NS2 Network and System Security Laboratory KAIST

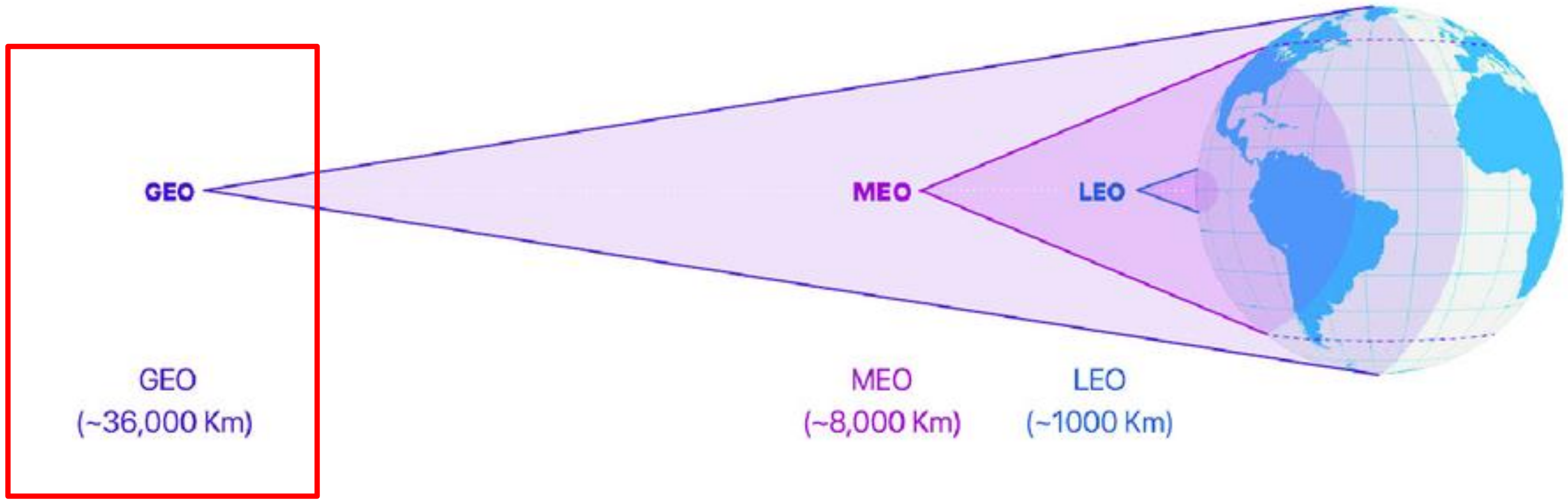
Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband

James Pavur, Daniel Moser, Vincent Lenders, and Ivan Martinovic

WiSec 2019

Presenter: Taeha Kim

Geostationary Satellite



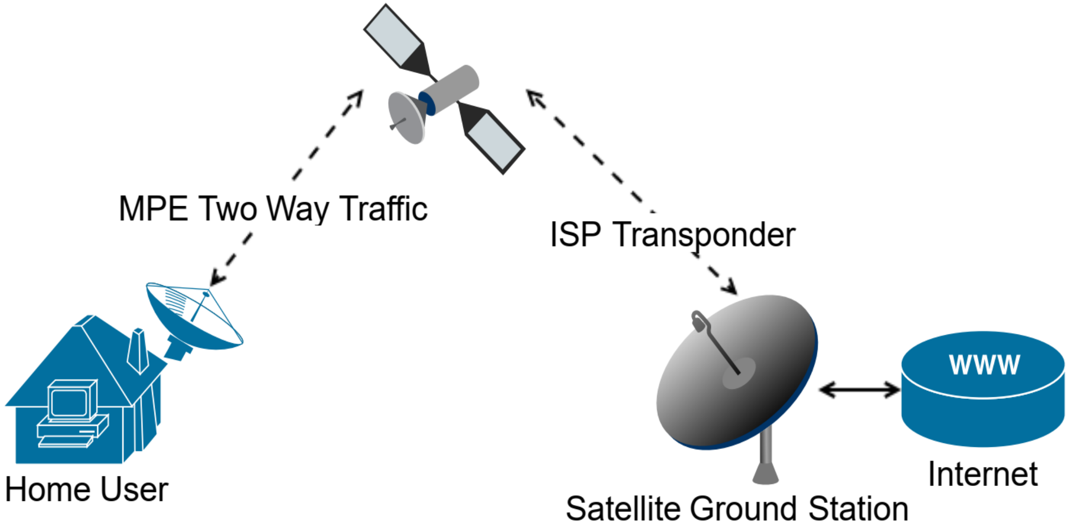
- ~36,000 km directly above the equator
- Appears nearly ***'stationary'*** to ground observers
- **Telecomm.** (broadcasting, internet, and telephone), weather monitoring, etc.

Image Ref: Darkening Low-Earth Orbit Satellite Constellations: A Review - Scientific Figure on ResearchGate.

Introduction

GOAL: Assess GEO Sat. broadband (internet) security

- **DVB-S**: widely used Sat. broadband protocol
- Focus on *low-resourced* malicious actors
- Recorded traffic from 14 GEO-Sat



Related Work

[1] André Adelsbach et al., **2005**, *“Satellite Communication without Privacy - Attacker’s Paradise”*
[2] Adam Laurie, **2009**, *“$atellite Hacking for Fun & Pr0fit!”*
[3] Leonardo Egea, **2010**, *“Playing in a Satellite environment 1.2”*
[4] S. Iyengar et al., **2007**, *“Security requirements for IP over satellite DVB networks”*
[5] L. Duquerroy et al., **2004**, *“SatiPSec : An Optimized Solution for Securing Multicast and Unicast Satellite Transmissions”*
[6] H. Cruickshank et al., **2005**, *“Securing multicast in DVBRCS satellite systems”*

- No recent works on “satellite broadband security”
- Focus on only individual satellite
- Primarily researched by hobbyist, criminal communities in recent
  - Illegal cracking, cloning private keys…

Related Work

[1] André Adelsbach et al., **2005**, *“Satellite Communication without Privacy - Attacker’s Paradise”*

[2] Adam Laurie, **2009**, *“Şatellite Hacking for Fun & Pr0fit!”*

[3] Leonardo Egea, **2010**, *“Playing in a Satellite environment 1.2”*

[4] S. Iyengar et al., **2007**, *“Security requirements for IP over satellite DVB networks”*

[5] L. Duquerroy et al., **2004**, *“SatiPSec : An Optimized Solution for Securing Multicast and Unicast Satellite Transmissions”*

[6] H. Cruickshank et al., **2005**, *“Securing multicast in DVBRCS satellite systems”*

- No recent works on “satellite broadband security”
- Focus on only individual satellite
- Primarily researched by hobbyist, criminal communities in recent
  - Illegal cracking, cloning private keys…

In this paper, authors aimed to

1. **Update findings in the contexts of modern internet traffic**
2. **Broad analysis on a multiple GEO satellite**

DVB-S Protocol

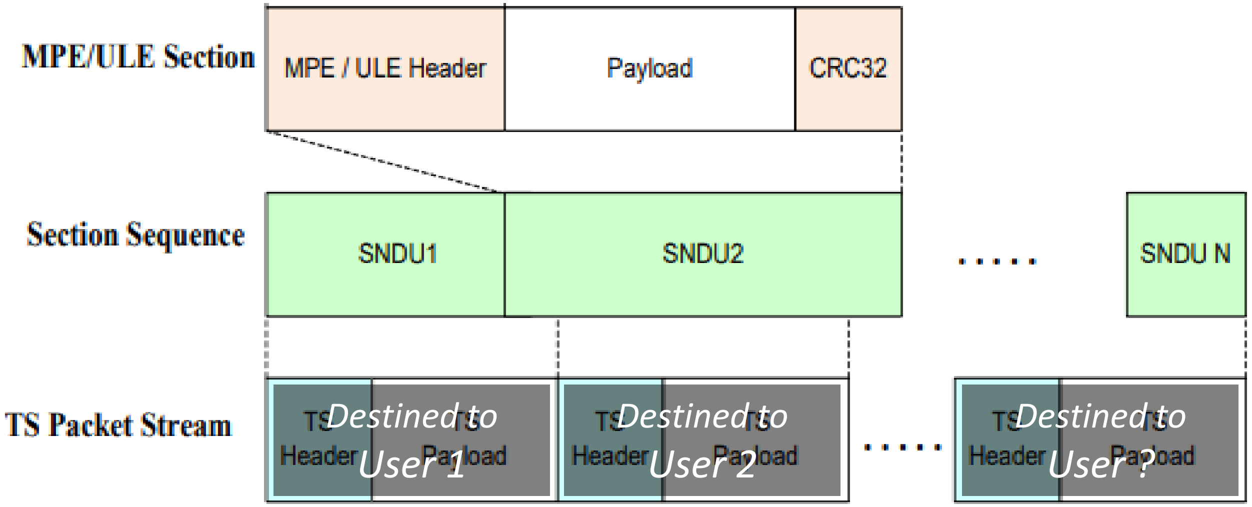
- DVB-S, DVB-S2 = Digital Video Broadcasting-Satellite
- Originally developed for satellite TV
- De facto standard for broadcast, IP services in GEO

  -> Various public tools, analyzers

DVB-S Protocol

- MPEG-TS: data stream transmitting standard
- MPE/ULE: encapsulation protocol
- **Shared stream**
  - Packets for multiple customers are transmitted on same stream
  - Extracted on customer equipment by information in header

DVB-S Protocol



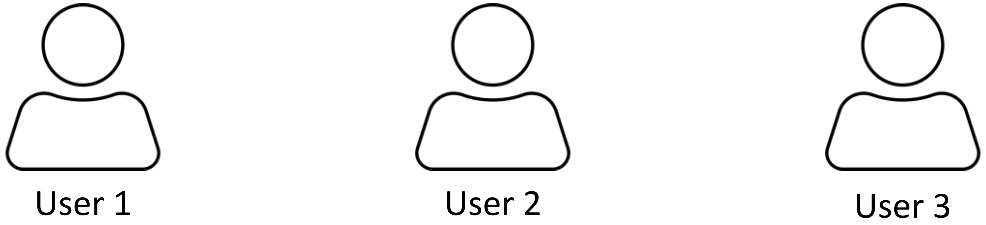
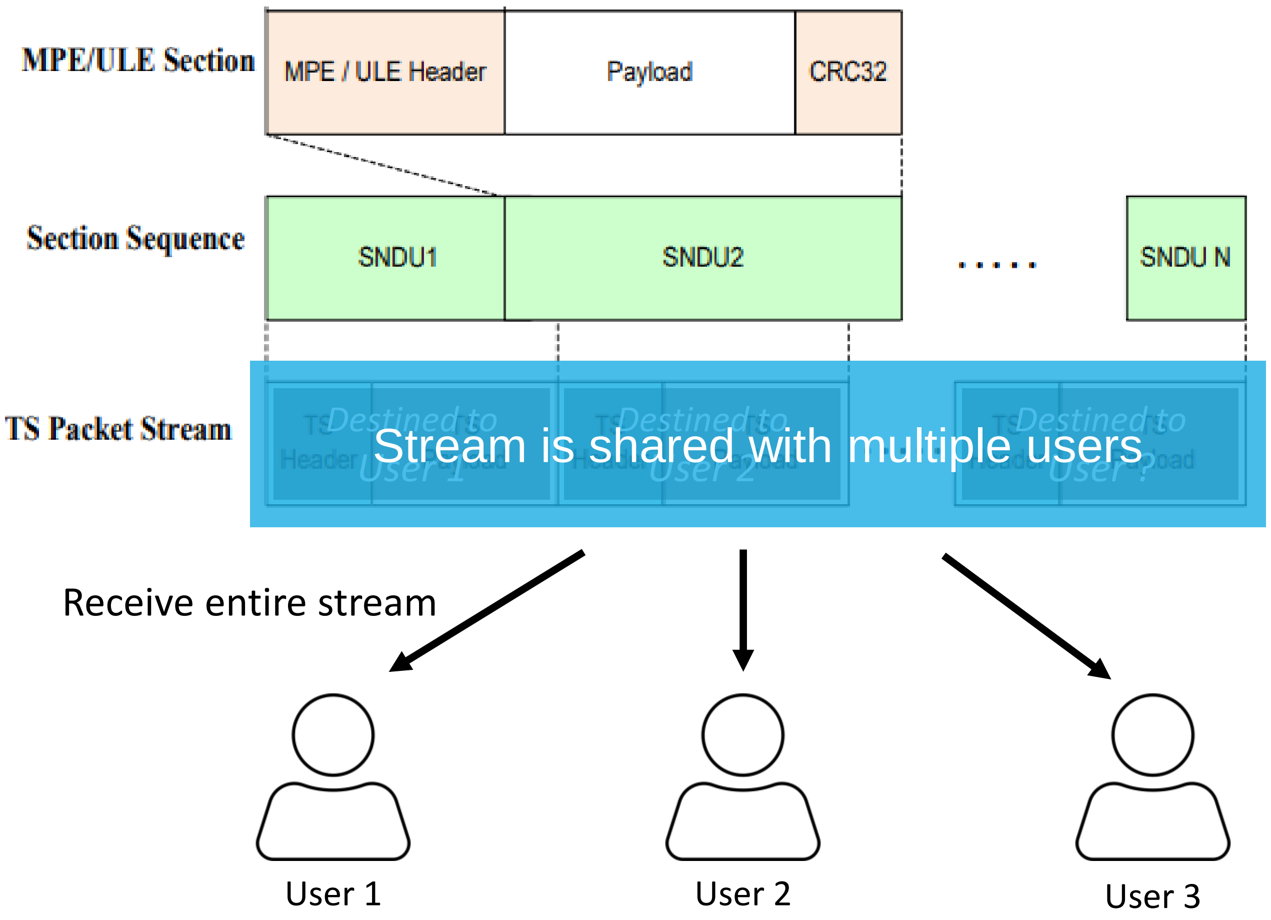


Image Ref: G. Tehashri et al., Analysis and Implementation of Encapsulation Schemes for Baseband Frame of DVB-S2 Satellite Modulator

DVB-S Protocol



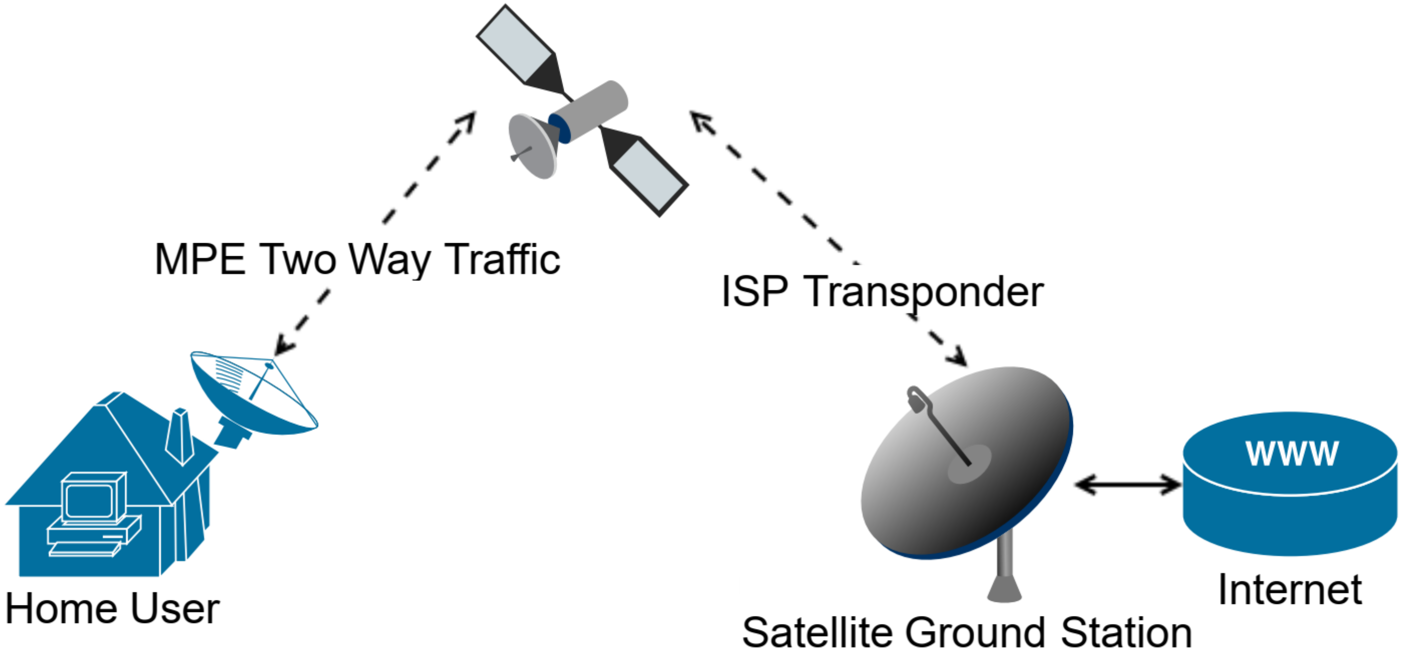
Stream is shared with multiple users

Receive entire stream

Image Ref: G. Tehashri et al., Analysis and Implementation of Encapsulation Schemes for Baseband Frame of DVB-S2 Satellite Modulator

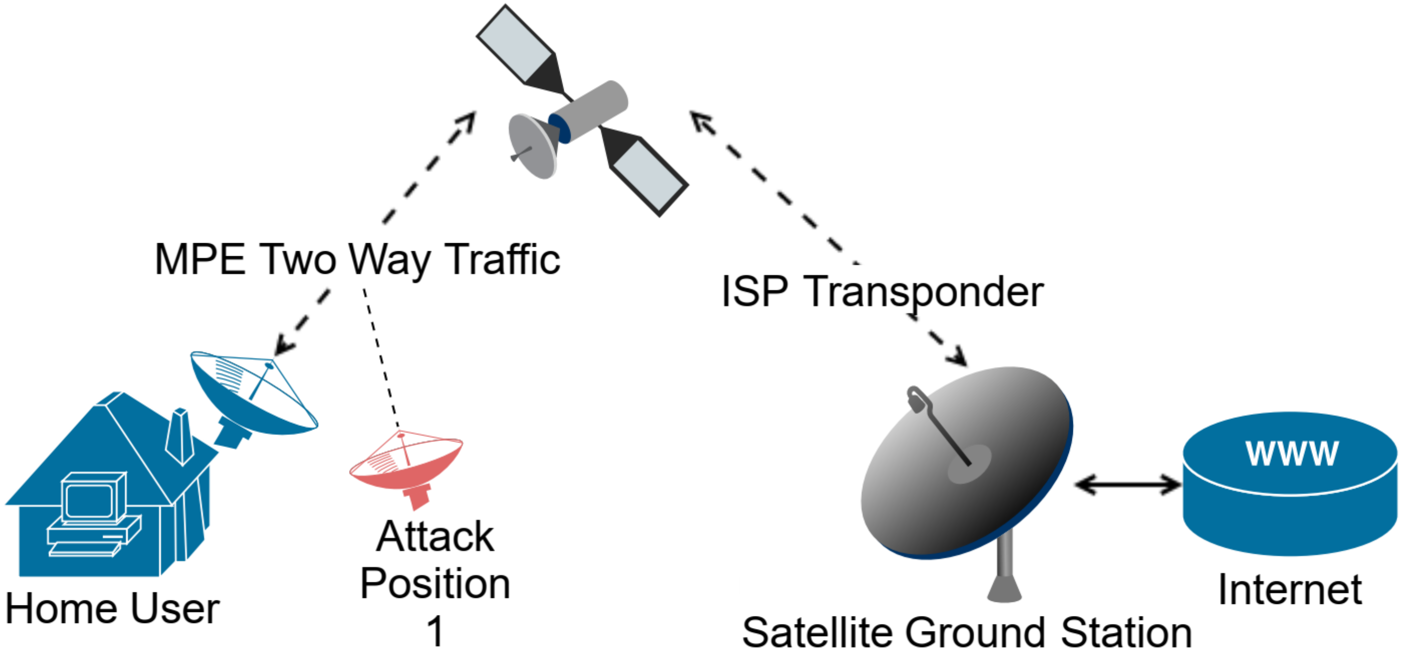
Threat Model

- Two-way satellite internet setup



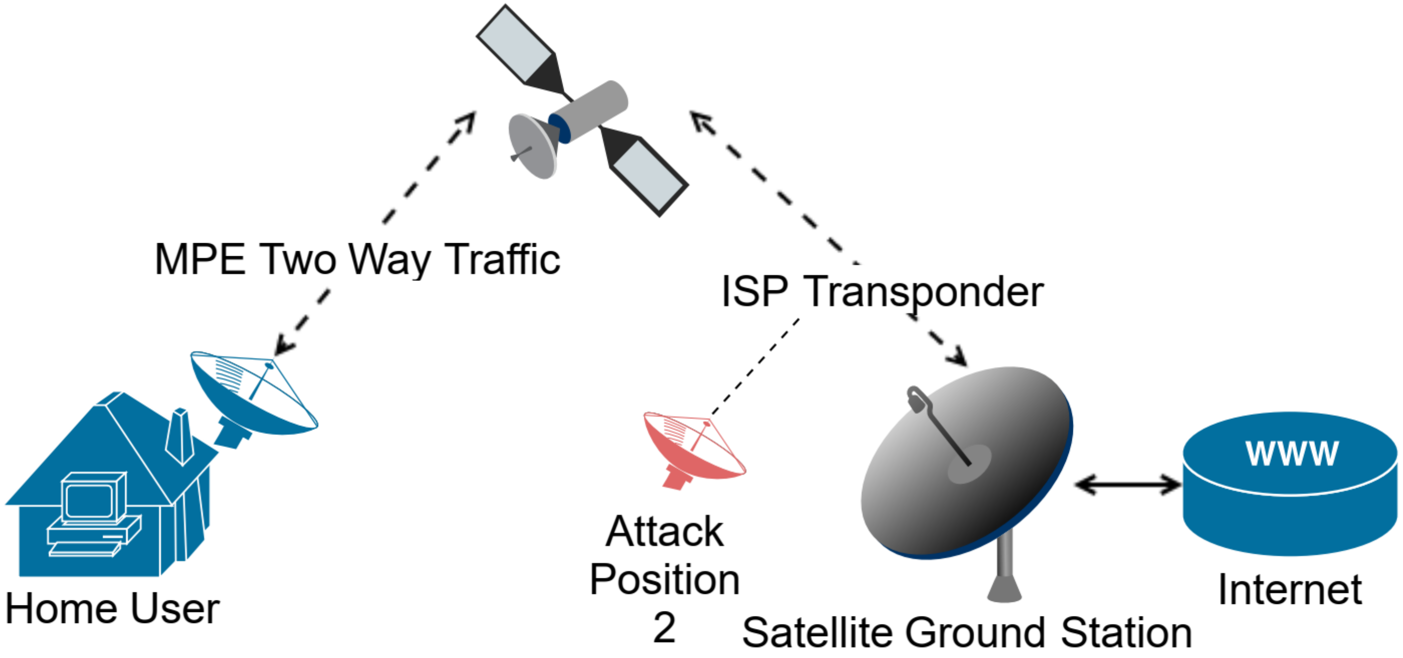
Threat Model

- Attack position 1: listening downlink-to-consumer



Threat Model

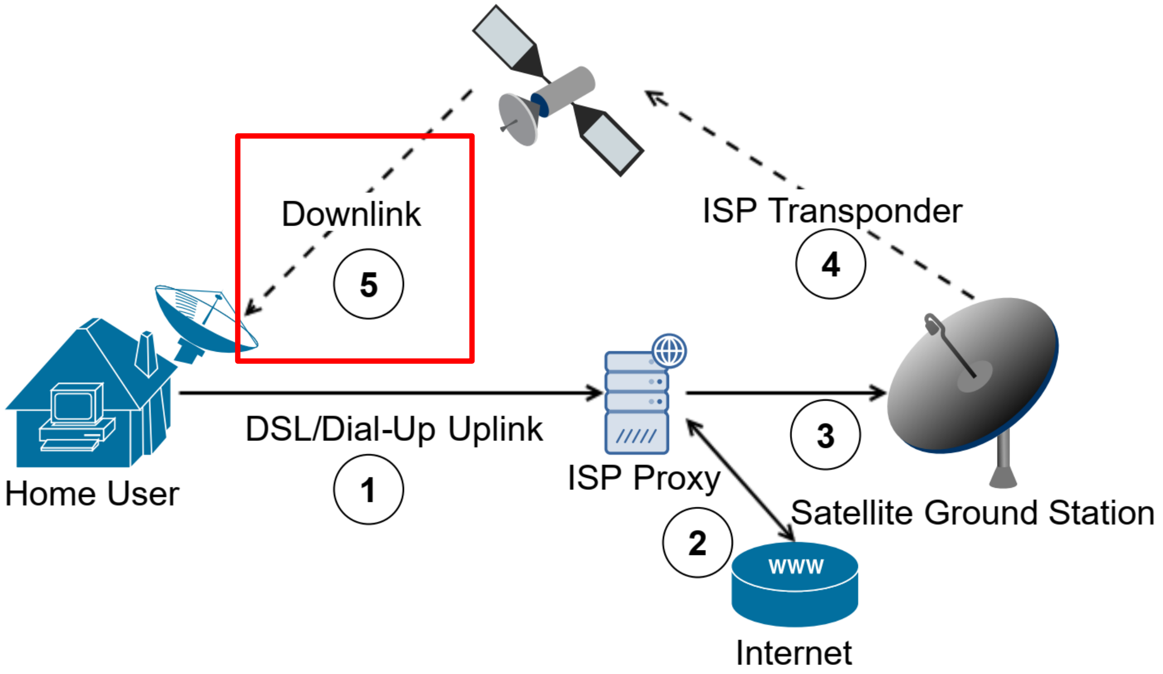
- Attack position 2: listening downlink-to-ISP



Threat Model

- For combined internet setup (uplink: terrestrial, downlink: satellite)

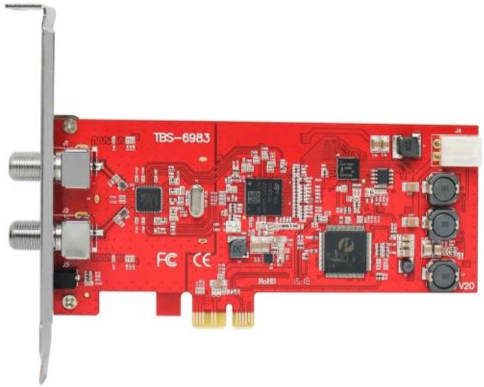
  -> only downlink-to-consumer (Position 1) available



Equipment

- Assumed single *low-resourced* malicious individual

Selfhat H30D Satellite Dish
€85



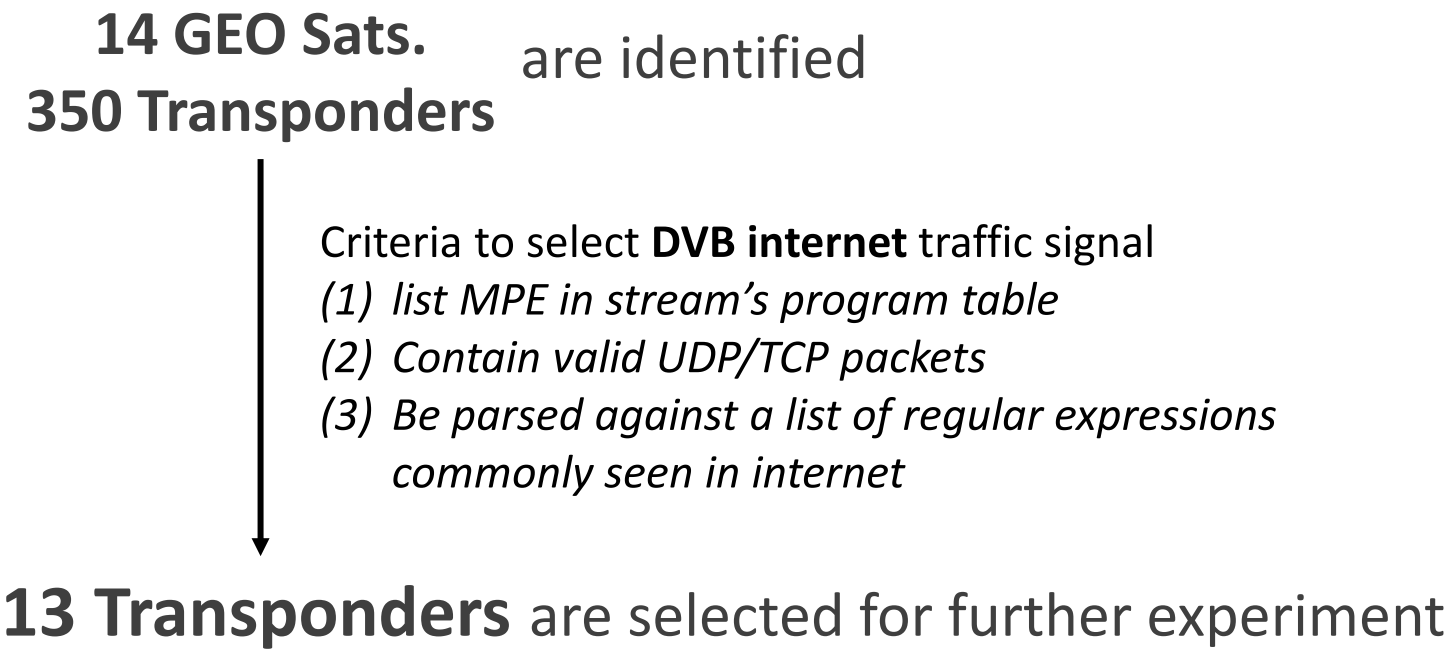
TBS 6983 Satellite PCI-E Card
€197

3 m Coaxial Cable
€3

Total cost of necessary equipment
= only **€285**!!

Deployment

- Locate 2 receivers in Europe (GEO in 40°E-37°W)



14 GEO Sats.
350 Transponders are identified

Criteria to select **DVB internet** traffic signal

(1) list MPE in stream's program table

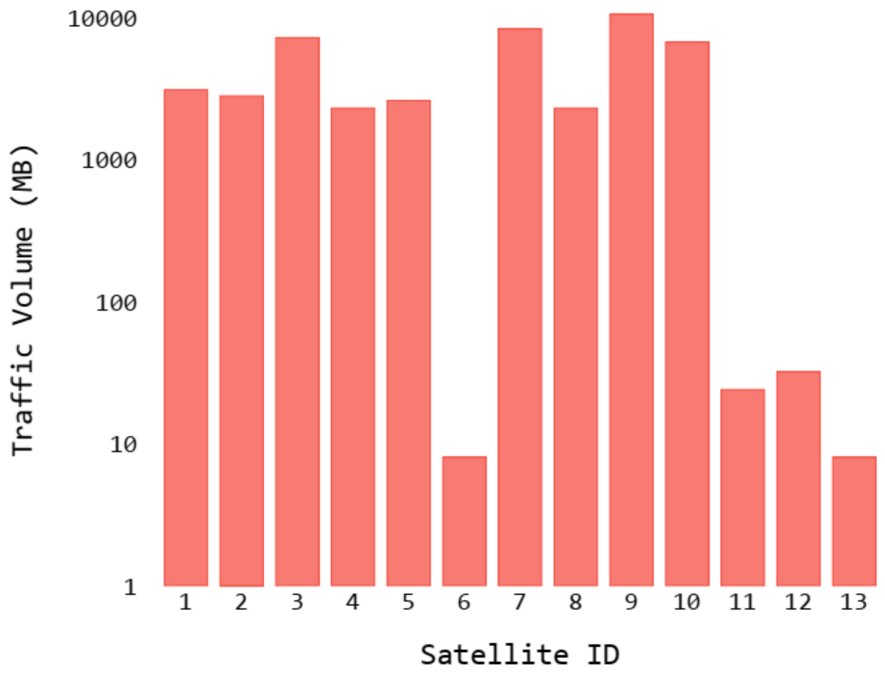
(2) Contain valid UDP/TCP packets

(3) Be parsed against a list of regular expressions commonly seen in internet

13 Transponders are selected for further experiment

Data Collection

- Recorded 5 hours traffic on 13 transponders
- Total 50 GB data
- Varied from 8 MB to 10 GB by transponders

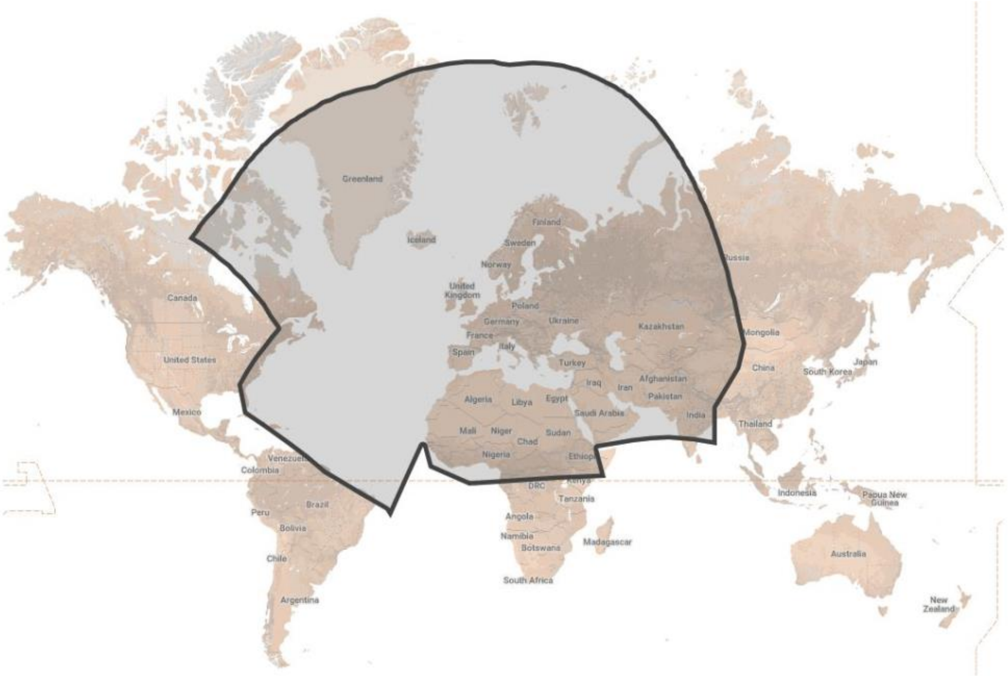


Result

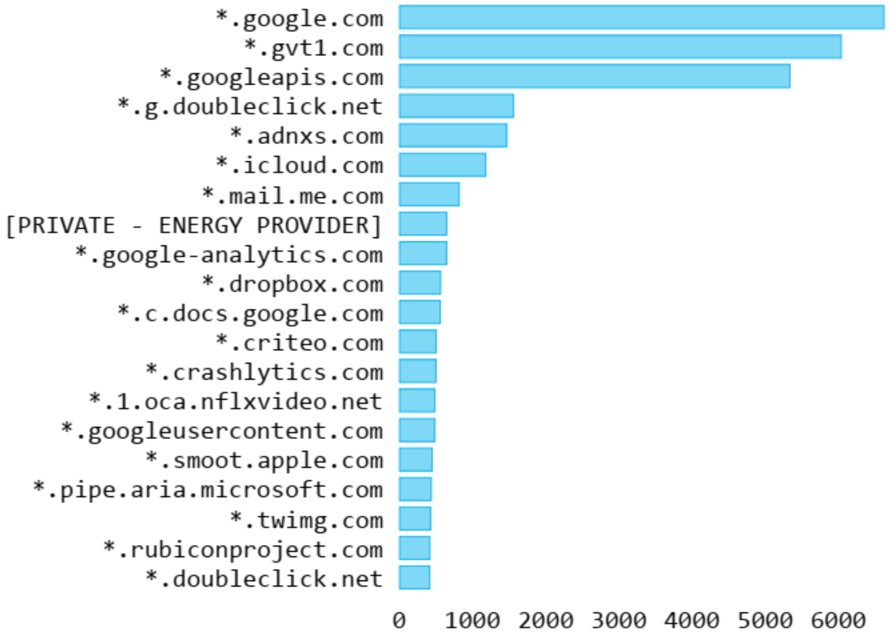
- Traffic was transmitted in ‘plaintext’

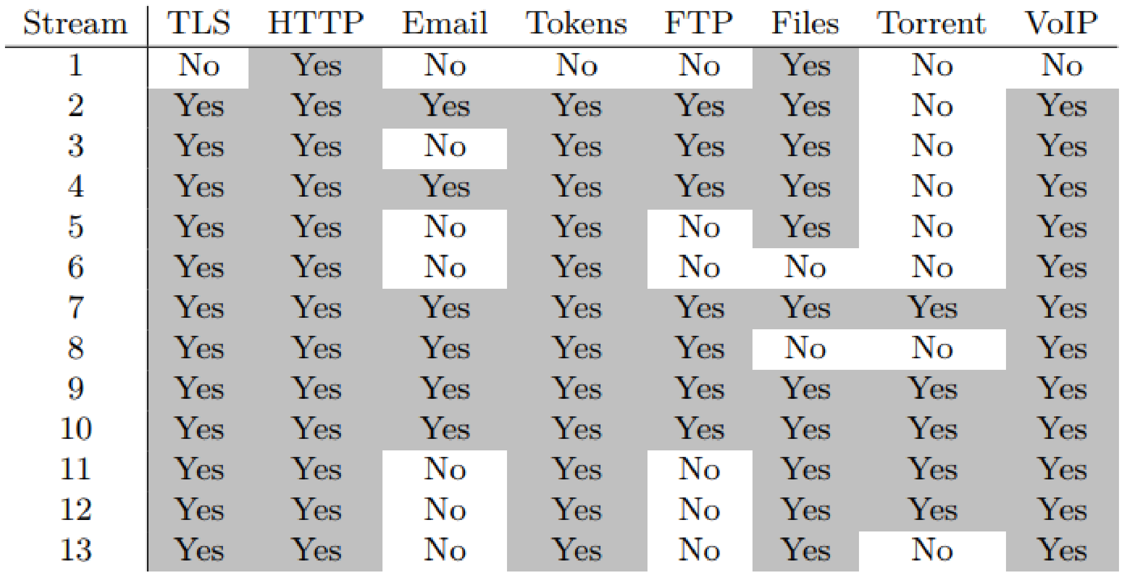
  -> potential eavesdropping

- Signal’s coverage footprint: 110m km^2



Result





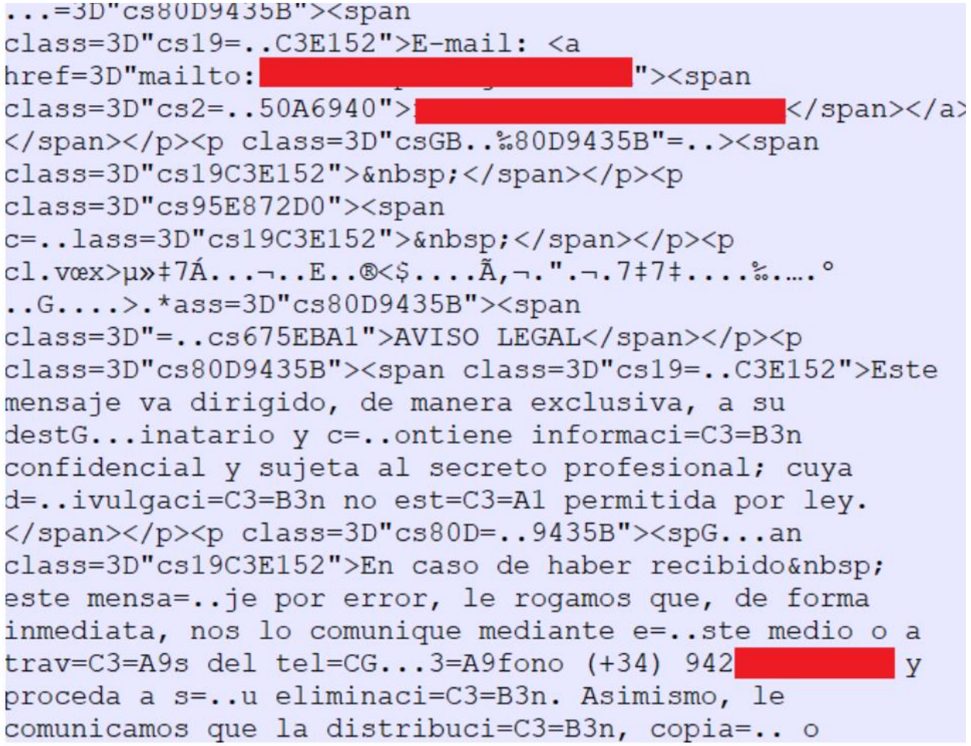
Stream	TLS	HTTP	Email	Tokens	FTP	Files	Torrent	VoIP
1	No	Yes	No	No	No	Yes	No	No
2	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
3	Yes	Yes	No	Yes	Yes	Yes	No	Yes
4	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
5	Yes	Yes	No	Yes	No	Yes	No	Yes
6	Yes	Yes	No	Yes	No	No	No	Yes
7	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8	Yes	Yes	Yes	Yes	Yes	No	No	Yes
9	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
11	Yes	Yes	No	Yes	No	Yes	Yes	Yes
12	Yes	Yes	No	Yes	No	Yes	Yes	Yes
13	Yes	Yes	No	Yes	No	Yes	No	Yes

- SSL/TLS certificates leakage
    - 52,000 SSL wildcard certificate from 1,200 domains

- Observed traffic contents

Result – Privacy Risk

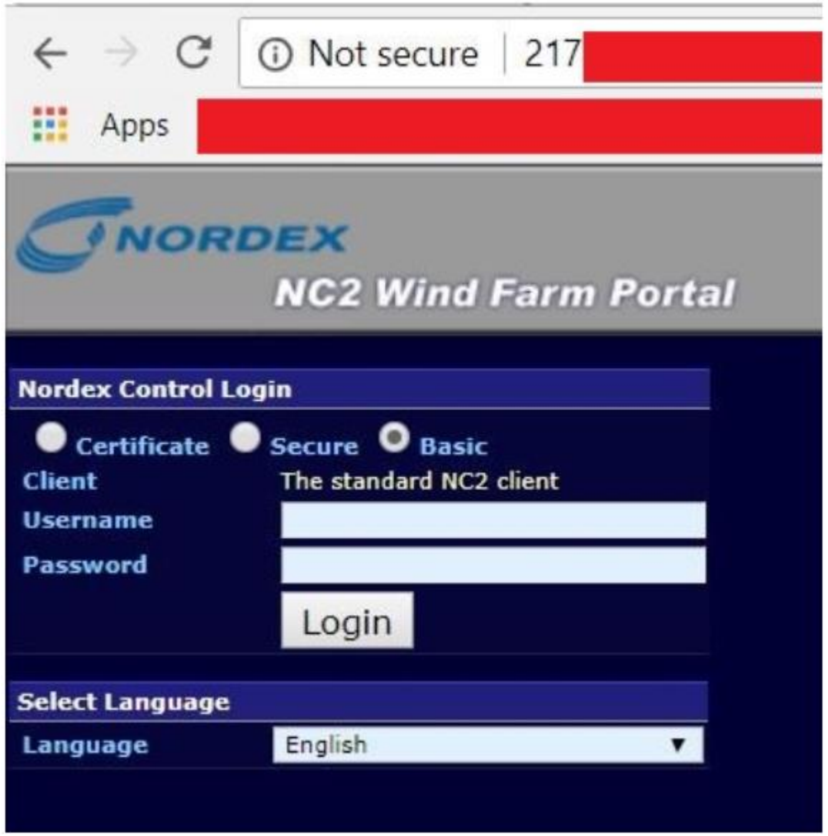
- Defense lawyer's confidential emails to client
- Connected iPhone to WiFi and sync over IMAP
- Able to know…
  - Full name
  - Phone number
  - Office/personal address
  - Job (defense lawyers)
  - Preparation of evidence for upcoming trial



```
...=3D"cs80D9435B"><span
class=3D"cs19=..C3E152">E-mail: <a
href=3D"mailto:[redacted]"><span
class=3D"cs2=..50A6940">[redacted]</span></a
</span></p><p class=3D"csGB..%80D9435B"=..><span
class=3D"cs19C3E152">&nbsp;</span></p><p
class=3D"cs95E872D0"><span
c=..lass=3D"cs19C3E152">&nbsp;</span></p><p
cl.vœx>µ»‡7Á...¬..E..®<$....Ã,¬.".¬.7‡7‡....‰.….°
..G....>.*ass=3D"cs80D9435B"><span
class=3D"=..cs675EBA1">AVISO LEGAL</span></p><p
class=3D"cs80D9435B"><span class=3D"cs19=..C3E152">Este
mensaje va dirigido, de manera exclusiva, a su
destG...inatario y c=..ontiene informaci=C3=B3n
confidencial y sujeta al secreto profesional; cuya
d=..ivulgaci=C3=B3n no est=C3=A1 permitida por ley.
</span></p><p class=3D"cs80D=..9435B"><spG...an
class=3D"cs19C3E152">En caso de haber recibido&nbsp;
este mensa=..je por error, le rogamos que, de forma
inmediata, nos lo comunique mediante e=..ste medio o a
trav=C3=A9s del tel=CG...3=A9fono (+34) 942[redacted] y
proceda a s=..u eliminaci=C3=B3n. Asimismo, le
comunicamos que la distribuci=C3=B3n, copia=.. o
```

Result – Infrastructure Security Risks

- Power plant
  - Unencrypted HTTP/FTP
  - Session token/cookies for authorization in plaintext
- Control traffic of automized factory
- Intranet credentials of national postal service



Not secure | 217[redacted]

Apps [redacted]

NORDEX

NC2 Wind Farm Portal

Nordex Control Login

○ Certificate ○ Secure ● Basic

Client	The standard NC2 client
Username	
Password	
	Login

Select Language

Language	English ▼

Potential Solution

Q: Encryption methods used on ground?

A: Satellite communication environment has…

- High latency (500ms for round-trip)
- Frequent packet loss
- Limited computing power

-> **Hard to apply on Sat. broadband**

Potential Solution

Q: “Scrambling” algorithms for TV networks?

- Cryptographic weakness
- All customers should share “master key”

Potential Solution

Q: Tunneling, end-to-end encryption (e.g., IPSec)

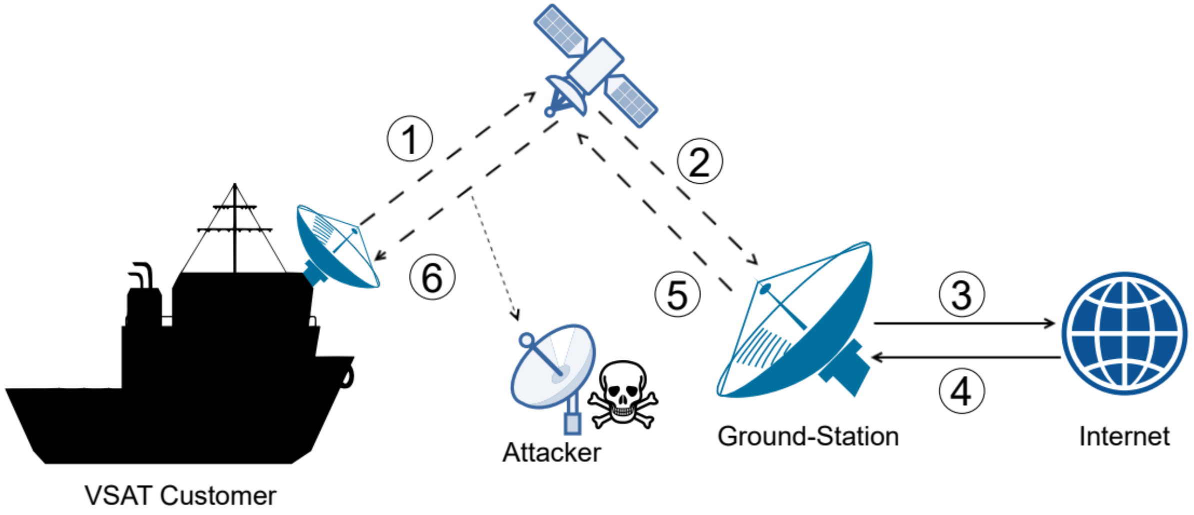
- Most realistic approach!
- Performance constraint problem…

  -> Connection acceleration techniques (e.g., PEP) could minimize!
- Prevent inspection of necessary packet headers…

Follow-up Study

Eavesdropping VSAT network (**J. Pavur**, et al. SP'20)

- Maritime VSAT (Very Small Aperture Terminal) network
- GEO-Sat, DVB-S2 based network
- Utilized same methodology

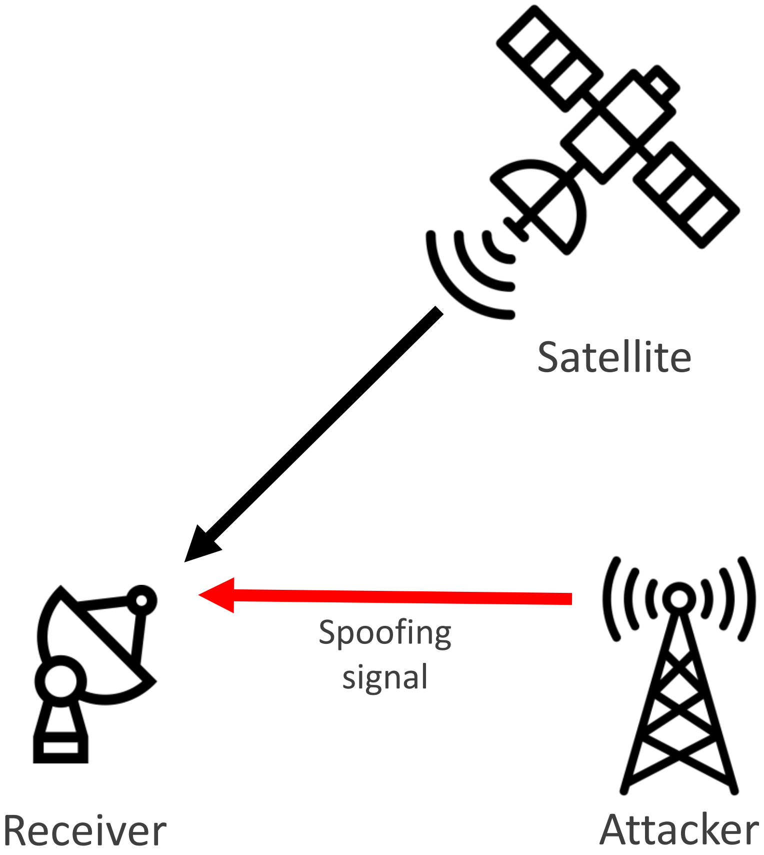


[1] J. Pavur, et al. A tale of sea and sky on the security of maritime VSAT communications. SP'20

Follow-up Study

Spoofing attack (E.Salkield, et al. WiSec'23)

- Feasibility of signal overshadowing
- Equipment under $2000
- Be able to attack at distances up to 1 km

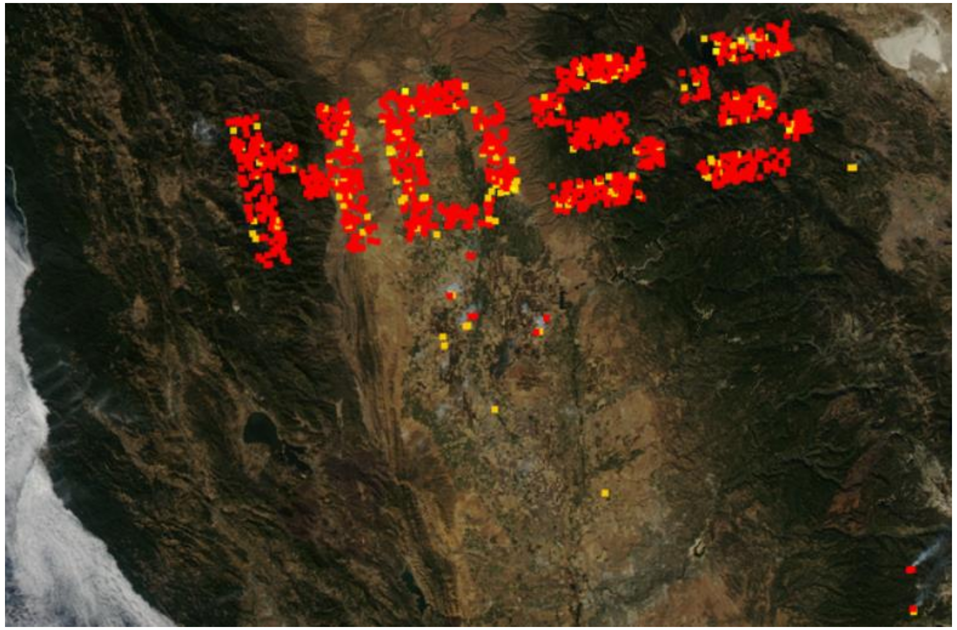


[2] E. Salkield, et al. Satellite spoofing from a to z: on the requirements of satellite downlink overshadowing attacks. WiSec'23

Follow-up Study

Spoofing attack on EO Sat. (E.Salkield, et al. NDSS'23)

- Application to Earth Observation Sat.
- FIRM: forest fire detection Sat. of NASA
- Inject malicious data

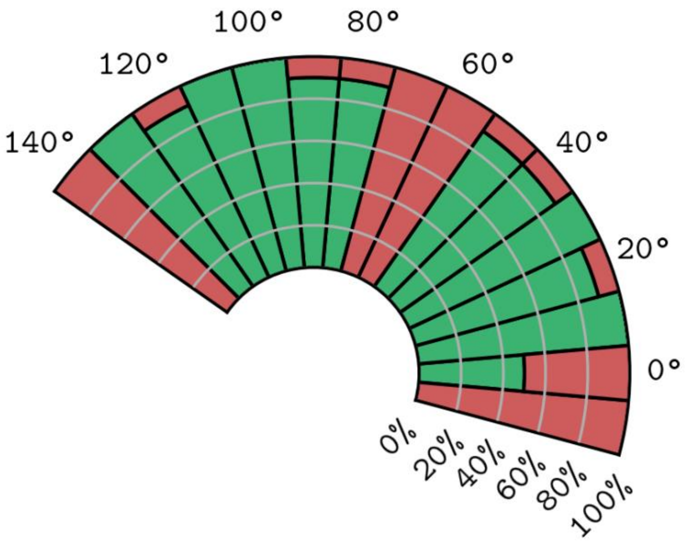


[3] E. Salkield, et al. Firefly: spoofing Earth observation satellite data through radio overshadowing. NDSS'23

Follow-up Study

Signal injection attack (R. Bisping, et al. USENIX sec'24)

- Target VSAT modem
- Disrupt operation, gain privileged access
- Analyzed channel condition



[4] R. BISPING, et al. Wireless Signal Injection Attacks on VSAT Satellite Modems. USENIX Security 24

Follow-up Study

QPEP encryption (**J. Pavur**, et al. NDSS'21)

- Hybrid of PEP & VPN, QUIC protocol based
- Performance: 72% faster then VPN, 54% faster than PEP
- Scalability: single-RT secure session
- Usability: doesn’t require modification to ISP infrastructure

[5] J. Pavur, et al. “QPEP: An Actionable Approach to Secure and Performant Broadband From Geostationary Orbit.” NDSS'21

Conclusion

Contribution

- Updated security assessment on DVB-S
- Analysis on various GEO satellite

Pros

- Identified real threats in the network.

Cons

- Explanation of the MPEG-TS packet structure was insufficient.
- Would be better if presented more severe attack scenario, beyond eavesdropping.

Thank you for listening!

Good Questions

- In what ways can Performance Enhancing Proxies (PEPs) be redesigned to support secure communications?
- Can we spoof unencrypted satellite communications like they did in the SigOver attack?
- What are the long-term implications of widespread adoption of satellite broadband on global cybersecurity policies, particularly in relation to critical infrastructure protection and international regulations?
- How would the implementation of encryption impact the latency and bandwidth efficiency of DVB-S networks, given their reliance on high-latency geostationary satellites?
- How do high latencies in satellite communication impact the adoption of encryption? For example, how does latency restrict key exchanges or handling large-scale traffic? Can you explain this in more detail?
- Considering the extensive deployment of DVB-S systems, what are the practical challenges in retrofitting existing infrastructure to support data link layer encryption?

Best Questions

- **Changgun Kang**

  Considering that this paper was published in 2019, it seems that there are too many basic security vulnerabilities (such as simply being unencrypted). In your opinion, why do satellite communications seem to be more vulnerable than the wired communication we use?

- **Isu Kim**

  While both traditional satellite systems and StarLink share similar ground station uplink/downlink vulnerabilities, StarLink introduces additional attack surfaces through its inter-satellite links (ISL). How do you think these additional ISL connections between multiple satellites impact the overall security compared to traditional single-satellite architectures?

- **Boris Testud**

  Can high density satellite constellations like Starlink improve the reliability of transmissions, therefore allowing for the use of conventional encryption algorithms on satellite communications? (more satellites = less clients per satellite = more computing power for encryption)