IAC-21-D5.4.1

INCREASING SECURITY IN SATELLITE NETWORKS

Klaus Schilling
University Würzburg, Germany, schi@informatik.uni-wuerzburg.de

Alexandra Dmitrienko
University Würzburg, Germany, alexandra.dmitrienko@uni-wuerzburg.de

Multi-satellite systems have a growing influence on crucial terrestrial infrastructures, for example in communication networks or in navigation support. Similar to many on-Earth systems (like the Internet), the satellite technologies were initially developed with functional requirements as a primary concern, while security objectives received second priority. Today's satellite systems do not employ elaborate security mechanisms at the same level as on-Earth networks and systems. Deployment of security mechanisms requires additional resources, which often deems too costly and unjustified, as long as in-space cyber-threats are absent. The situation, however, is about to change. We have to face the perspective to deal with skilled adversaries, while often even simple security practices such as encrypted and integrity-protected communication and software patching are not applied. In this contribution, we aim to transfer and adapt terrestrial countermeasures to cyber-attacks in-space towards securing satellite systems further. This paper performs an analysis of potential threats and formulates security requirements for satellite systems. A balanced trade-off between required resources for security and achieved benefits will be addressed. Notably, in-space security threats are different from those relevant for on-Earth systems, as, for instance, an adversary is likely to attack communication links, but is unlikely to have physical access to satellite hardware. On another hand, software attacks, such as exploitation of software vulnerabilities, as satellites run the software and this software may have similar vulnerabilities as on-earth systems. To identify relevant threats, we define various adversarial models targeting common commercial satellite applications, analyze potential attack vectors, formulate security objectives and requirements, and make recommendations on how to address them.

Keywords: security, cyber-attacks, network attacks, endpoint attacks

I. INTRODUCTION

With the growing capabilities of satellite networks, their contribution to crucial infrastructures on the ground increases, too. Today's Global Navigation Satellite Systems (such as GPS, Galileo, Glonass, or Beidou) are the basis for a broad spectrum of navigation applications. As there are alternative sources this localization information is considered in increasing terrestrial critical infrastructures, like in airplane or ship navigation. Nevertheless, these data can be significantly manipulated by signal jamming and spoofing. Thus to realize the inherent economic potential it will be essential to have related countermeasures at hand.

The mega-constellations by thousands of satellites, currently implemented for global communication networks, will offer on one side fascinating new opportunities for continuous connectivity everywhere, but will also need mechanisms to prevent misuse of illegally acquired data.

The Consultative Committee for Space Data Systems (CCSDS), an interagency working group recommending standards for spacecraft data handling and control, identified the importance of related security threats and provided recommendations in [1]. In particular, the tendency for

- increased use of commercial standards and components in space and ground systems
- increased complexity based on on-board software

leads to higher vulnerability of the spacecraft. This contribution addresses the transfer of successful protection techniques in terrestrial data systems to the space environment.

II. SPECIFIC SATELLITE SECURITY REQUIREMENTS

The satellites in-orbit is dependent on communication links between space segment and ground stations in both directions. If the uplink, e.g., the telecommand link, is attacked, the satellite will run out of control and will not deliver the planned services. If the downlink is disturbed, the data sent from the satellite will not be received by ground stations. Thus the ***availability*** of the satellite will be affected. Also, a physical attack on satellites will fall into this problem class.

In case the data sent in the link between satellite and ground station are copied in an unauthorized way, the ***confidentiality*** is violated.
If transmitted data will be modified in an illegal way, the ***integrity*** of information in the system is affected.
Ways to increase security is ***access control*** to space and ground segment for restricted personnel with limited individual access rights, as well as authentication that the information source is verified.
Security requirements vary significantly in different space missions with respect to the protection of telemetry and telecommand data, as well as information in the ground data system. When considering the generic satellite operation setup depicted in Fig. 1, the attack vectors imposed by an adversary can be split into (i) network-level attacks, or (ii) attacks targeting end-points.

Network-level attacks. Network-level attacks target communication between communicating entities, e.g., inter-satellite communication, or command and control communication. They can be categorized into passive and active attacks. In passive attacks, the adversary is limited to passive eavesdropping, where the transmitted signals/packets are intercepted and interpreted. Eavesdropping can result in illegal copying of transmitted data and undermines the confidentiality requirement.

Active attacks are more advanced and are characterized by the ability of an adversary to perform active actions, e.g., to drop or jam, inject, alter or replay previously recorded packets and/or signals.
- Drop, or Denial-of-Service (DoS) attacks: The attacks that allow an adversary to achieve information loss result in interruption of service and undermine the availability requirement of the system. Examples of such attacks in satellite systems are jamming [2] and flooding with an excessive amount of packets to cause network congestion [3].
- Injection, or Spoofing: Spoofing attacks result in the injection of illegal messages into communication. For instance, GPS spoofing attacks were reported against 20 US ships in the Black Sea [4]. Notably, spoofing signals from GPS satellites were are far more dangerous than jamming as it appears that the GPS is working as intended [5]. This attack vector undermines the authenticity requirement.

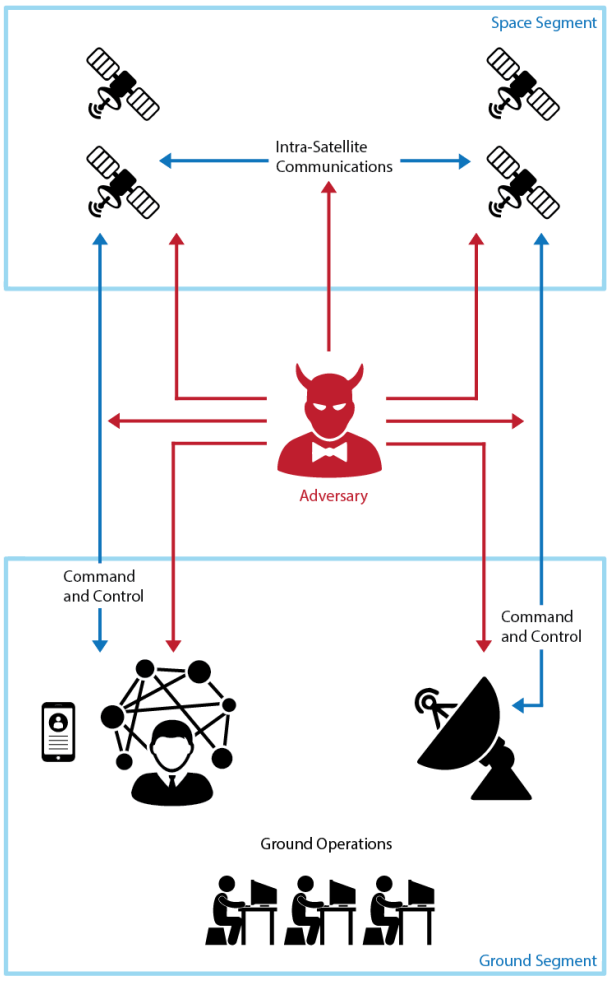

Fig.1: Survey of different points of attack in typical satellite operations setups

- Alternation attacks result in illegal modification of transmitted data and undermine the integrity requirement of the system. To conduct such an attack successfully, an adversary needs to be able to (i) suppress the original signal, and (ii) inject the new spoofed version.
- Replay attacks involve a combination of passive eavesdropping and active injection. Here, an adversary records communication and replays it at a later point in time. Such attacks undermine the freshness requirement.

The above discussed passive and active network-level attacks can be used as building blocks to achieve more high-level attack goals:
- Impersonation of end-points: An adversary performs its actions using the identity of another entity in order to, e.g., get unauthorized access to the system (undermines authenticity) or impose harm without being hold accountable for it (undermines accountability).

- Deanonymization: This attack vector is relevant for systems that provide anonymous communication. Here, an adversary aims to deanonymize communicating end-points. This attack vector undermines the anonymity requirement and, to date, seems to be less relevant for satellite networks. In the future, however, it may become important, if, e.g., sat phones will provide anonymous communication channels to their users.

Endpoint attacks target the endpoints of communication, such as satellite vehicles or ground stations.

- ground stations
  - if ground stations are remotely accessible over the Internet, they can be subjected to the same attack vectors as any other terrestrial system.
- satellites:
  - Denial-of-Service (DoS) attacks: Examples are kinetic-physical and non-kinetic physical attacks [6]. Kinetic-physical attacks attempt to strike directly or detonate in the proximity of a satellite or a ground station. Aim to cause irreversible damage. Non-kinetic physical attacks aim to induce physical effects without direct physical contact. For instance, High-Powered microwave emission can interfere with satellite electronics and cause temporal or permanent damage.
  - Remote software-based attacks: In this attack vector, an adversary aims to infect the target through the exploitation of software vulnerabilities. This attack vector becomes more relevant for satellite vehicles, as the use of commercial off-the-shelf software becomes more widespread [5].
  - Physical capturing: In physical capture attacks, an adversary aims to gain control over the target by gaining physical access and tampering with the target. For instance, an adversary can eavesdrop on communication busses, read out cryptographic material and other secrets from the memory, inject backdoors, overwrite the control logic with a malicious version, roll back software version to older/vulnerable ones, brick the target, etc. While, in general, this is a very powerful attack vector that undermines many security requirements at once (e.g., confidentiality, integrity, freshness, authenticity, availability), its scope is limited in the context of satellite vehicles since it is unlikely for an adversary to gain physical access to the satellite in its operational phase. Yet, such attacks in the pre-launch phase are possible and could be used to, e.g., make the satellite unfunctional or even take full control over it.
  - Cloning attacks: In this attack scenario, an adversary creates an exact copy (or copies) of the target, normally in order to be able to impersonate it. If the target deploys any cryptographic protection methods, this would require an adversary to disclose the confidentiality of cryptographic secrets stored on a target. In case the adversary can clone many copies, one can launch a so-called Sybil attack, where many entities pretend to have the same identity. This attack vector is normally relevant in the context of voting schemes and, to date, does not seem to be important for satellites.

III. TERRESTRIAL DATA SECURITY APPROACHES WITH TRANSFER POTENTIAL

To address the wide spectrum of possible attacks on satellite systems and to fulfill the security requirements, it is necessary to deploy a holistic approach to cybersecurity. In past years, a lot of knowledge was collected on how to secure terrestrial systems in a holistic way, and a plausible approach would be to transfer this knowledge to the satellite operation systems.

The holistic approach by NIST. NIST Cybersecurity Framework [7] developed by the National Institute of Standards and Technology formulates core concepts of cybersecurity. It was developed as a holistic approach to cybersecurity regardless of the application domain and can fulfill the needs of various industries. Another NIST document [8] leverages the generic NIST Cybersecurity Framework [8] and applies it in the context of commercial satellite operations. Using an example, this document demonstrates how to apply the Cybersecurity Framework for a notional low Earth orbit (LEO) “small satellite vehicle”, a small part of a larger Space Operations. It helps to identify assets that need protection and specify impact in case of cybersecurity events. For instance, it is identified that intentional jamming of sensor data may result in the “loss of data assets for customers”, while malicious code injection results in “loss of satellite vehicle, data corruption, and data loss” [7]. It also formulates a list of recommended actions that can help to achieve the protection of assets. For instance, it is postulated that data in transit and at rest need to be protected, and that “access permissions and authorizations need to be managed, incorporating the principles of least privilege and separation of duties”.

Adversary models. Similar to terrestrial systems, in satellite operation setups it is likely unreasonable or impractical to address all possible attack vectors. Certainly, implementing security measures impose additional costs, and the system is likely to have a limited budget for the implementation of countermeasures. Especially for commercial applications, it might not be economical to consider the full spectrum of attack vectors. Hence, it is reasonable in practice to balance the

security risks and the associated costs for their elimination.

The approach for finding an optimal balance is to prioritize the list of actions that need to be taken in order to prevent specific attack vectors along with the identification of their costs. As a result, it becomes possible to create a target security profile that defines the properties of the system with respect to its resilience to cyberattacks. The resulting profile defines the capabilities of the system to defend against various attack vectors. Based on such a profile, it becomes possible to establish a so-called adversarial model -- a model which defines adversarial capabilities. Following this approach, one can prove the security of the system in a given adversary model, even though the system might still be vulnerable to attack vectors that are impossible or too costly to defend against.

Dealing with the network-level attacks. The state-of-the-art approach to deal with both, passive and active network-level attack vectors is to apply cryptographic algorithms, such as encryption [9] and message authentication [10]. They rely on cryptographic secrets, or keys -- small pieces of secret information that, need to be either kept private, if Public Key Cryptosystem (PKC) is used, or, in the case of Secret Key Cryptosystems (SKC), securely shared between communicating parties. Innovative approaches regarding secure communication on basis of quantum technologies are investigated [11], [12], [13], which could be well-suitable for the distribution of key material. Generated quantum keys will be distributed by entangled photons. Here fibre glas connections will only allow key distribution over distances of several hundred meters. For quantum key distribution at intercontinental distances satellites seem to be the only way to transfer quantum keys generated on-board the satellite to distant communication partners via optical links [14].

To address the problem of impersonation of end-points, a large body of authentication protocols was developed in terrestrial systems. Most of them, however, rely on computationally expensive PKC and require the deployment of Public Key Infrastructure (PKI), which is sub-optimal for resource-constraint satellite vehicles. Hence, authentication schemes that were adopted in the context of satellite systems leverage more efficient SKC [15] or even entirely rely on efficient one-way functions [16]. Some protocols also aim to address the anonymity of users in mobile satellite communication systems [17].

Dealing with end-point attacks. Dealing with end-point attacks in the context of satellite systems is challenging due to associated costs, such as computational and management overhead. For instance, the problem of software vulnerabilities is traditionally dealt with by tracking vulnerability information and managing software patches, which implies the need for support of software update methods. Such methods impose additional (storage) overhead and also open new and powerful attack vectors. Preventive methods include address space layout randomization (at different levels of granularity) and various solutions (e.g., [18,19] that leverage the concept of Control-Flow Integrity (CFI) [20]. The former is not bullet-proof against certain attack methods, while CFI introduces non-trivial overhead which is prohibitive in the context of satellite systems.

IV. CONCLUSIONS

There is an immediate need in space to increase the reliability and safety of data transfer. Already existing economic potential in terrestrial Internet-related solution approaches inspire transfer to the space environment and offer significant application potential. Quantum key distribution via satellite offers new approaches for secure communication.

REFERENCES

[1] CCSDS. The Application of Security to CCSDS Protocols, Green Book March 2019, https://public.ccsds.org/Pubs/350x0g3.pdf

[2] H. Rausch. Jamming commercial satellite communications during wartime an empirical study. In IEEE International Workshop on Information Assurance, pages 8–118, 2006

[3] Giacomo Giuliari, Tommaso Ciussani, Adrian Perrig, and Ankit Singla, ICARUS: Attacking low Earth orbit satellite networks, Annual Technical Conference (USENIX ATC), 2021

[4] 2017-005A-GPS Inference-Black Sea, U.S. Dept. of Transportation, Maritime Administration, 2017. https://www.maritime.dot.gov/content/2017-005a-black-sea-gps-interference

[5] Gregory Falco. Cybersecurity principles for space systems. Journal of Aerospace Information Systems, 2018

[6] Todd Harrison, Katylin Johnson, Joe Moye, and Thomas G. Roberts. Space threat assessment 2021. https://aerospace.csis.org/space-threat-assessment-2021/

[7] National Institute of Standards and Technology. NIST Cybersecurity Framework. v1.0 https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[8] Matthew Scholl. Introduction to Cybersecurity for Commercial Satellite Operations. Draft NISTIR 8270. June 2021
https://doi.org/10.6028/NIST.IR.8270-draft
[9] M.N. Hasan, T. Xu, L. Jianwei. An Efficient Encryption Algorithm for Perfect Forward Secrecy in Satellite Communication. Advances in Cyber Security. 2020.
[10] I. Fernandez-Hernandez et al., *A navigation message authentication proposal for the Galileo open service.* Journal of The Institute of Navigation, 63 (1), 2016
[11] N. Gisin et al., *Quantum cryptography.* Reviews of Modern Physics **74,** 145-195 (2002) https://doi.org/10.1103/RevModPhys.74.145
[12] H.-K. Lo et al., *Secure quantum key distribution.* Nature Photonics **8,** 595-604 (2014) https://doi.org/10.1038/nphoton.2014.149
[13] F. Xu et al., *Secure quantum key distribution with realistic devices.* Reviews of Modern Physics **92,** 025002 (2020)
https://doi.org/10.1103/RevModPhys.92.025002
[14] S.-K. Liao et al., *Satellite-to-ground quantum key distribution.* Nature **549,** 43-47 (2017) https://doi.org/10.1038/nature23655
[15] M.S. Hwang, C.C. Yang, C.Y. Shiu, *An authentication scheme for mobile satellite communication systems.* ACM SIGOPS Oper Syst Rev. 145(2-3), 42–47 (2003)
[16] Y.F. Chang, C.C. Chang, An efficient authentication protocol for mobile satellite communication systems. ACM SIGOPS Opering Systems Review 39(1), 70–84 (2005). https://doi:10.1145/1044552.1044560
[17] E.-J. Yoon, K.-Y. Yoo, J.-W. Hong, S.-Y. Yoon, D.-I. Park, and M.-J. Choi, An efficient and secure anonymous authentication scheme for mobile satellite communication systems, EURASIP Journal on Wireless Communications and Networking, no. 1, p. 86, 2011
[18] L. Davi, A. Dmitrienko, M. Egele, T. Fischer, T. Holz, R. Hund, S. Nürnberger, A.-R. Sadeghi. MoCFI: A Framework to Mitigate Control-Flow Attacks on Smartphones. Networks and Distributed Systems Security Symposium, 2010
[19] M. Zhang and R. Sekar. Control flow integrity for COTS binaries. USENIX Security 2013
[20] F. B. Cohen. Operating system protection through program evolution. Computer & Security 1993