WORKSHOP REPORT: Space Security Scoping

February 2019

Authors: Marie Farrell, Matthew Bradbury, Michael Fisher and Carsten Maple

Institution: University of Liverpool/University of Warwick

Date: 1.2.19

Funded by: FAIR-SPACE Hub

Governmental Funding Bodies:

INDUSTRIAL STRATEGY | UK Research and Innovation

UK SPACE AGENCY

University Partners:

UNIVERSITY OF SURREY

Imperial College London

THE UNIVERSITY OF EDINBURGH

UNIVERSITY OF LIVERPOOL

University of Salford MANCHESTER

WARWICK THE UNIVERSITY OF WARWICK

FAIR-SPACE

fairspacehub.org

Contents

1 Background

Overview

The Space Security Scoping Workshop was jointly organised by the Universities of Liverpool (Marie Farrell and Michael Fisher) and Warwick (Matthew Bradbury and Carsten Maple). It was held on the 1st of February 2019 at the University of Liverpool Campus in London. There were 58 registrants but, due to adverse weather conditions, 29 attendees. The attendees were from a mix of academia and industry, including the UK Space Agency, Roke, RHEA Group, Space Platform Technologies, Softcat, Northern Space and Security, National Physical Laboratory, ESA Business Apps/STFC, Satellite Applications Catapult, Department of International Trade and the Universities of Liverpool, Warwick, Surrey, York, Northumbria, Leicester and Ss Cyril & Methodius University, Skopje.

Aim

The aim of the workshop was to discuss the cyber security issues related to robotic systems deployed in space in order to scope out research priorities and to develop collaborative R&D programmes on the topic of cyber security between FAIR-SPACE and industrial partners. To this end, the workshop began with an introduction to the FAIR-SPACE Hub by Michael Fisher. Following this, Carsten Maple spoke about cyber security in general and Michael Fisher presented on the topic of verification and validation (summarised in Section 2 below). Then, Matthew Bradbury and Marie Farrell led a discussion session that was guided by five questions about the cyber security issues faced when deploying robotic systems into space (summarised in Section 3).

Epilogue

A number of the industrial attendees expressed interest in joining the FAIR-SPACE Hub and they have been put in touch with the appropriate people. After the workshop, the slides were shared with the attendees and those registrants who sent their apologies via Dropbox.

2. Summary of Talks

2.1 Introduction to Cyber Security

This presentation provided a general and accessible introduction to cyber security with an emphasis on space applications. Notably, cyber security differs from information security because hardware is involved. It outlined a number of attacks that have been directed against space systems, such as jamming of satellites, and discussed how easy it can be to hack satellites using the Iridium attack as evidence[1]. Other attacks included a group of Texas students spoofing the GPS of a superyacht[2] and a report that Chinese hackers took control of a NASA satellite for eleven minutes[3].

From the perspective of cyber security, the UK Space Agency is concerned that an attacker could influence an operator's ability to control their spacecraft and so compromise both the operator's IP and their ability to provide a service. From this, it is important to assess the range of impacts that an attack may have and whether the type of mission, engineering infrastructure, or concept of operations affect this.

As a result, it is vital to analyse risk. To achieve this analysis a number of aspects must be considered, including the ground and space cyber security controls and mitigations used, the level of penetration testing performed, the frequency and scope of IT health checks, the cyber security expertise of the staff in the organisation, etc. Some of the challenges to providing secure systems are the use of phishing attacks, insider attacks, supply chains, use of Commercial Off-The-Shelf (COTS) technologies, use of Software Defined Radio (SDR), the complexity of space missions, and the ubiquity of legacy systems. In particular, satellite missions tend to last a few (3-5) years but the satellite often takes up to 25 years to de-orbit.

In the classical risk model, risk is considered as the likelihood that a threat actor will exploit a vulnerability to have an adverse impact on an asset. Threat modelling is an approach that is used to identify the various threats to a product or service from a security perspective with a view to identifying and understanding where the greatest risk may be, providing for targeted mitigation. The likelihood that a threat actor will exploit a vulnerability depends on a number of factors. The threat actor must be motivated to conduct an attack, require the skills or resources to conduct an attack and must have the opportunity to exploit a vulnerability. The likelihood of a vulnerability being exploited by a threat actor also depends upon the difficulty for the vulnerability to be exploited.

Threat actors could be state-sponsored, from Hacktivists, insiders (including supply network), or mischief-makers, or could even be directly from organised crime. To assess the likelihood of an attack we must consider how motivated the threat actors are and what reward they (believe they) will realise. If the reward is particularly high then the motivation, and so risk, must be higher. Potential motivations include crime (e.g. financial gain), espionage (state and

[1] https://motherboard.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite

[2] https://www.theregister.co.uk/2013/07/29/texas_students_hijack_superyacht_with_gpsspoofing_luggage

[3] https://www.geek.com/geek-pick/chinese-hackers-took-control-of-nasa-satellite-for-11-minutes-1442605

industrial), (h)activism, terrorism and warfare. The difficulty in executing an attack depends on the difference between skills required to exploit a vulnerability and the skill level of the attacker in realising the opportunity.

2.2 Introduction to Verification and Validation

This presentation outlined the basic approaches to verification and validation of software systems. In particular, formal verification is the act of proving (or disproving) the correctness of a system with respect to a certain formal specification or property. In order to correctly develop a software system, the developer must first capture the requirements of the system as a specification of what the system should do. This specification can be implemented and, once implemented, the code can then be verified to check if it corresponds to the specification. Approaches to verification include formal verification, simulation-based testing and physical testing. When the system is complete it undergoes a validation phase including physical testing, user validation and test scenarios. In a nutshell, verification assesses whether or not the system has been built correctly, whereas, validation assesses whether the correct system has been built. Of course, both validation and verification are meaningless if the requirements of the system have not been captured.

Requirements can be devised from a number of different perspectives such as safety, preferences, ethics, regulations and security. These informal requirements can then be formalised using a variety of logics. It is often the case that complex systems are to be certified before their use is permitted, particularly in the safety-critical domain. Certification amounts to the determination by an independent body that checks whether the systems are compliant with particular regulations. The certification process is a legal, rather than scientific, assessment and usually involves external review, typically by some Regulator. In general, these regulators appeal to Standards that have been developed and provide guidance on the proving of compliance. There are many standards for robotic systems, however, most ignore the issue of autonomy which is becoming more prevalent.

Software systems have many possible executions/runs and it is difficult to decide what kind of verification is most suitable/required. Testing selects a subset of these runs and assesses them against the requirements. In contrast, formal verification assesses *all* runs of the system, but can only work feasibly for relatively small components. Simulation-based testing can handle much broader systems but relies heavily on what requirements are assessed, the subset of behaviours tested and environmental assumptions. With respect to verifying security properties, testing involves modelling the threats and assessing these over a subset of runs. Formal verification involves modelling the threats and proving the system will avoid these in all runs. With formal verification, it is also possible to decipher what combination of communications and actions can lead to security breaches.

3 Space Security: The Key Issues

Matthew Bradbury and Marie Farrell posed 5 questions to the attendees and we have summarised the responses and discussion that followed each of these questions below (full notes are contained in the Appendix).

Q1: What are the security issues in space?

One particular issue in space concerns the decommissioning of satellites. In general, satellites ''burn up'' after 5 years and are either replaced by something else, often a more up to date version, or they have completed their mission and now become defunct. In either case, they are turned off and normally de-orbit after a period of time (the guideline is ~25 years). There is a concern that these `dormant' satellites could potentially be hijacked and `revived' by attackers without the owners' knowledge or control. Furthermore, the use of legacy software is hugely problematic from a security perspective. Currently, if there is a problem with the running version of a piece of software, then the default is to revert back to a previous version which will still have all of the old bugs/vulnerabilities present.

Q2: Are they different to the issues in autonomous ground/air vehicles?

There is certainly some overlap between the cyber security issues encountered in autonomous ground/air vehicles and those deployed in space. However, it is generally more difficult to identify/classify objects (and so, attackers) in space. Although, the US government provides a record of the objects that it `knows' about, this record is incomplete as only objects that are above a certain size and that can be traced back to a specific launch are reported. This is further complicated by the fact that space traffic management guidelines are often quite vague so it is difficult to track objects in space. Satellites are becoming cheaper to manufacture/buy and this, coupled with the lack of strict regulations, means that malicious or insecure devices are easily launched into space.

Q3: What will be the problems in the future?

Currently, robotic systems in space are remotely monitored and controlled from a ground station. As new technology becomes available, it is likely that these robotic systems will behave much more autonomously and also communicate with one another (e.g. constellations/swarms of autonomous, communicating satellites). Attacked communications between autonomous satellites could cause collisions or disruption of swarm behaviour. N.B: This is where our work on Cooperative Awareness Messages (CAM) security threat verification could offer some benefits since the way that these satellites will communicate has not yet been formalised (see Section 5).

Currently, satellites typically transmit all collected data to a ground station where is can be analysed and interpreted. New technology facilitating on-board data analysis will be very useful and save time, however, transmitting the result back to the ground station may also be vulnerable to hacking.

Q4: What are current ways of detecting/stopping attacks in these systems?

At ground level, there are ways to shield from, detect, and jam the attacker. Unlike some sectors (e.g. nuclear industry), companies are reluctant to share information when things go wrong. Sector needs to develop ways of privately sharing this data in a timely fashion.

Q5: How do environmental considerations impact on security?
(Environmental conditions here include radiation, communication delay, movement, etc.)

Space weather events and radiation can cause ''bit flips'' that need to be detected and corrected. In particular, it is important to be able to distinguish between changes caused by these (innocent) environmental issues and those caused by attacks on the system. During the workshop, there was a discussion on how to distinguish malicious ''jamming'' from naturally occurring weather events though no clear conclusion was reached.

4 Summary of Discussion

Historically, the space industry has been risk averse. However, this has changed in recent years, becoming more entrepreneurial with a greater acceptance of risk for more financial gain. As a result, the regulations and standards for space are lacking and often ignored. In particular, rules enforced by the European Space Agency (ESA) when launching satellites can be, and often are, disregarded by other organisations, and so those that do not meet the ESA's requirements may still be launched. As outlined in Carsten Maple's talk, trying to understand the motivations of the attacker is important when assessing risk and analysing threats to these systems. Part of the discussion highlighted that the main purpose/target of an attack may well be an ''on-the ground business'' (e.g. disruption/hijacking of broadcasts) or a particular target (e.g. autonomous ship/navigation system/etc.) and this will most likely be for financial gain or intelligence gathering. There was also mention of a green book entitled ''Security Threats against Space Missions''[1] that may be useful for the work that we are undertaking as part of the FAIR-SPACE Hub. Finally, one thing that is consistently missing from documentation about space operations is a consideration of the roles that people play and their motivations in space operations and cyber security.

5 Future Directions/Next Steps

Future work will build on our work on using threat analysis techniques to guide the formal verification of the sending and receiving of Cooperative Awareness Messages (CAM) between autonomous vehicles [2]. To this end, we intend to devise a methodology for security-informed verification. We also aim to examine the potential ''denial of service'' attacks on autonomous space systems, together with mechanisms for detecting and avoiding these.

A second workshop will be organised which will examine the cyber security threats and their verification for the FAIR-SPACE use cases that have been distributed by the Hub.

References

[1] CCSDS. SECURITY THREATS AGAINST SPACE MISSIONS, 2015. URL:https://public.ccsds.org/Pubs/350x1g2.pdf Green Book 350.1-G-2.

[2] Marie Farrell, Matthew Bradbury, Michael Fisher, Louise A. Dennis, Clare Dixon, Hu Yuan and Carsten Maple. Using Threat Analysis Techniques to Guide Formal Verification: A Case Study of Cooperative Awareness Messages. Under review, 2019.

Acknowledgements:

The authors would like to thank Clare Dixon, Matt Luckcuck, Alexei Lisitsa and Rafael Cardoso for sharing their notes with us.

Appendix: Notes

Q1: What are the security issues in space?

- Use of legacy code/systems: if there is a problem with the current, running, version of a piece of software being used then the default is to revert back to a previous version which will still have all of the old bugs/vulnerabilities present.
- Use of ransomware to jam satellite signals.
- Compromised ground control (insider threat, phishing, etc.).
- Evolution of both known attacks and new attacks with the development of new technology. For example, Software Defined Radios (SDRs) rapidly decreasing cost has lowered the barrier of entry to interacting with satellites. There needs to be the capability to handle similar technological revolutions due to the long lifetime of space missions.
- Delayed communications in space although this depends on where - Mars has a much larger delay than the moon.
- Decommissioning of satellites: in general, satellites ''burn up'' after 5 years and are replaced by something else. Once turned off, they de-orbit after a period of time. These sleeping satellites could potentially be hijacked and turned back on by attackers without the owners' knowledge.
- Financial motivations for attacks.
- There is an overarching lack of understanding of operations in space throughout the community. For example, incomplete understanding of the environment, weather, etc. There is also no formal or well understood description of how remote operations are handled. Autonomous operations present even more challenges.
- There is a focus on security issues of devices in Earth orbit and the devices that depend on these satellites. Whereas there is (currently) less interest in the security of devices on moons or planets.

Q2: Are they different to the security issues for autonomous ground/air vehicles?

- There are quite a few similarities but the differences are mainly due to the environment in space. For example, range and pace of movement is more restricted in space due to lack of knowledge about the environment. A hugely limiting factor is the fact that all space maneuvers (including collision avoidance) are currently controlled from the ground station - there is no autonomy in the satellites/rovers themselves. From this perspective, attacking the ground station potentially renders the satellite inaccessible although it may still be sending information to the ground.
- It is vastly more difficult to track spacecraft than it is to track autonomous cars - partly due to latency in communications

- It is difficult to identify/classify objects in space. Although, the US government provides a record of the objects that it knows about, this record is incomplete because only objects above a certain size are reported and objects are selectively omitted. Also, the objects that are reported are only those that can be traced back to a launch. In particular, space traffic management guidelines are vague.

- The main issue is that there are no international rules or standards governing what can or cannot be put up there. In fact, the international community is reluctant to sign up to standards because they don't want to be their capabilities to be limited in any way

.

- Satellites are becoming cheaper to manufacture/buy and this, coupled with the lack of regulations, means that malicious or insecure devices are easily launched into space.

Q3: What will be the problems in the future?

- Attacked communications between autonomous satellites could cause collision or disruption of swarm behaviour. This is where our work on CAM security threat verification could offer some benefits.
- Malicious debris and malicious/compromised space cleaners or IoT devices that are too small to be detected.
- New technology facilitating on-board data analysis and transmission vulnerable to hacking.
- Ecoterrorism/competing companies taking control of robots/rovers.
- Cheap off-the-shelf (COTS) devices may play an important role in the future development of new cheap satellites. How can correctness, reliability, safety and security be ensured? Regulations currently prohibit access to their proprietary code.

Q4: What are the current ways of detecting and stopping attacks in these systems?

- Need ways of improving situational awareness in both spacecraft and remote human operators.
- At ground level, there are ways to shield from, detect and jam the jammer.

Unlike in the nuclear industry, companies are reluctant to share information when things go wrong. Need to develop ways of privately sharing this data in a timely fashion.

- Open source events shared amongst nations.

Q5: How do environmental considerations (e.g., radiation, communication delay, movement) impact on security?

- Space weather events and radiation cause bit flips that need to be detected and corrected. In particular, it is important to be able to distinguish between innocent environmental causes and attacks.
- One thing that is consistently missing from documentation about space operations is a consideration of the roles that people play in space operations and cybersecurity.

FAIR-SPACE

E fairspacehub@surrey.ac.uk

W fairspacehub.org

twitter.com/fair_space_hub

linkedin.com/company/fairspacehub

facebook.com/fairspacehub