CYBERSECURITY FOR A SUSTAINABLE, SECURE AND SAFE SPACE ENVIRONMENT

Luca del Monte

Directorate of Industry, Procurement and Legal Affairs
European Space Agency

SINAIA, 18/04/2016

ESA UNCLASSIFIED – For Official Use

Examples of hacking, spoofing, spying in space

Some unclassified examples from open literature include:

1. In 1998, German-US ROSAT space telescope inexplicably turned towards the sun, irreversibly damaging a critical optical sensor following a cyber-intrusion at the Goddard Space Flight Center.
2. On October 20, 2007, Landsat 7 experienced 12 or more minutes of interference. Again, on July 23, 2008, it experienced other 12 minutes of interference. The responsible party did not achieve all steps required to command the satellite, but the service was disturbed.
3. In 2008, NASA EOS AM–1 satellite experienced two events of disrupted control: in both cases, the attacker achieved all steps required to command the satellite, but did not issue commands.

NewSpace = new cyber threats

- The cybersecurity of space missions is a matter of competiveness for our space industry, and, at the same time, is a vital subject for the EU as owner of Copernicus and Galileo.

- The need to guarantee high production rates (e.g. 4 satellites per day in the case of the OneWeb constellation) requires the system integrators to stretch globally the existing supply chain, and to include new components providers.

- The globalization of manufacturing capabilities and the increased reliance upon commodity software and hardware for space and ground segments has expanded the opportunities for malicious modification in a manner that could compromise critical functionality.

ESA study on cybersecurity of space missions

- ESA has the very specific need and obligation to protect the European tax-payer investments based in space (and sometimes in deep-space) from cyber menaces, both of operational nature, or hidden and latent in the on-board components of the spacecraft.

- Two parallel **CLASSIFIED** studies – with GMV (Spain) and THALES (with the support of ThalesAlenia Space France) – have been conducted by ESA.

- First results show that, alongside technology development, **policy measures** are needed to address the cyber threats to which ESA is exposed

Cybersecurity risks associated to the supply chain (1/2)

- **Hardware, firmware and software can be maliciously modified in a manner that goes undetected.** The modifications can be made directly by individuals that have access to the **development processes** or by the tools that are used during design, development, or manufacturing. The malicious capabilities could be triggered at a later time by other cooperating components or by environmental factors.
- Within the context of a space mission supply chain, some **spacecraft on-board** components and items available on the market may contain spyware or logic bombs, which, when triggered, will render the system useless or worse, vulnerable to espionage or sabotage, even when far from the Earth orbit.
- The globalization of manufacturing capabilities and the increased reliance upon commodity software and hardware for **ground segments** has expanded the opportunities for malicious modification in a manner that could compromise critical functionality.

Cybersecurity risks associated to the supply chain (2/2)

- These and other vulnerabilities may not become apparent until the systems are under attack. When that happens, fixing the problem will require coordination between both supplier and user.

- Another source of risks in the supply chain is the **external personnel** who are involved in the outsourced services or who collaborate by any way with the organization.

Recommendations to address the supply chain and procurement security (1/2)

In order to mitigate cyber security risks stemming from the supply chain, the studies propose the development and implementation of policy measures including:

- The establishment of lists of:
  - ✓ Cyber components procured from Non-EU industries
  - ✓ sensitive items to be procured in Europe
  - ✓ sensitive cyber skills and know-how critical for the project/program (during development, deployment and operation phase)

  which shall be identified at the Kick Off of the project/program and maintained during all life of the project/program.
- The establishment of a verification team (full internal or with a trusted partner) to verify the security of the components/equipment provided by the manufacturers.
- The definition of a baseline Cyber security requirements list as a contractual document.

Recommendations to address the supply chain and procurement security (2/2)

The studies further propose to:

- Define all key terms about security in frame of Purchase and subcontracting activities, and share these terms with all the stakeholders (partners, subcontractors, ESA).
- Require contractually the manufacturers to be able to audit with respect to security aspects at each step of the realization of the components/equipment (e.g. samples)
- Purchase required systems items only from original equipment manufacturers, their authorized resellers, or other trusted sources
- Incorporate “cyber security in acquisition” into required training curricula for all appropriate ESA and partners workforces

Redu’s cybersecurity training range

1. One of the recommendations stemming from the studies: for specific training to increase the preparedness level of the space system operators to detect and react to a cyber-attack.

2. The main goal of the facility is to provide training, simulation and testing environment, and develop knowledge in awareness, detection/investigation, response and forensics to counter cyber-attacks. The exercises performed in this facility will include role playing by different teams (e.g. attackers, defenders, spies, hackers, hacktivists, crackers, etc...) trying to manage or to damage (depending on the role) the outcome of a specific simulated space mission.

3. Kick Off of the implementation phase was held on 25/2/2016. Initial operational capability to be achieved by end 2016.

Cooperation with EDA (1/2)

1. ESA DG and EDA CE concluded a Letter of Intent confirming the interest of EDA to enter into formal agreement with ESA in order to include the ESA's unique "space assets dedicated" facility in Redu within the set of cybersecurity facilities which will be pooled by EDA Member States.
2. The cooperation proposed by EDA represents an opportunity for the long term sustainable development of Redu. In this respect, the Agency intends to explore how to further open the utilisation of the facility also to other categories of users namely:

- ESA MS national institutions (e.g. defence or security related)
- EDA MS national institutions (e.g. defence or security related)
- EDA and other EU agencies (e.g. the Cyber Crime Center in the Hague)
- European Space Industry (including European satellite operators)
- Within this context, the Agency intends also to explore the feasibility of opening the utilisation of the facility to NATO (e.g. the Cooperative Cyber Defence Centre of Excellence in Tallin).

Cooperation with EDA (2/2)

A 400keuro study (200K€ from EDA and 200k€ from ESA) to:

1. Perform the cybersecurity risk assessment of defence-related space missions
2. Develop additional services to be provided as e.g.
   - **Technology research, development, experimentation and test (“**Redu as an independent security evaluation facility)
   - **Collaborative information sharing and analysis**
   - **Operations procedure development and experimentation**
   - **Legal, Policy and Capability requirements research**
   - **Secure access to space-based infrastructures**
   - **Hosted cyber-security operations centres**
   - **Hosted secure data centre services**