Space Law and the Internet: New Space Architectures, Connectivity and Cybersecurity
New Space Architectures, Connectivity, and Cybersecurity

Outline

1. What happened so far? Some publicly known attacks...
2. Cyber Security Risks – Concepts and Definitions
3. Evolution from Infrastructure to End-to-End Service Providers
4. Attack Vectors & Trends
5. Traditional Key Challenges
6. Evolution brings new Challenges
7. Threat Actors, Motivation and Impact
Cyber Security Threats to Satellites and Satellite-based Services

What happened so far? Some publicly known attacks…

- **1998**
  - UK Skynet military satellite reported to have been hacked, moving satellite’s position

- **1999**
  - US/German ROSAT X-Ray telescope satellite damaged by turn towards the sun
  - Link to hack into NASA Goddard Space Flight Center

- **2007 / 2008**
  - Landsat-7 and Terra EOS AM-1 experienced interferences leading to service unavailability
  - Attackers acquired commanding capabilities on Terra EOS AM-1, but did not issue commands

- **2014**
  - Russian cyber-espionage group abusing satellite based Internet connections to exfiltrate sensitive data of government, military, embassy, research, and pharmaceutical organisations in over 45 countries

- **2018**
  - THRIP espionage group compromised satellite operator; specific focus on systems monitoring and controlling satellites

- **2014**
  - Local jamming and spoofing of GPS / GNSS by Russia
Cyber Security Threats to Satellites and Satellite-based Services

Cyber Security Risks – Concepts and Definitions

Example
- Cyber Terrorists
- RF Replay of Telecommand
- Spoofability of RF
- Weak TC authentication
- Loss of control over Satellite
- Loss of satellite and associated services

(Source: OWASP)
Cyber Security Threats to Satellites and Satellite-based Services
Evolution from Infrastructure to End-to-End Service Providers
Cyber Security Threats to Satellites and Satellite-based Services

Attack Vectors

▲ Physical Attacks on
- Ground infrastructure (Gateways, TT&C sites, etc): directly via conventional weapons or indirectly via supporting systems (power and telecommunications provider, etc)
- Satellites
  - Kinetic (e.g., anti-satellite weapons, e.g., missiles) or
  - Non-Kinetic (laser, microwaves, electro-magnetic pulse, …)

▲ Electronic / RF Attacks: Jamming, Replay or Spoofing of different types of uplink/downlink signals
- Telecommand,
- Telemetry and/or
- Payload signals (TV, data services, navigation, etc)

▲ Cyber Attacks on Satellites and Ground Infrastructure, such as Ground Control Systems, Operations Support Systems (OSS) and Business Support Systems (BSS)
- Various attack vectors on satellite links, terrestrial networks, user terminals, systems, social engineering, malware, mobile media, …. 
Cyber Security Threats to Satellites and Satellite-based Services

Trending Attack Vectors: Destructive Malware (Ransomware and Wipers)

Wannacry and NotPetya Outbreaks in 2017 – the most devastating cyberattacks in history so far

▲ NotPetya – a Software Supply Chain Attack
• Attackers compromised Ukrainian accounting software vendor and deployed malware in software update repositories
• Customers got initial infection via software updates
• NotPetya spread across networks and spilled over to interconnected organisations

▲ 2018: Wannacry outbreak at Apple chip producer TSMC (one year after initial outbreak)

4000 servers and 45000 PCs unusable

$300m

$400m

$870m

$150+m turnover loss

Total Damage 10 Billion $
Cyber Security Threats to Satellites and Satellite-based Services

Trending Attack Vectors: Supply Chain Attacks

▲ Attackers attack their targets via their supply chain

▲ Campaign by Russian state actors targeting hundreds of US organisations in Energy, Nuclear, Aviation, Critical Manufacturing, Government

▲ Leveraged Supply Chain Attacks
  • compromising actual victims via suppliers with a lower security posture

▲ Supply Chain Risks moved up on the Agenda of NIST Risk Management Framework and US Federal Government

▲ As Satellite Service Providers are important suppliers to governments, military, critical infrastructure providers, they are becoming an even more interesting target

Source: CISA
Cyber Security Threats to Satellites and Satellite-based Services

Traditional Key Challenges (“Weaknesses”) driving Cyber Security Risks (1/2)

▲ Use of proprietary systems; often incompatible with standard security technologies (e.g., Anti-Virus) and security practices, like patching or hardening the configuration
  • Loss of supplier support or warranty if systems are changed by applying security patches or installing security software
  • System configuration often not fully adhering to good security practices; hardening of configuration may cause loss of warranty / supplier support

▲ Long system lifetimes: ground control systems are usually running as long as the lifetime of a satellite (15+ years)
  • Hardware and Operating System software usually not supported by their manufacturers over the full lifetime of a ground control system
    ➤ Maintaining stock of replacement hardware to replace failed hardware
    ➤ Running end of life software, that does not receive security patches anymore and has known vulnerabilities with public exploits
Cyber Security Threats to Satellites and Satellite-based Services

Traditional Key Challenges (“Weaknesses”) driving Cyber Security Risks (2/2)

▲ Systems have been designed and implemented 10+ years ago, based on security principles and standards at that time, which may not resist today’s threats, e.g.,
  • Perimeter security vs. defense-in-depth
  • Cryptographic algorithms, which are considered weak today (e.g., RSA 1024-bit, MD5 hash function, …)

▲ Many specialized, small manufacturers – some with limited focus and expertise in secure product development
  • Some components are insecure by design
  • Compensating security controls have to be implemented “around” these components (“walled garden”)

▲ Operational Safety sometimes conflicting with security controls and procedures, e.g.,
  • TT&C encryption sometimes considered an additional operational risk; requirement to fail “open”
  • Other controls sometimes perceived as conflicting with operational safety:
    - screensavers, locking of screens and session timeouts
    - (individual) accounts and complex passwords
Cyber Security Threats to Satellites and Satellite-based Services
Evolution brings new Challenges ("Weaknesses") (1/2)

▲ Space assets and customer services are strongly dependent on IT, OSS and BSS systems
   ➔ Attacks impacting support systems potentially impact dependent assets and services
   ➔ Digital transformation initiatives will further increase this dependency in the coming years

▲ HTS and MEO/LEO satellite systems require more complex ground infrastructure, including ground systems, TT&C sites and additional gateway and monitoring sites
   ➔ Driving complexity and attack surface

▲ Extending the use of 3rd party sites, hosting critical ground system infrastructure
   ➔ Physical security becoming more important, but also more difficult and more expensive to achieve
   ➔ Flow-down of security requirements to 3rd parties
Cyber Security Threats to Satellites and Satellite-based Services

Evolution brings new Challenges (“Weaknesses”) (2/2)

▲ New services require direct customer access to OSS and BSS systems and even the Space Segment (payload) via open interfaces (e.g., Internet)

⇒ new Security Engineering Challenges in a field that traditionally relied on perimeter security and complete isolation

▲ Complex eco-system of stakeholders, complex systems with separate operational responsibilities; interdependency, i.e., security failure/compromise of one sub-system may impact the security of another system, e.g.,

• Attacks leveraging physical access to hosted equipment at customer premises or 3rd party sites
• Attacks were published at Blackhat US 2018, where security researchers proved the feasibility of compromising a VSAT modem on board of an aircraft from the ground; the compromised modem can then serve as a pivot point to attack other systems to intercept communications and to manipulate antenna positioning (see https://ioactive.com/article/ioactive-reveals-major-satellite-communication-and-operating-system-vulnerabilities-at-black-hat-usa-2018-def-con-26/)
Cyber Security Threats to Satellites and Satellite-based Services

Threat Actors, Motivation and Impact (1/2)

▲ Mainly performing opportunistic target
▲ CEO fraud: scams targeting individuals with authority to conduct financial transactions
▲ Opportunistic infections with ransomware and crypto miners may impact services
▲ Cyber Espionage: theft of intellectual property with the aim to monetize or contract work

▲ Ideologically motivated, hence performing targeted attacks

▲ Satellite Operators and Service Providers are potential targets
   • to manipulate or disrupt media and playout services
   • due to serving specific military organisations and missions
   • interrupt satellite communication services or damage infrastructure to harm the victim organisation

▲ Targeted use of destructive malware poses a critical risk for victim organisations
   • Dependency on “difficult to secure” systems to deliver services and to control space assets
   • Outbreak of destructive malware may affect critical systems, potentially leading to outage of customer services or loss of control over space assets
Cyber Security Threats to Satellites and Satellite-based Services
Threat Actors, Motivation and Impact (2/2)

- Several nation states established groups targeting our industry
- Studies suggest that telcos and high-tech companies are targeted on average by 7 nation state threat actor groups
- Satellite Operators and Service Providers are potential targets for nation state actors
  - service provider for military, governments and critical infrastructure providers around the world (supply chain attacks)
  - holding valuable (space) assets and intellectual property of strategic interest to various states
- Cyber Espionage, aiming at
  - monitoring high value targets and military communications
  - stealing intellectual property and strategic business plans to support national economy
- Cyber Warfare
  - Nation states established capabilities to compromise, disrupt or destroy communication infrastructure, including satellite communication
  - Satellite Operators and Service Providers, are serving critical infrastructure providers, safety applications and military operations, and may become strategic targets in specific cyber warfare scenarios
    - Subversion or disruption of SATCOM operations in conflict areas
    - Advanced threat actors may seek systemic access to satellite communications through the use of implants or theft of encryption keys
References and Further Reading

- Space Threat Assessment 2018, Center for Strategic and International Studies
- William J Malik, Attack Vectors in Orbit, RSA Conference 2019