Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS

armasuisse

Source: https://www.5gworldpro.com/

The looming perils to **end users** in satellite communications

Vincent Lenders, Cyber-Defence Campus, Switzerland

50 new satellites are taking to the skies every week

LEO, MEO and GEO satellite constellations

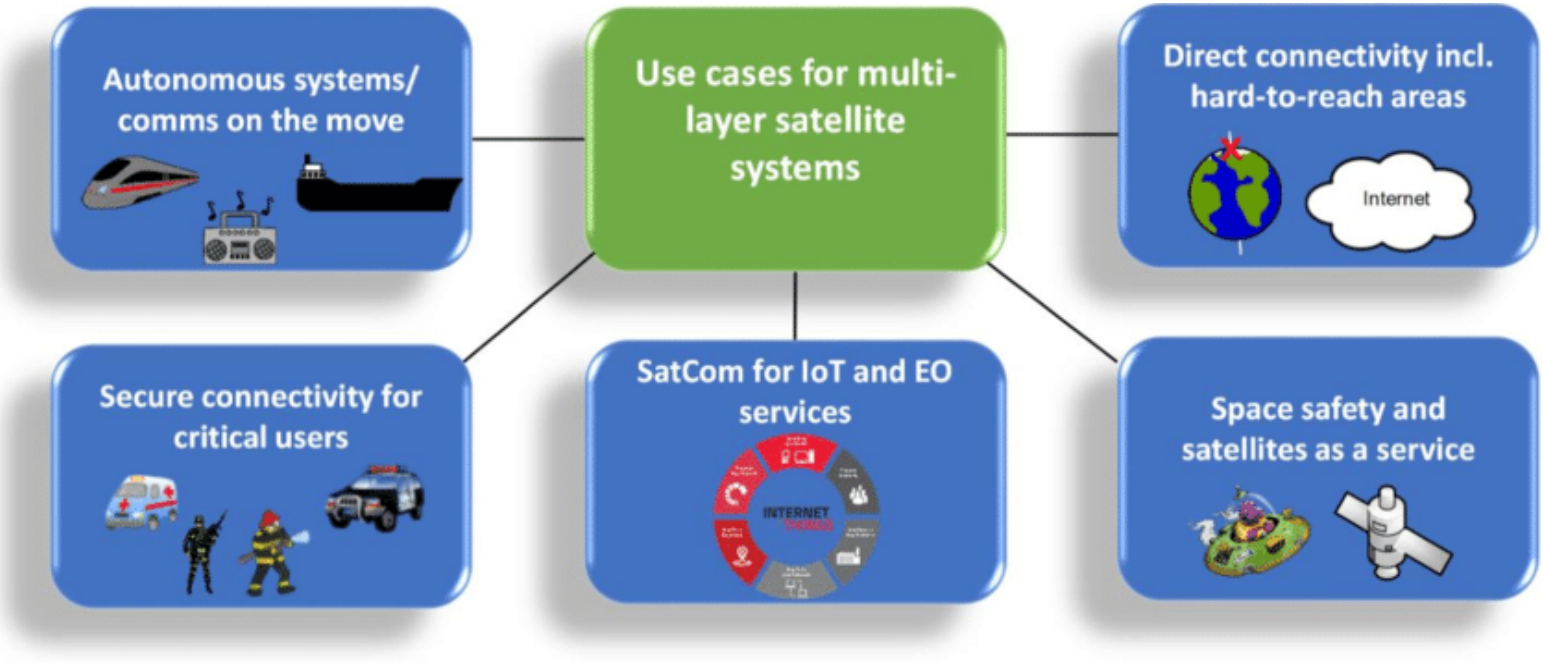
Source: https://eos.com/blog/satellite-constellation/

LEO: Starlink, OneWeb, Iridium, GlobalStar, RapidEye, …

MEO: Global Positioning System (GPS), Galileo, GLONASS, …

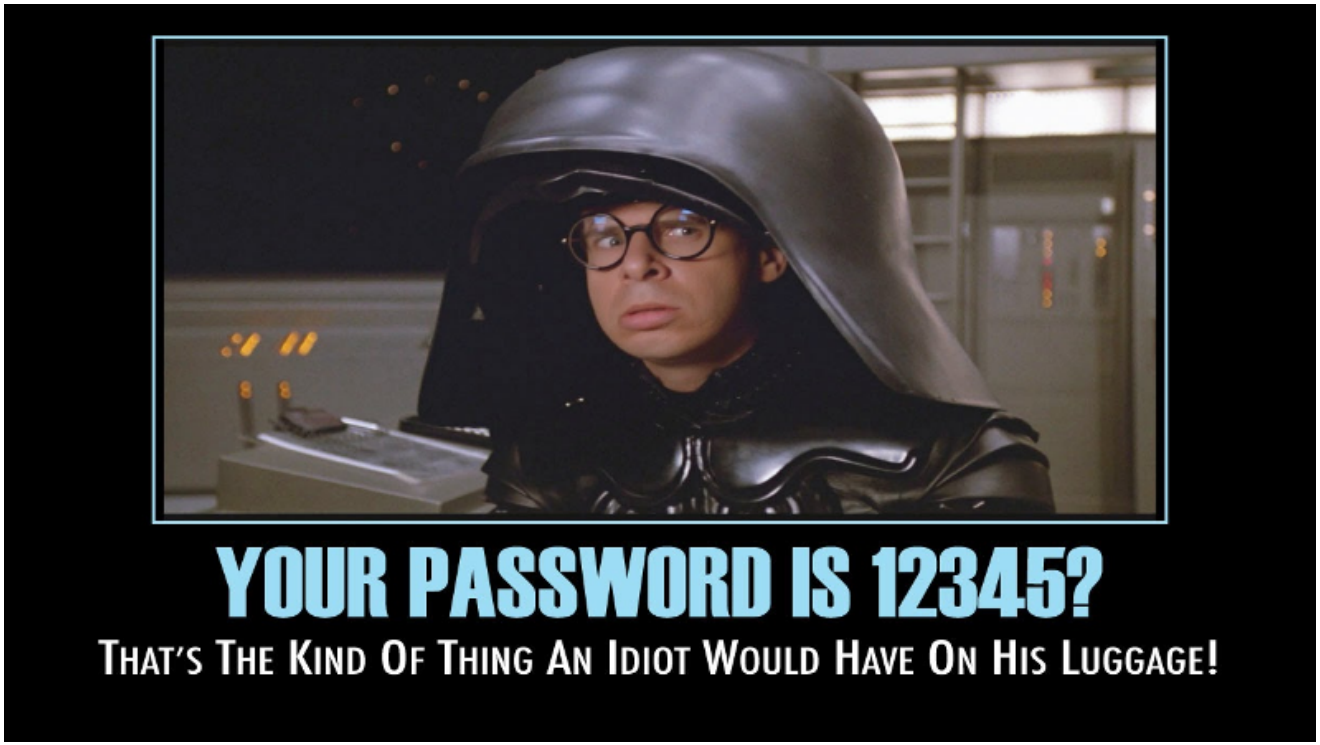
GEO: Viasat, SES, Inmarsat, Astra, Eutelsat, …

5G/6G Satellite Communications **Use Cases**

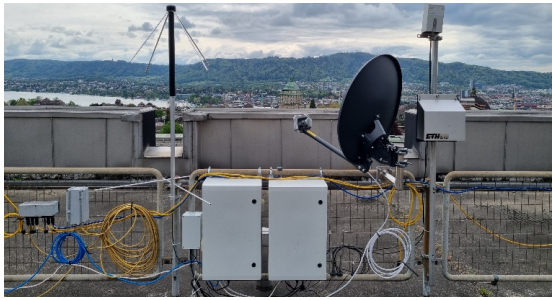


Source: DOI:10.1109/ACCESS.2022.3206862 under License CC BY 4.0

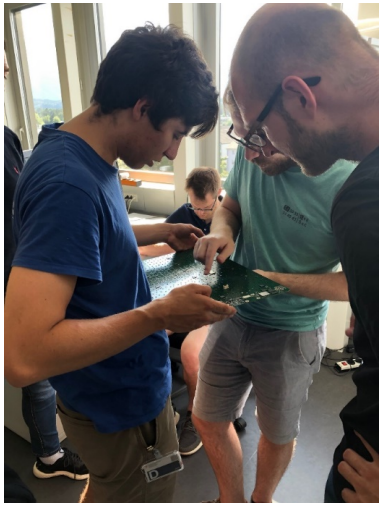
Cyber Security in Space?



SATCOM Security Research Lab Infrastructure at **Switzerland's Cyber-Defence Campus**



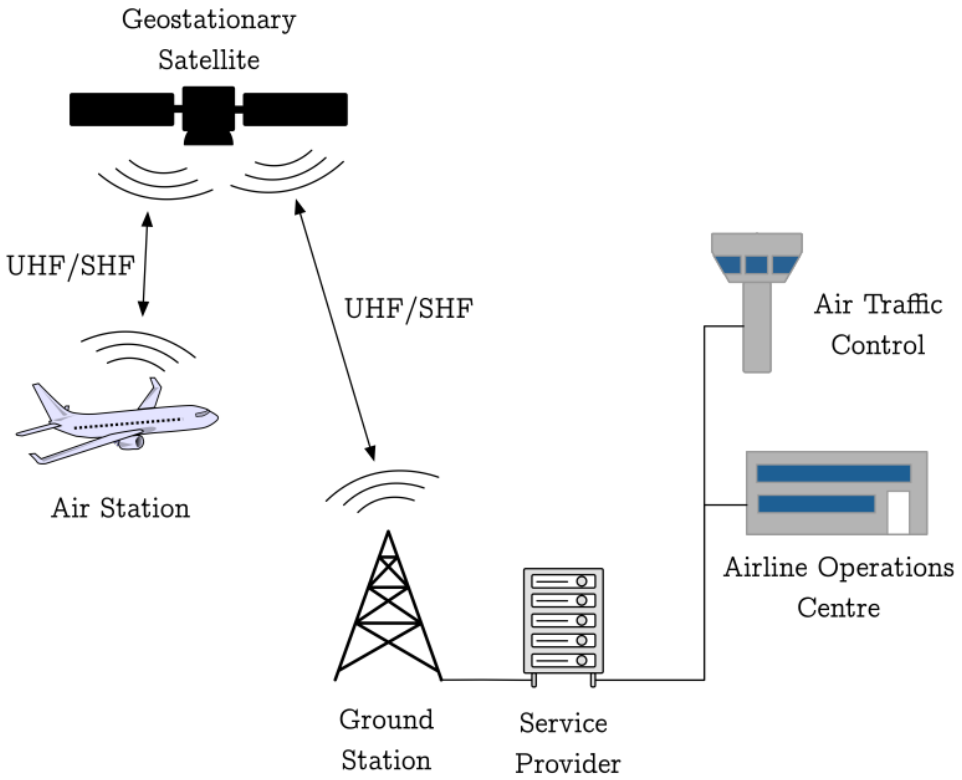
SATCOM Security Hackathons at **Switzerland's Cyber-Defence Campus**



Back a few years ago,

our first look at the **state-of-the-art**

ACARS – The short message service in aviation



SATCOM ACARS infrastructure

Bad Crypto in SATCOM ACARS

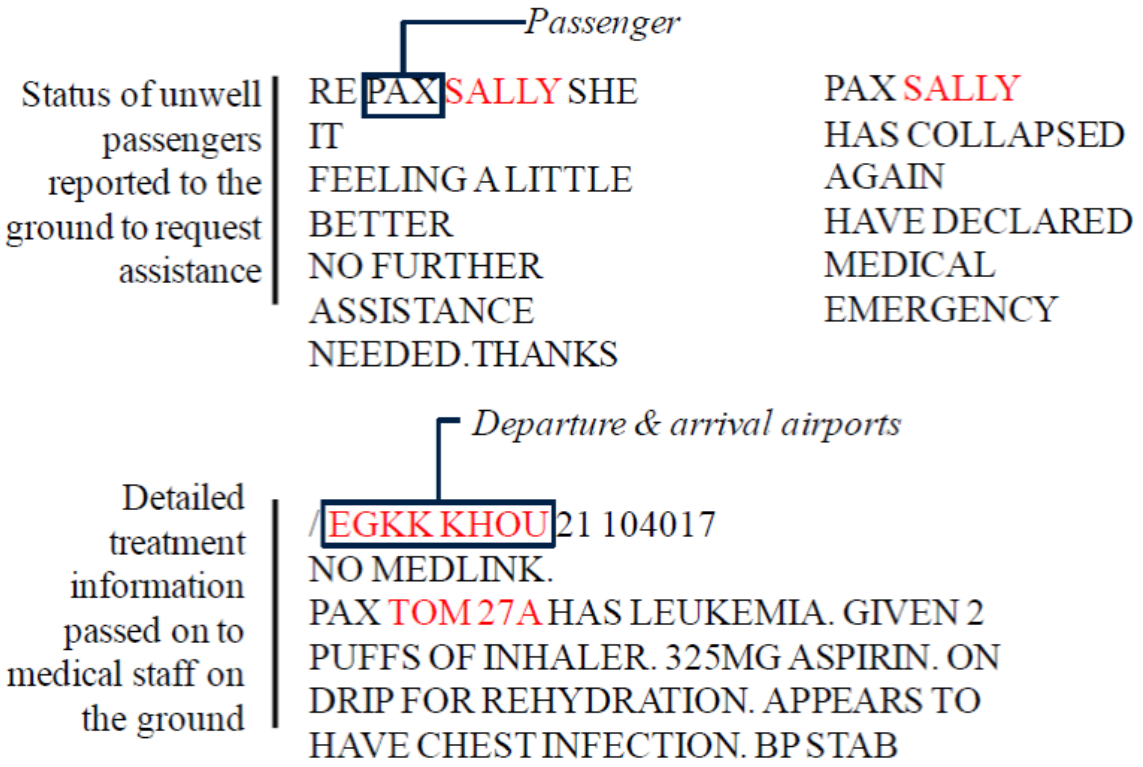
Key identifier

```
07*?X.0)Emk.;M].;4;Dm)m..) Y(*)]s($).M4U).U;;).MmD)..D+0
07*?X.0)EmUmkm]..D00M)4k.)]rr6) Y-\).k.<);4<k);000).;;+U
07*?X.0)EmUmUU]..D0Mk)m;.)]E{-) 6-r).k.;);;;;);4;;)..U+.
```

- ACARS encryption using a weak substitution cipher broken in minutes.
- Used by a wide range of private, military and government aircraft.

Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS, in *Financial Cryptography and Data Security 2017.*

Eavesdropping on ACARS: **Medical Issues**



Eavesdropping on ACARS: **Data at Risk**

Forgotten belongings, including hotel name, room number and specific items

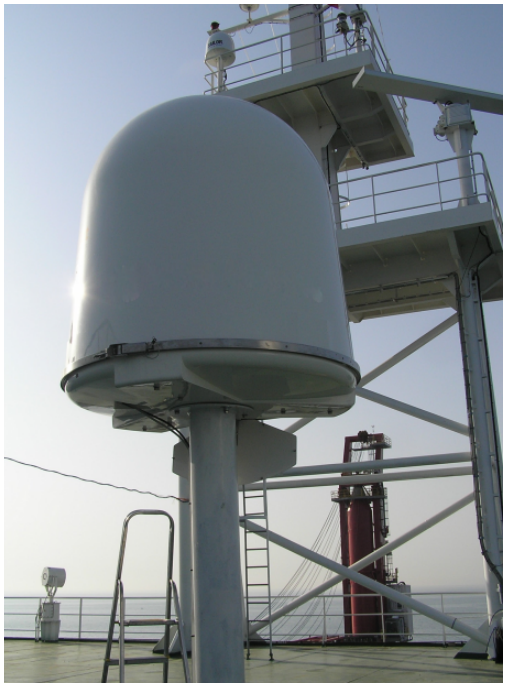
DEAR CCO COULD U PLS
ADVSE CAPT PAUL
TO RECOVER PASSPORT AND PERSONL
BELONGING LEFT
THAT CAPT JOHN LEFT IN ROOM 522
HOTEL WESTIN WASHINGTON DULLES
AIRPORT

Credit card details, sufficient to make a card-not-present transaction

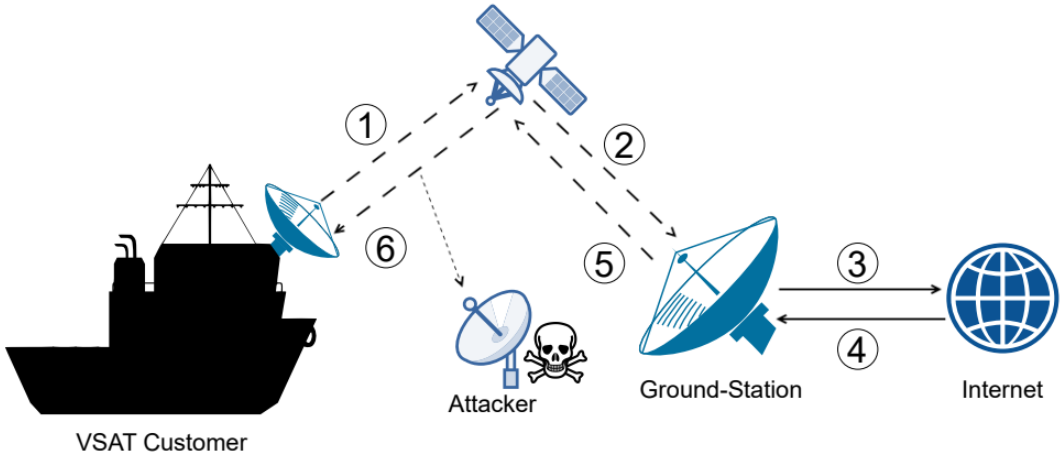
FR2200
PLS VERIFY CREDIT
CARD:
MASTERCARD
1234 5678 1234 5678 EXP
10/20
USD 552

Card type
Card number & expiry date

Maritime VSAT Communications

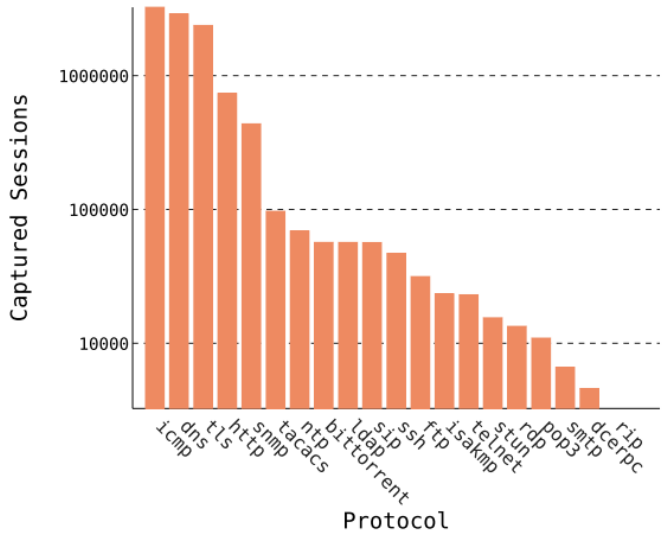


A typical marine VSAT system



Flow of data and interception of a maritime VSAT network

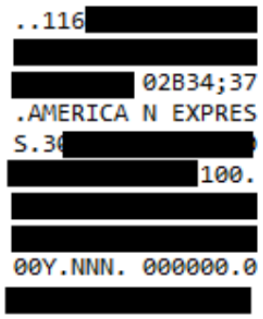
Eavesdropping on VSAT traffic



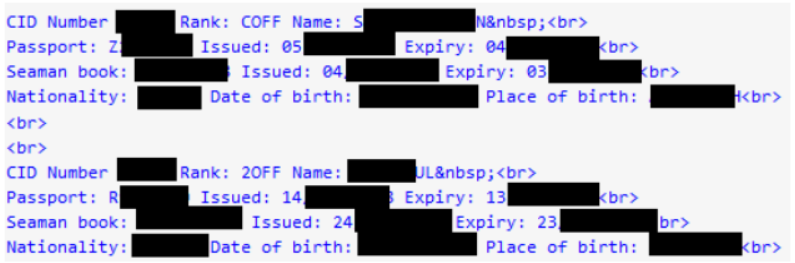
Top 20 protocols across all VSAT traffic

crew manifest from a $50 million luxury yacht

2nd Engineer","phone":null,"createdDate":1555016097,"inactive":false,"pictureUrl":null,"presencelog":
{"id":[redacted]"crewmemberId":[redacted],"present":true,"date":1556830579}},
{"id":[redacted]"groupId":[redacted],"idealId":null,"badgeId":null,"order":39,"lunchOrder":null,"
firstName":"H[redacted]","lastName":"D[redacted]","job":"Chief Stewardess","phone":null,"createdDate":1556961769,"inactive":false,"pictureUrl":null},
{"id":[redacted]"groupId":[redacted],"idealId":null,"badgeId":null,"order":40,"lunchOrder":null,"
firstName":"M[redacted]","lastName":"K[redacted]"job":"Stewardess","phone":null



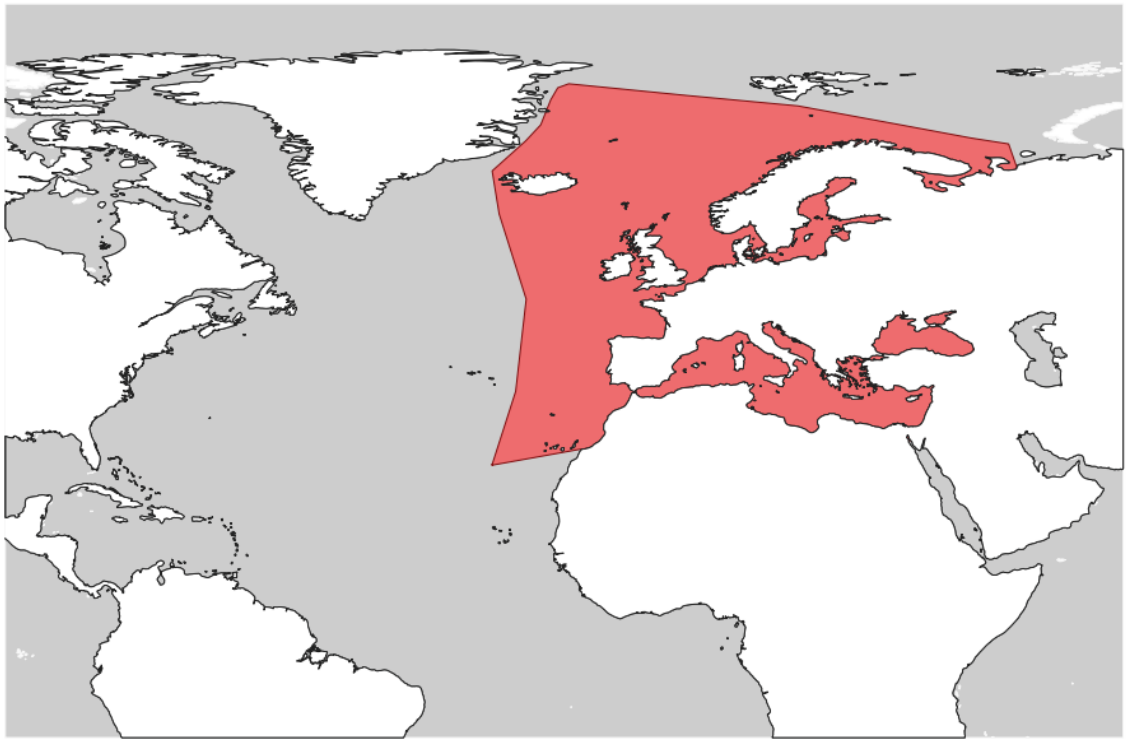
credit card information



passport and crew member data

A Tale of Sea and Sky: On the Security of Maritime VSAT Communication, in *IEEE Security and Privacy (S&P) 2020.*

Signal coverage footprint of a single receiver in Europe



- Founded by Motorola
- Deployed in the Late 90s
- 780km Low Earth Orbit
- 66 Operational Satellites in 6 Orbits (Plus Spares)
- Downlink in L-Band, Inter-Satellite Link in K_a-Link
- Satellite Change Every 9 Minutes (120 Minutes Worst-Case)
- **Voice** / Data

Eavesdropping on Iridium

Clear-text server connections

```
CONNECT.........................
Trying 193 [redacted]246, 4709 ..
Open............................
```

```
Trying 192 [redacted]98, 5200 ...
Open............................
```

```
ecIDCA02.}^0|1.0...U....Test cl
ients CA1.0...U....Illinois1.0.
duction, Inc...0.1.0...U.... [redacted]
[redacted]backend..0}^1.0...U....T
est client..~~!E..@..@...A[.z.i
```

Unencrypted emergency services

```
Ansbach;Kleinkind At
emnot  RTW 1 83 1 ([redacted]
[redacted]weg 4, 74549 Wo
lpertshausen) (RLS A
nsbach, Kanal 407);1
```

```
grierte Leitstelle K
oblenz;ExplosionB3 F
L Flugplatz Mendig
```

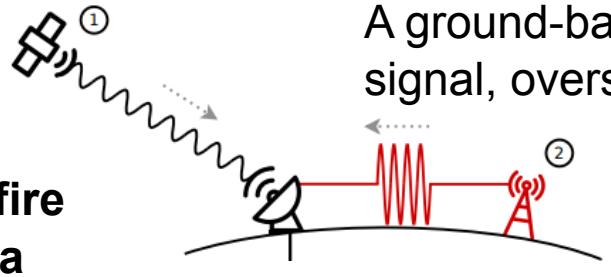
```
Lausitz;N6:Psychiatr
ischer-NF  Meissen [redacted]
[redacted]str. 3 / F[redacted],J[redacted]
smine Tablettenindox
```

```
grierte Leitstelle K
oblenz;Person droht
zu springenH2 [redacted]
rucke - jetzt auf de
m Ruckweg zur Treppe
```

```
 Mann liegt in der W
HG mit Schlinge um d
en Ha..............
```

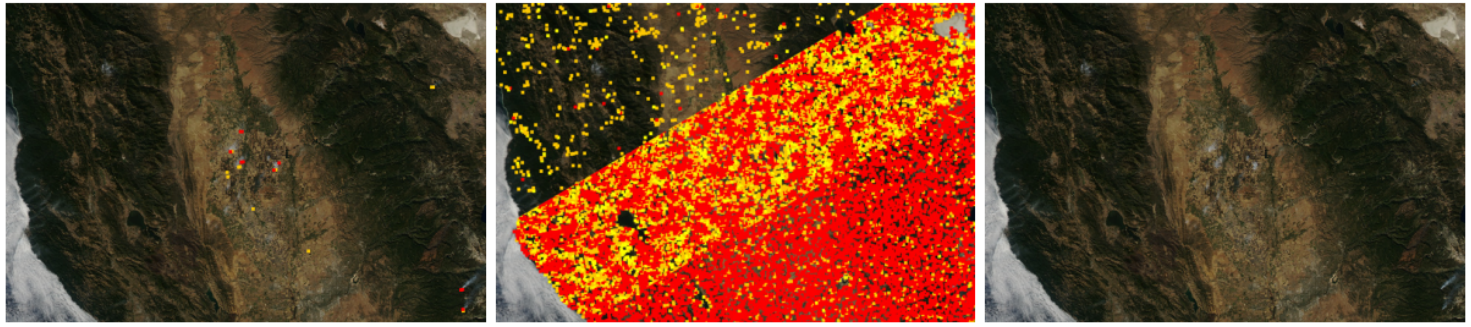

Let’s have a look at
active attacks

Spoofing Satellite Signals through **Radio Overshadowing**



A ground-based attacker **injects** a crafted signal, overshadowing the satellite signal

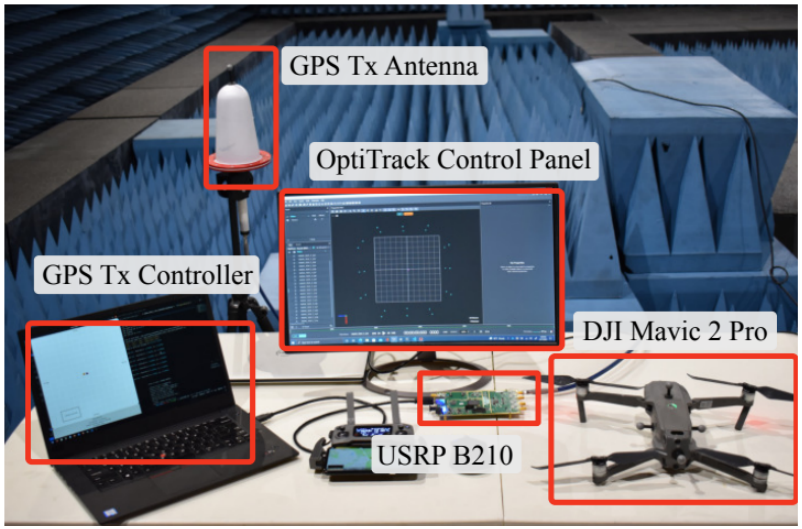
Spoofing earth fire observation data

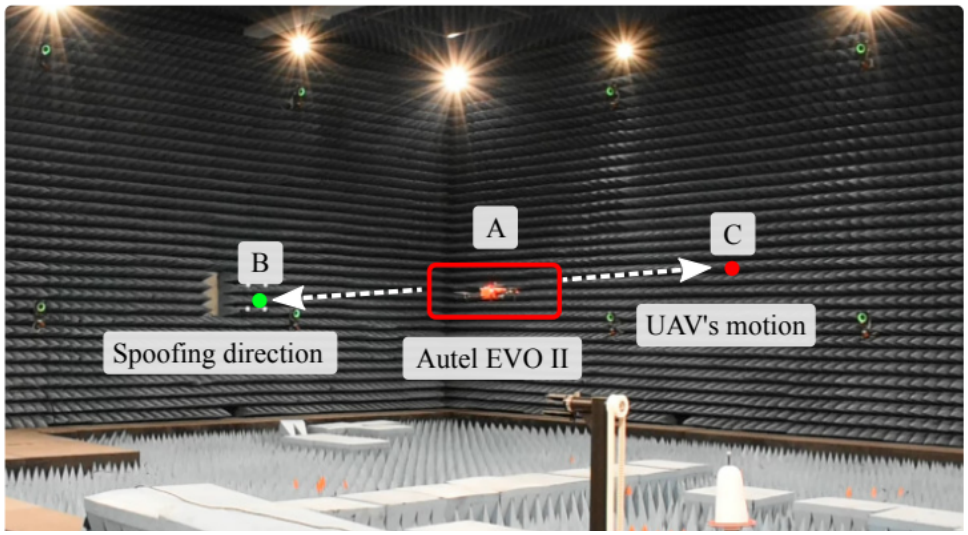


(a) Original image with some fires. (b) Fires randomly inserted uniformly across the map. (c) MODIS image with legitimate fires masked out.

Firefly: Spoofing Earth Observation Satellite Data through Radio Overshadowing, in *Workshop on the Security of Space and Satellite Systems (SpaceSec23).*

Controlled UAV Takeover via **GPS Spoofing**





An Experimental Study of GPS Spoofing and Takeover Attacks on UAVs,
in USENIX Security 2022.

M

oftware

MATT BURGESS SECURITY 23.03.2022 11:00 AM

A Mysterious Satellite Hack Has Victims Far Beyond Ukraine

The biggest hack since Russia's war began knocked thousands of people offline. The spillover extends deep into Europe.

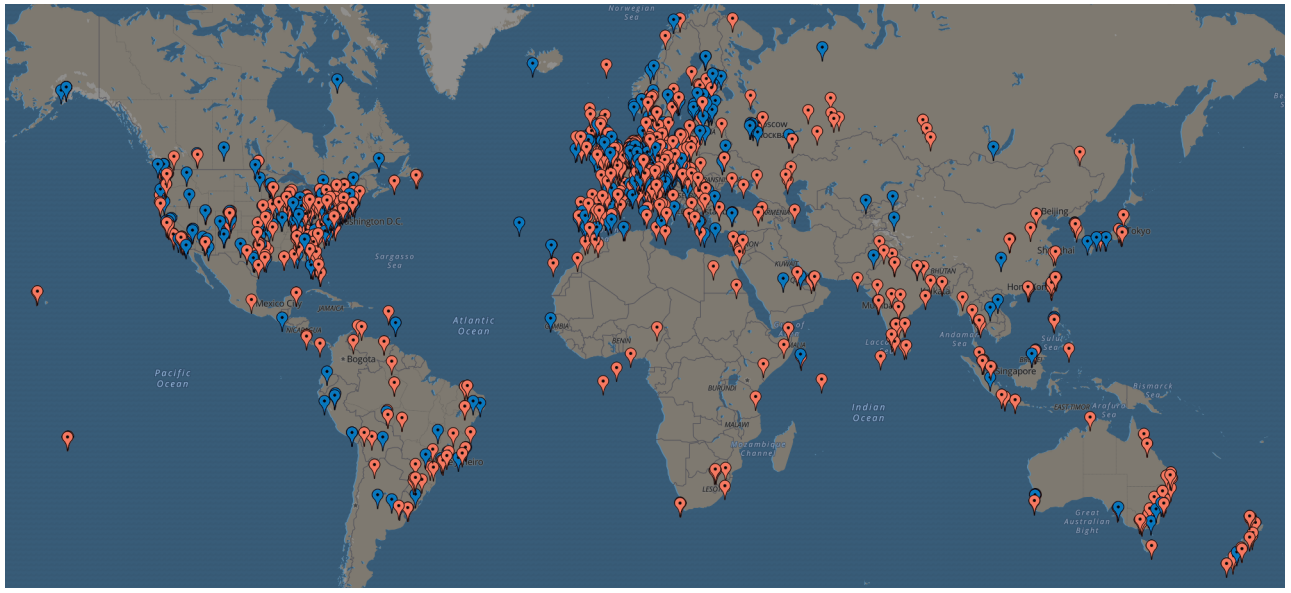
PHOTOGRAPH: BJDLZX/GETTY IMAGES

The need for **security countermeasures**

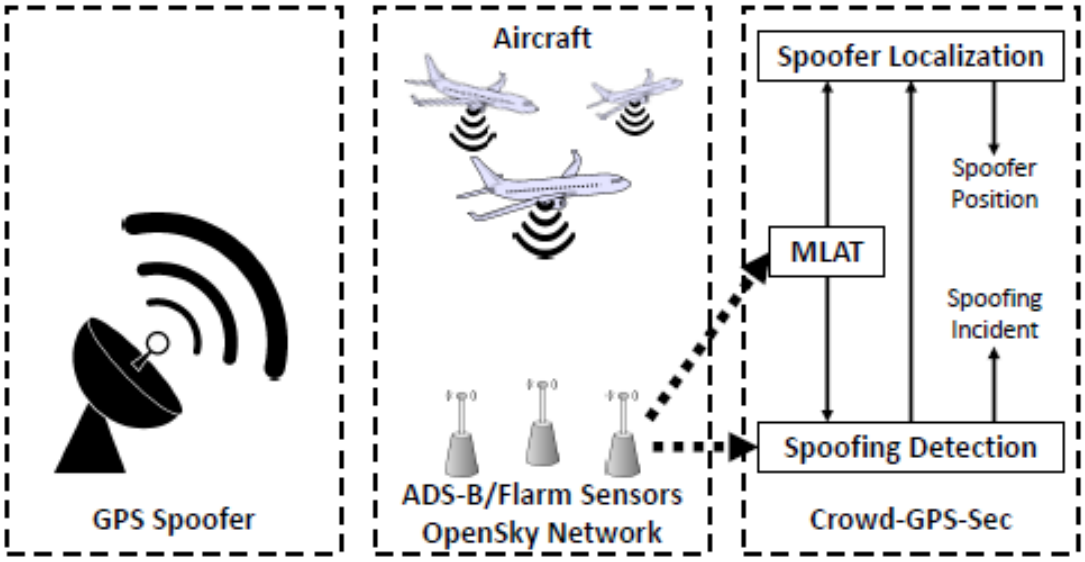
Leveraging **crowdsourcing** to detect GNSS spoofing attacks

OpenSky Network (opensky-network.org)

- Petabytes of real-world GNSS-derived air traffic data
- 6000 registered receivers worldwide
- Most coverage in EU, followed by US (about 7,500 active airports covered)



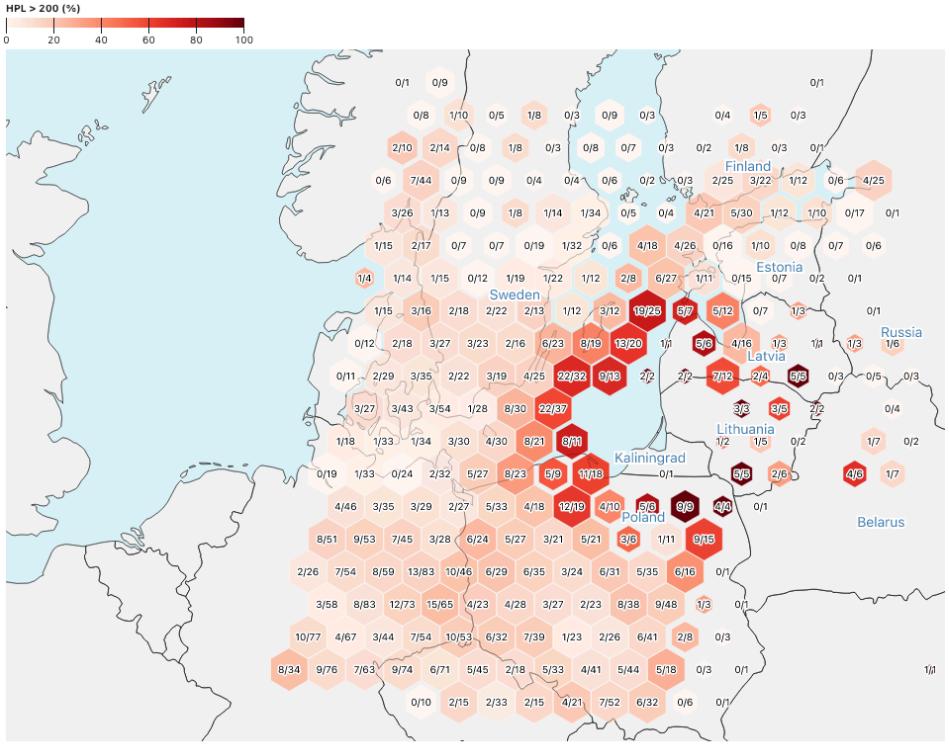
Crowd-GPS-Sec: Live GPS Spoofing Detection and Localization



- Exploits t**ime-difference-of-arrival** at different receiver locations
- GPS spoofing **detection** < 5 s
- GPS spoofer **localization** < 15 min

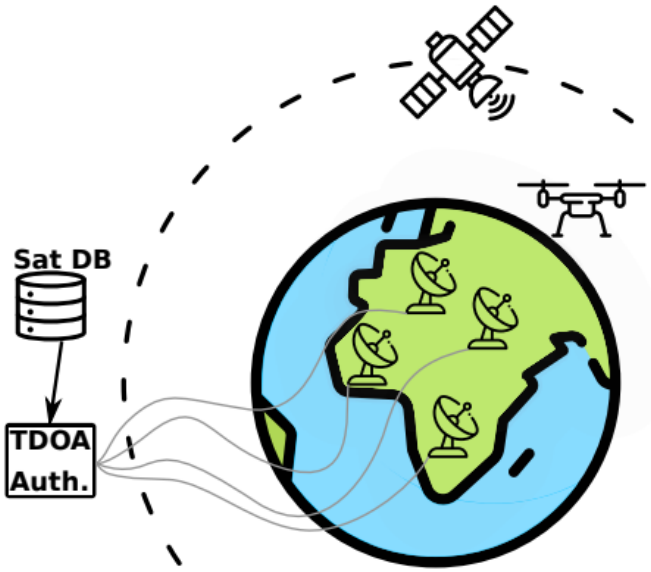
Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks,
in *IEEE Security & Privacy (S&P) 2018.*

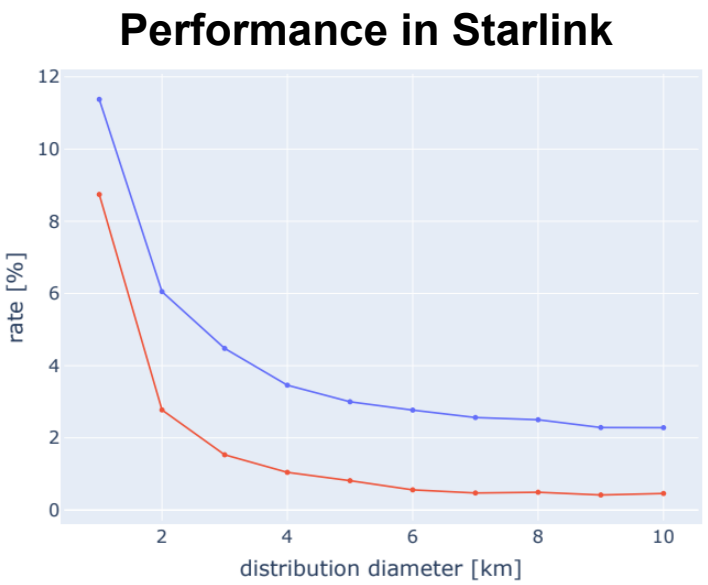
Detection of GPS Jamming around **Kaliningrad** during Ukraine conflict



Source: Xavier Olive, https://observablehq.com/@xoolive/gps-jamming

Orbit-based authentication using TDOA signatures



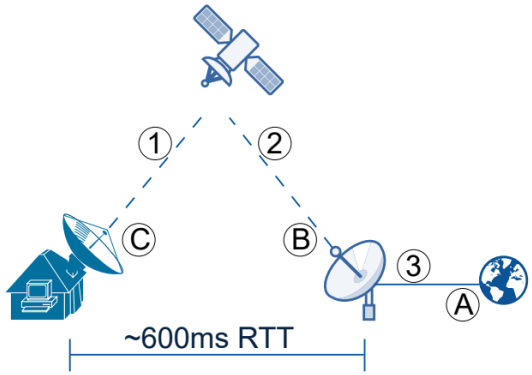


False rejection rates (blue) and false acceptance rates (red) at 6 receivers and 5 messages

Orbit-based Authentication Using TDOA Signatures in Satellite Networks,
in *ACM WiSec 2021.*

QPEP: An Actionable Approach to **Secure** and **Performant** Broadband From Geostationary Orbit

- **The problem**: GEO satellite links exhibit high round-trip times

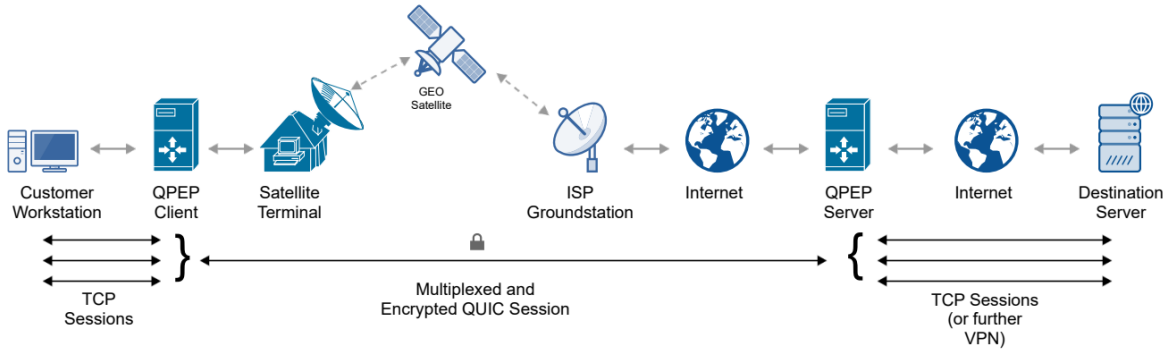


- **The state-of-the-art**: To speed up, performance enhancing proxies (PEP) acknowledge TCP packets already at the ground station, but these solutions do not work well with end-to-end encrypted VPN traffic

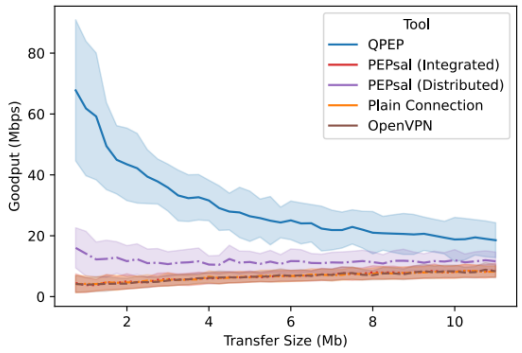
- **Our solution**: QPEP – a PEP/VPN hybrid solution based on QUIC

QPEP: An Actionable Approach to Secure and Performant Broadband From Geostationary Orbit

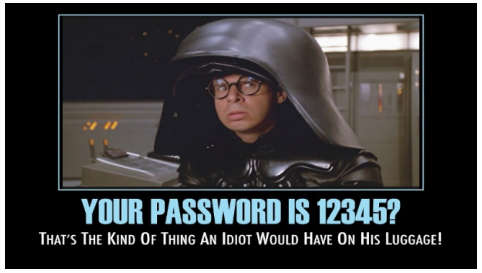
- QPEP system architecture



- QPEP performance



Conclusions



Satellite communication security is still **not mature** in 2023

Weakly protected data links allow for **low-cost** passive and active attacks

We need more research on **countermeasures** to protect **legacy** and **future** SATCOM systems

First **Scientific Workshop** dedicated to **Satellite and Space Systems Security**

Co-located with NDSS, 27 February 2023

19 Submissions
10 Accepts
3-4 Reviews/Paper

Full Room
~60 In-Person
~15 Virtual