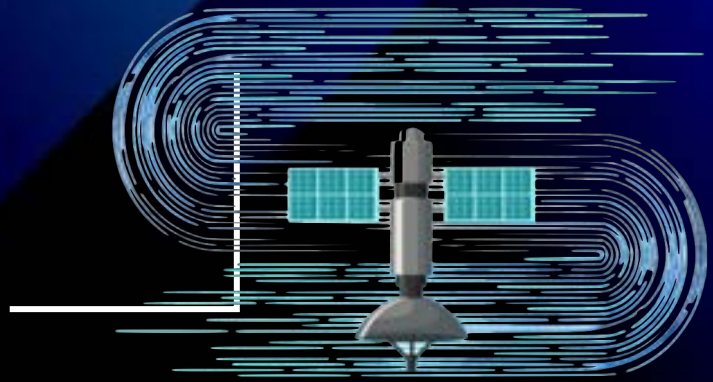
CYSEC

The best ways to protect LEO Satellite Communications



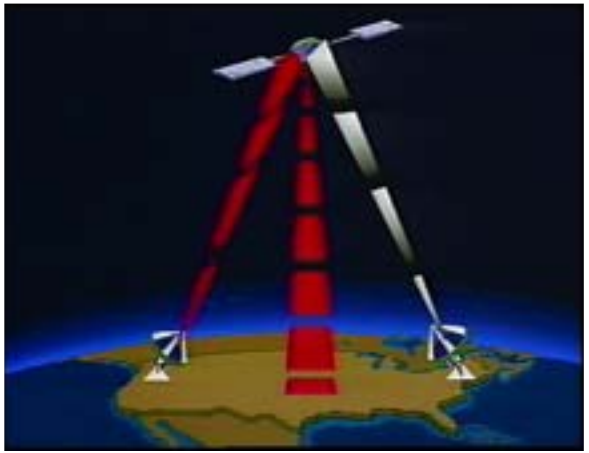
Patrick Trinkler

CUBESAT, 14.12.2023

Satellite hacking: happening since 1986!!

April 27, 1986

"Captain Midnight" jammed HBO's GEO satellite Galaxy 1 to protest against increasing prices for cable TV



2019, Pavur: “it’s not that hard”

Today many commercial satellite broadband services are unencrypted and vulnerable to eavesdropping attacks

James Pavur (ethical hacker from Oxford University) demonstrated in 2019 how to eavesdrop **sensitive data** transmitted over satcom links with 300$ equipment

WiSec’19, James Pavur et al. “*Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband*”

Feb 24th, 2022: an Earthquake in satcom security

Mar 30 2022 | Viasat Corporate

KA-SAT Network cyber attack overview

Viasat is providing an overview and incident report on the cyber-attack against the KA-SAT network, which occurred on 24 February 2022, and resulted in a partial interruption of KA-SAT's consumer-oriented satellite broadband service.

Viasat

On 24 February 2022, a multifaceted and deliberate cyber-attack against Viasat's KA-SAT network resulted in a partial interruption of KA-SAT's consumer-oriented satellite broadband service. While most users were unaffected by the incident, the cyber-attack did impact several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe. This incident was localized to a single consumer-oriented partition of the KA-SAT network that is operated on Viasat's behalf by a Eutelsat subsidiary, Skylogic, under a transition agreement Viasat signed with Eutelsat following Viasat's purchase of Euro Broadband Infrastructure Sàrl ("EBI"), the wholesale broadband services business created as part of Viasat's former partnering arrangement with Eutelsat. The residential broadband modems affected use the "Tooway" service brand. This cyber-attack did not impact Viasat's directly managed mobility or government users on the KA-SAT satellite. Similarly, the cyber-

Recent Posts

In-flight connectivity trends with Don Buchman

March 22, 2022

7 ways to maximize your Wi-Fi network

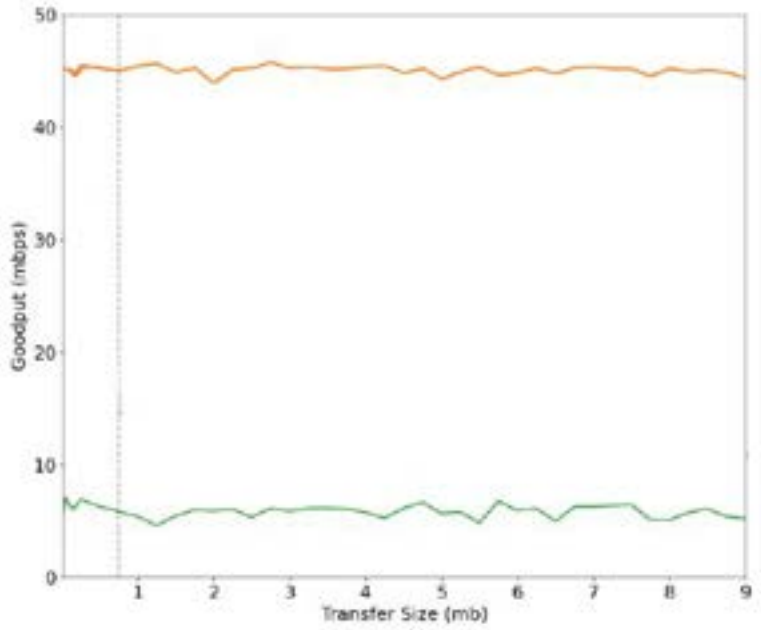
March 21, 2022

Feb 24th, 2022: Russia takes down satcom modems used by Ukrainian army

State-sponsored attack on civil satcom provider: game-changer

Satcom data confidentiality? Easy! Let's use a VPN!

Measurement on a GEO commercial satcom link



Plain

OpenVPN

State-of-the-art VPNs like **OpenVPN can reduce the link throughput by as much as 80% [1]** making them inacceptable by ISPs and end-users

[1] Jason Fritz. "Satellite Hacking: A Guide for the Perplexed". In: Culture Mandala 10.1 (2013), p. 5906. url: https://cm.scholasticahq.com/article/5906-satellite-hacking-a-guide-for-the-perplexed.

GEO and LEO users have to choose between performance and exposing their data to eavesdropping attacks

Recap' GEO / LEO: a common ground but different situations

GEO

- Historically (GEO players), civil satellite communications have been mostly in clear
- Encryption was the problem of the end-user: "Good luck!"

-> Eavesdropping GEO satcom data is NOT HARD

- Unfortunately, there is no "easy fix" since most of the time applying security (e.g. VPN) to GEO links impact performances -> not acceptable for users

LEO

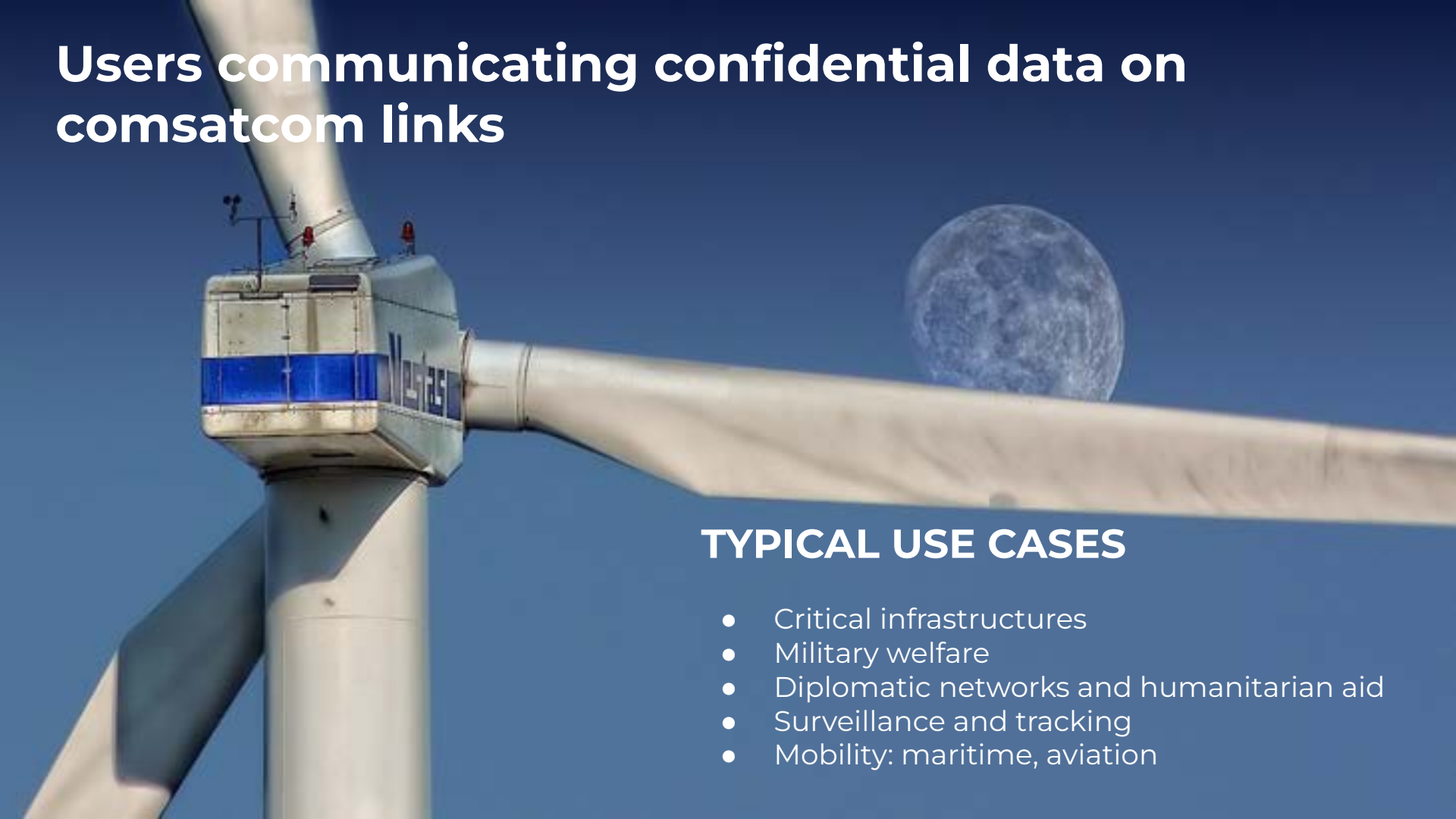
- LEO constellations using modern tools (Starlink with DevSecOps)
- Traditional tools like VPNs do work on LEO links without much impact

However, data confidentiality remains a challenge:

- Legal obligations to provide access to data to governments
- Users still have to trust a third-party infrastructure deployed on a global stage

Multi-orbit connectivity = "multi-security" challenges!

Users communicating confidential data on comsatcom links



TYPICAL USE CASES

- Critical infrastructures
- Military welfare
- Diplomatic networks and humanitarian aid
- Surveillance and tracking
- Mobility: maritime, aviation

What is “Zero trust”?

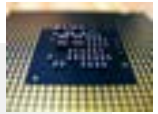
Definition

“Zero Trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location *(i.e., local area networks versus the Internet) or based on asset ownership (enterprise or personally owned).”*

NIST SP 800-207 Zero Trust Architecture, August 2020

In reality..



- ”Zero” is not realistic

Applied to satcom:

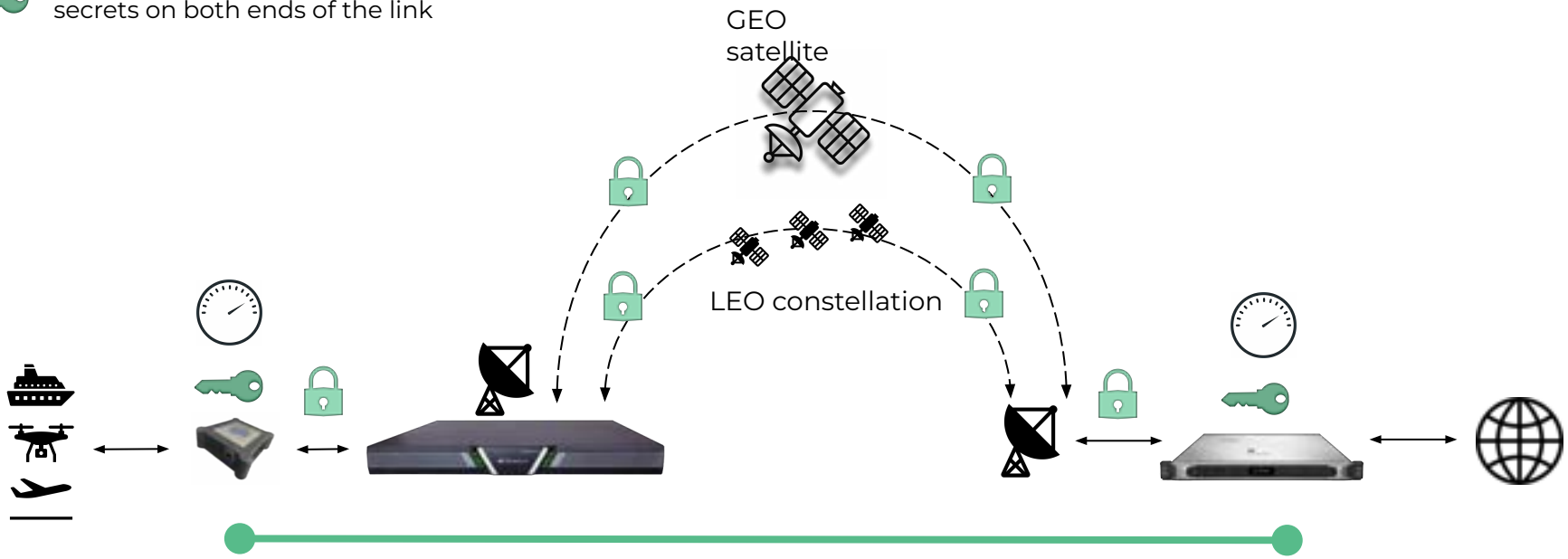
- Goal is to reduce dependency on third party’s infrastructure

-> **Cryptography is a powerful tool**

ARCA SATCOM: “Zero Trust” security & speed

Performances: latency (LEO), throughput (GEO)

“**Zero Trust”**: full control over cryptographic secrets on both ends of the link



End-to-end protection of satcom data

Real-world testing..

Client connection on the roof

- Remote access to two different Satellite connections (Lausanne & Zurich). Allows for cross-validation of the data, as well as detecting issues specific to either of the test setups (misconfiguration, maintenance, etc)

LEO Starlink connection at CYSEC's office

- Testbed for different satellite network (LEO), in order to investigate ISP-specific induced latency / compatibility
- Easy access and fast test implementation

Thank you

CYSEC

Patrick Trinkler

patrick.trinkler@cysec.com