming era of ‘new space’ is characterised by key advancements in the satellite industry, driven by private companies as opposed to nation states. This includes the deployment of commercial-off-the-shelf components, faster development cycles enabled by key technologies such as software-defined radios, innovative services and applications involving mega-constellations of smaller low-cost satellites.

The team found that a lack of proper security analysis of deployed systems and protocols, coupled with the prevailing ‘security-by-obscurity’ mentality, represents a major threat and an obstacle to the secure and safe operation of future satellite constellations.

While the ground station seems one of the easiest attack targets, the research highlights that direct attacks on satellites is also a real risk. Therefore, there is a need to balance mission functionality, such as providing low-latency broadband, with the security of satellite technology.

Dr Mark Manulis, co-author of the paper and Deputy-Director of the Surrey Centre for Cyber Security, said: “We are entering an incredibly exciting era of satellite technology that could bring fast broadband to very remote areas of the world, improve sustainability with new data collected from Earth observation, and enable intelligent transportation and autonomous driving in future smart cities. However, it is important to make sure that satellites launched today will remain secure and resistant to cyber-attacks as their vulnerabilities may cause chaos in space and harm humans on earth”.

Andy Davis, co-author of the paper and Transport Assurance Practice Director at NCC Group, said: “The satellite industry has, in recent years, started to implement more and more creative uses for space-based assets. It is extremely important that as more connectivity and complexity is added, the satellite industry keeps resilience front of mind and puts in place secure manufacturing and design processes throughout the development lifecycle.”

To find out more and read the full paper, head over to our research blog.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970