CYD | CYBER DEFENCE CAMPUS

ETH zürich

RUHR UNIVERSITÄT BOCHUM

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse

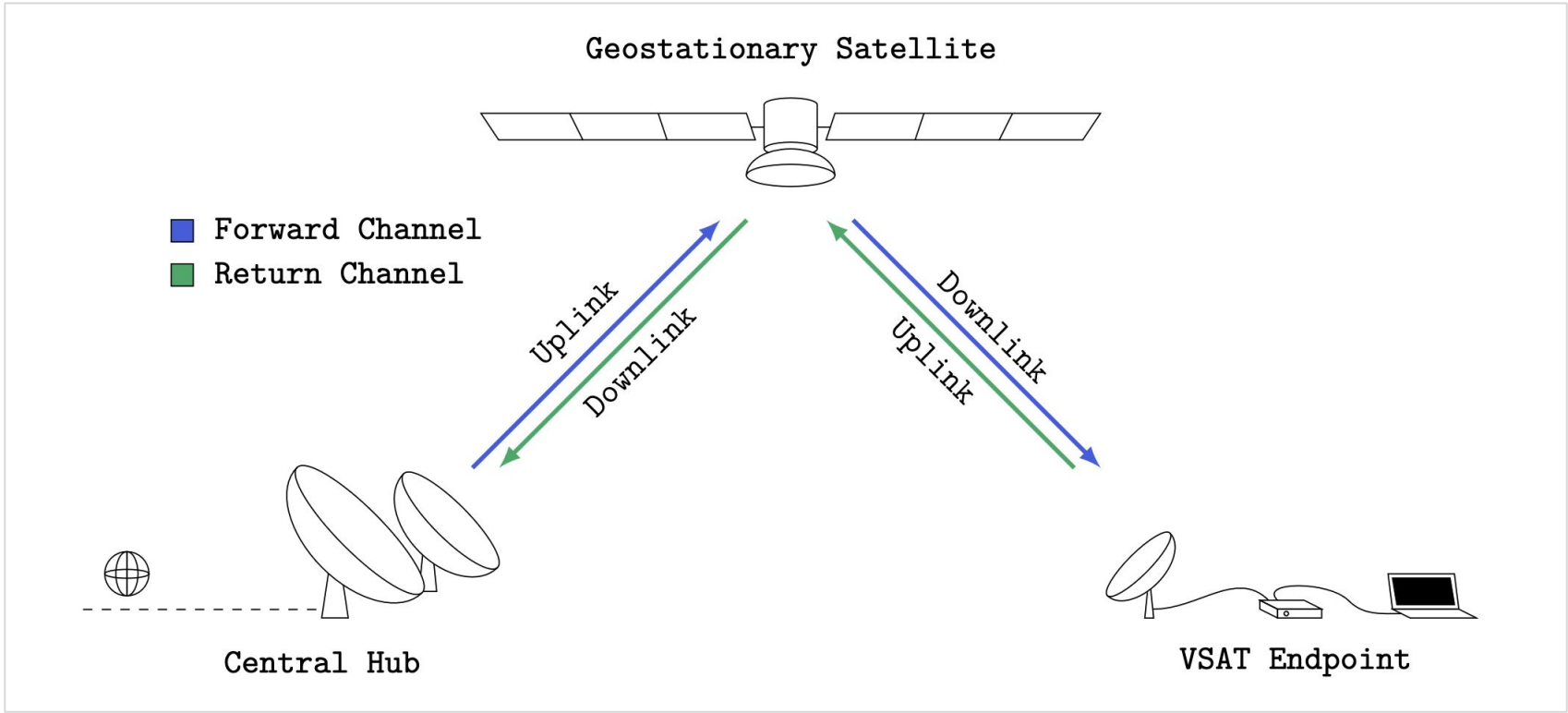
Wireless Signal Injection Attacks on VSAT Satellite Modems

Robin Bisping, Johannes Willbold,
Martin Strohmeier, Vincent Lenders

USENIX Security ‘24, Philadelphia

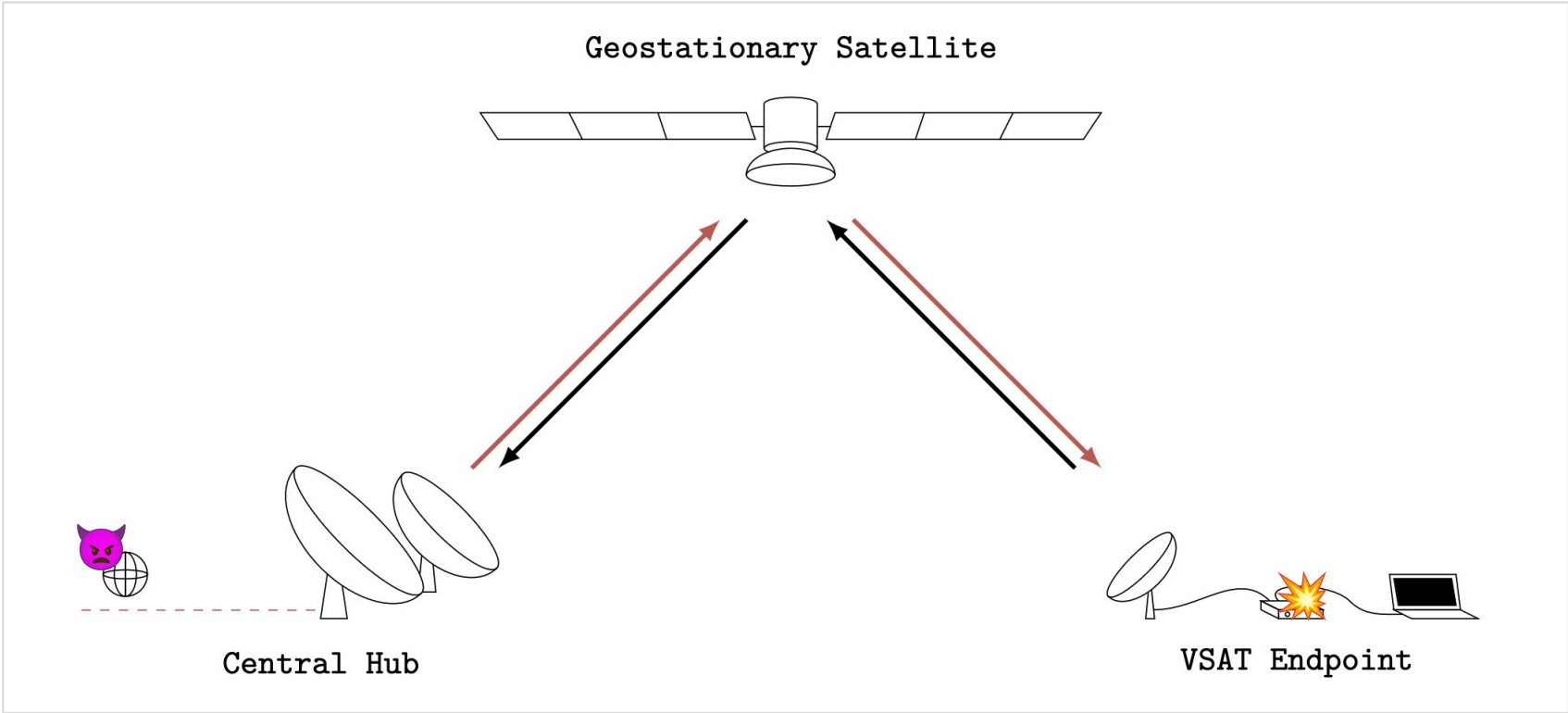
Ben Wicks / Unsplash

Background
VSAT Satellite Communication Systems

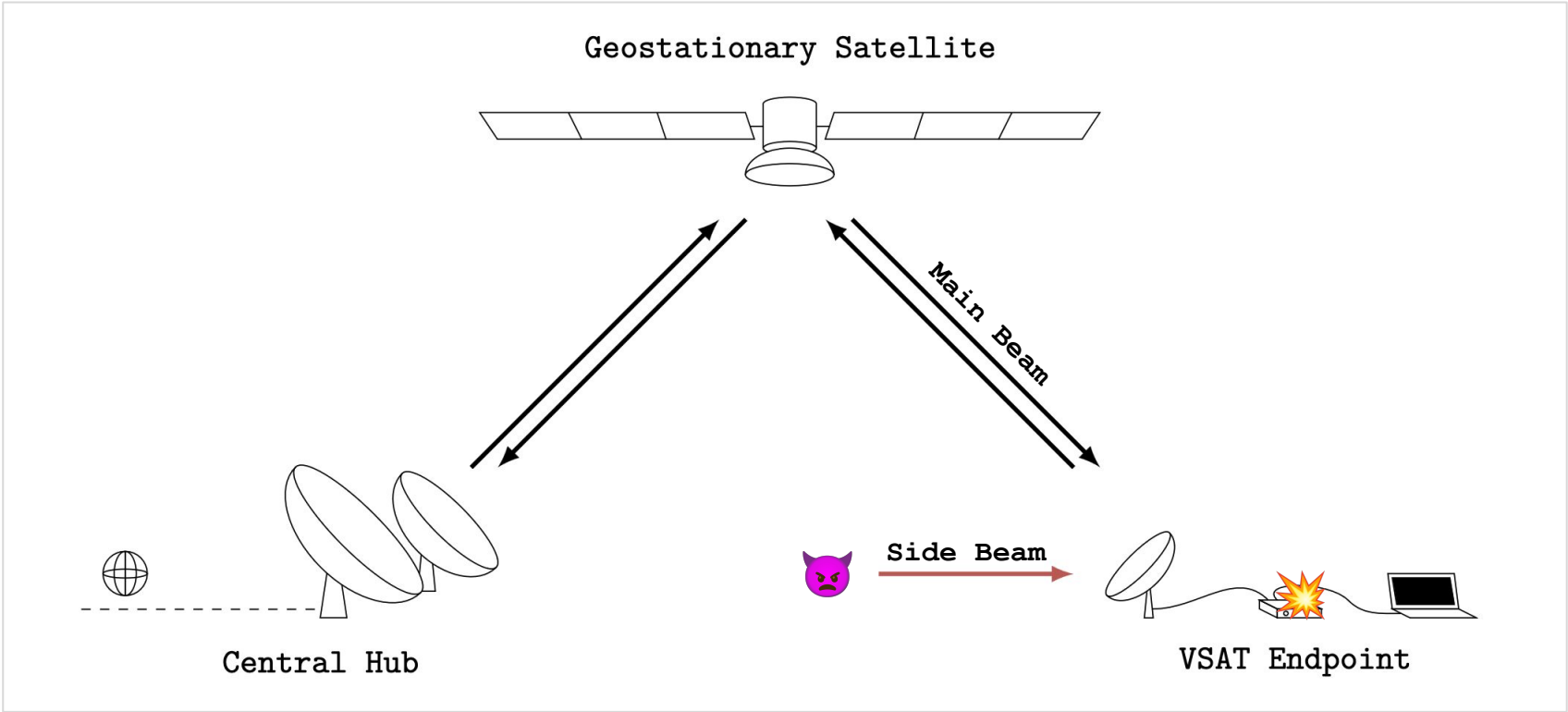



Businessweek
The Satellite Hack Everyone Is Finally Talking About
As Putin began his invasion of Ukraine, a network used throughout Europe—and by the Ukrainian military—faced an unprecedented cyberattack that doubled as an industrywide wake-up call.
By Katrina Manson
Illustrations by Jordan Speer
1 March 2023 at 00:01 GMT+1
https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/

Attack Scenarios
Attacking Central Hubs



Attack Scenarios
Attacking VSAT Endpoints



Research Question

How are VSAT satellite modems susceptible to side beam signal injection attacks?

Attacker Model

Knowledge 📖

- Knowledge of the modem's communication stack and applications

Transmission capabilities 📡

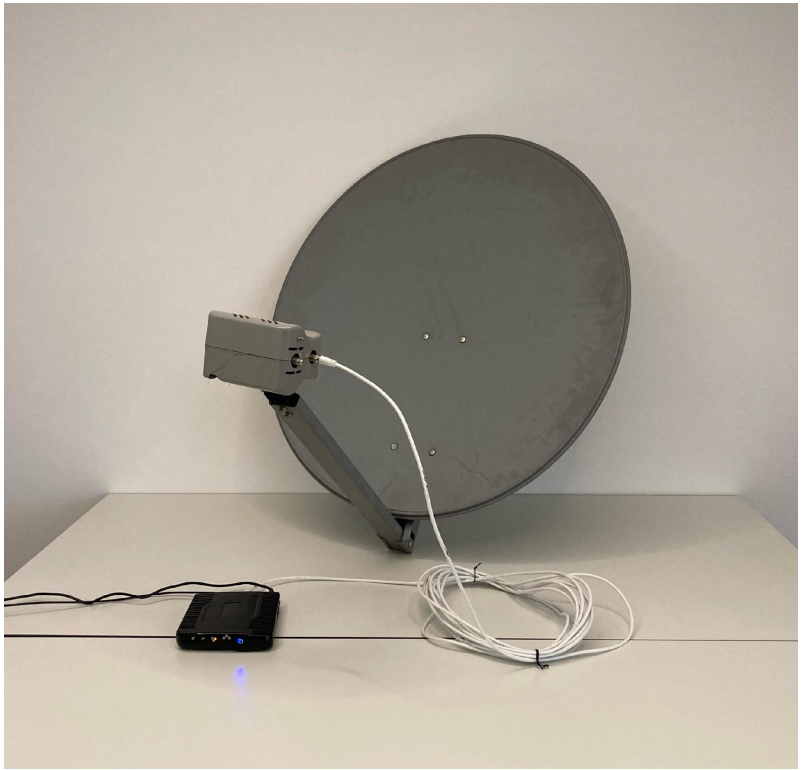
- SDR-based transmission on the forward channel
- Ability to upconvert to satellite frequencies (Ku- and Ka-band)

Line-of-sight 🔭

- **No physical access to modem**
- Line-of-sight to the modem, but outside of the main beam

https://pxhere.com/en/photo/1290044

Case Study
Newtec MDM2200



Centers of Excellence in the U.S., Belgium & Singapore serve the unique needs of each region

5000 hubs deployed supporting over half million modems

#1 Ranking in maritime market – trusted by **8 of the 9 leading service providers** – connecting seafarers and vessels worldwide amongst cruise, oil and gas, commercial shipping and fishing industries

#1 Ranking in aero with 44% market share – linking thousands of passengers, cockpit and ground support crew across **3,000+ commercial planes and business jets**

#1 Ranking in media and broadcast market – enhancing live broadcast capabilities for more than 5 years, enabling more than **3 billion people to watch TV every day**

Leading the digital transformation of the ground segment through strategic partnership with Microsoft Azure and the DIFI consortium

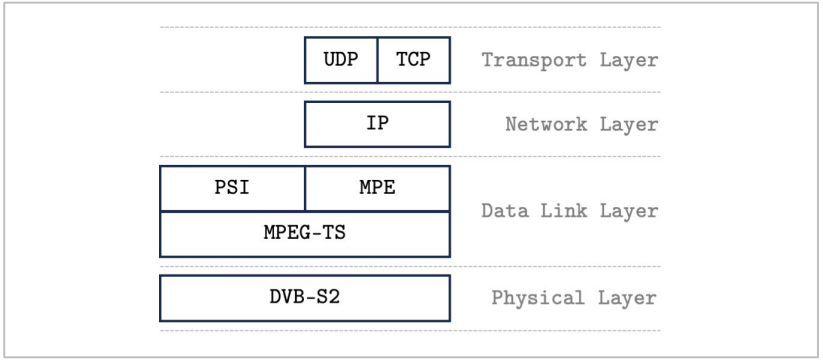
Leading industry collaboration and unified standardization to enable the integration of **5G over satellite**

Global leader in government and defense – **#1 ranking in U.S. DoD VSAT** and relied on by 21 of 28 EU nations and 19 of 29 NATO member states

https://www.idirect.net/wp-content/uploads/2020/01/2022-Corporate-Factsheet-US.pdf

Case Study
DVB-RCS / Sat3Play

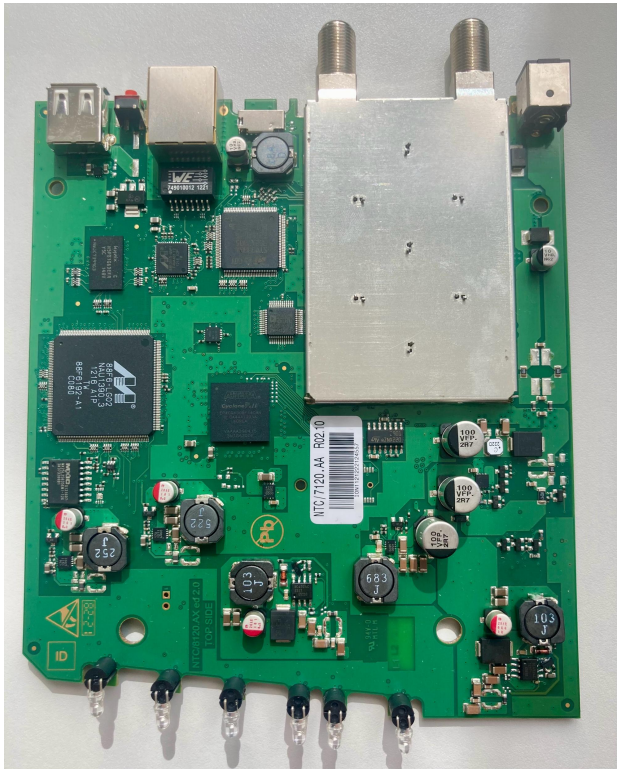
DVB-RCS provides a **standardized framework for satellite communication**.

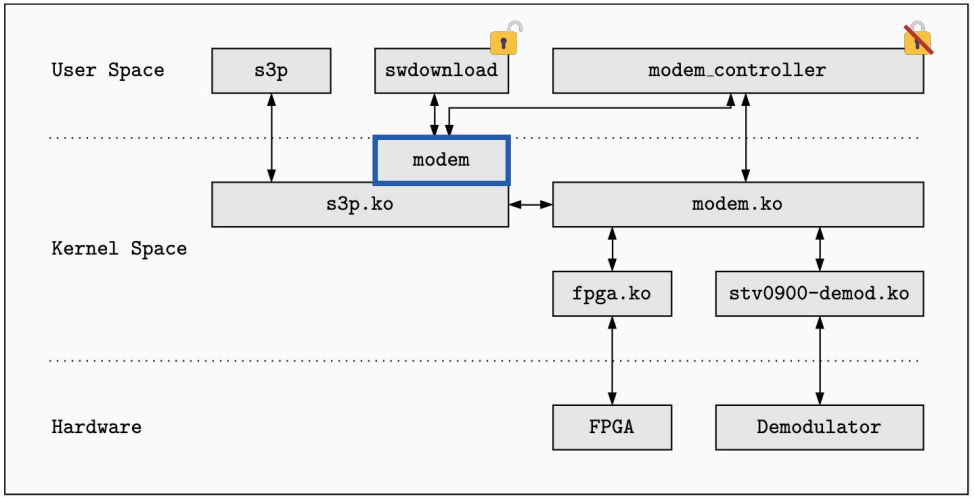


S3P is Newtec's **proprietary implementation of DVB-RCS**.

- It deviates from DVB-RCS in some respects.
- **Encryption is optional** and not enforced.

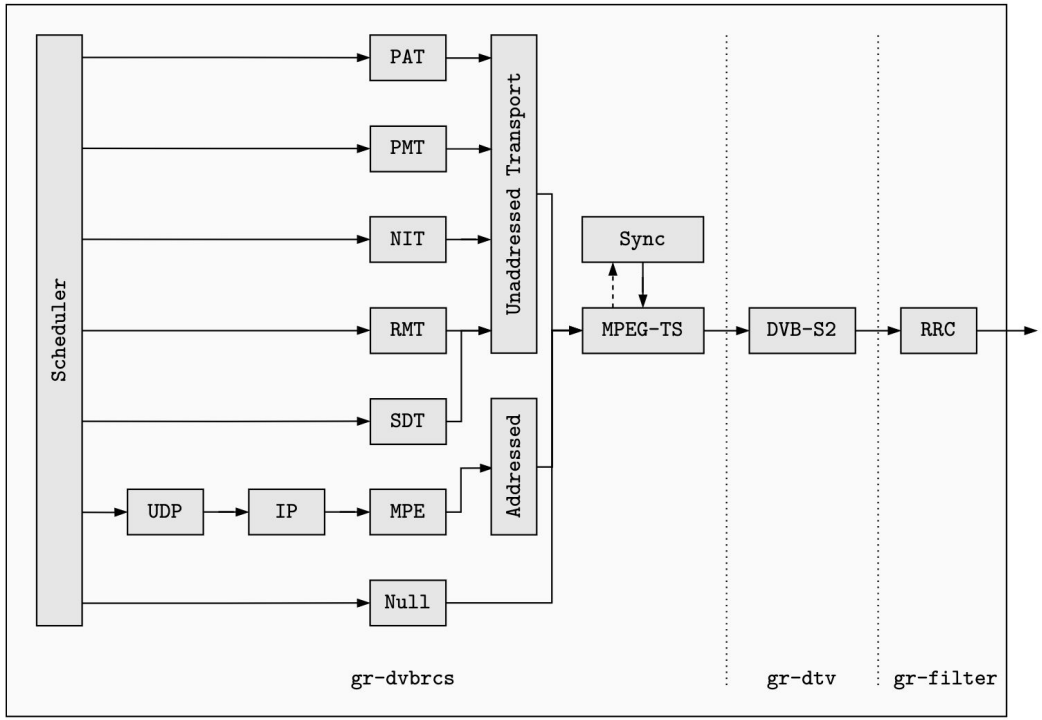
Case Study
Newtec MDM2200





- The modem abstracts the signal processing behind a **network interface**, which accepts all incoming traffic.
- There is **no coordinated approach to security**. Management applications apply unencrypted and unauthenticated instructions.

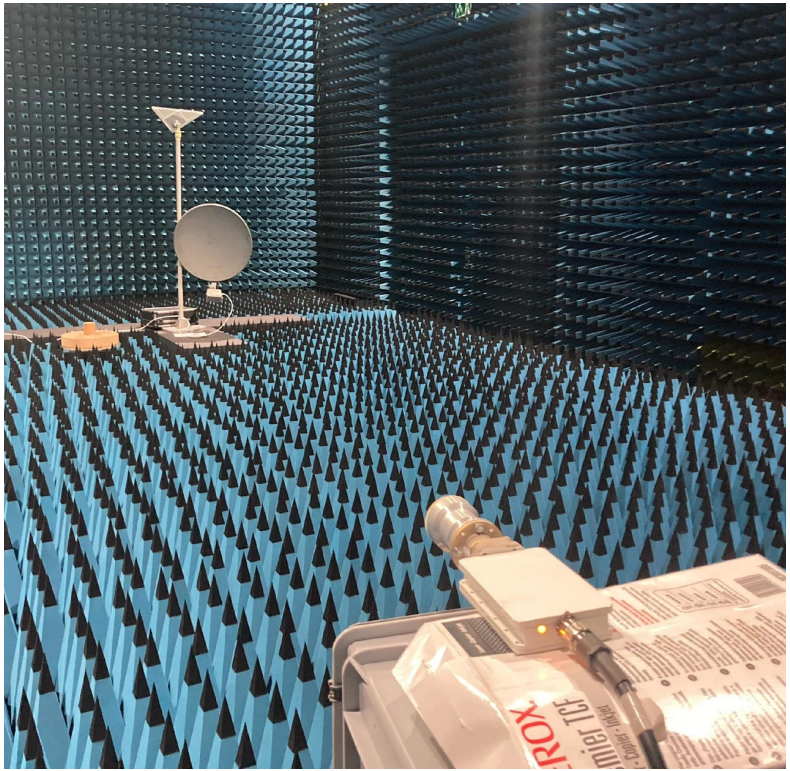
Implementation
Transmitter

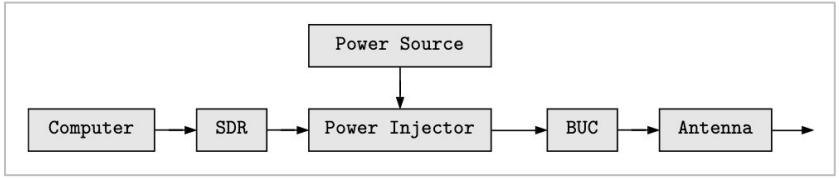


- GNU Radio based implementation of only the **forward channel**.

✓ Our implementation allows us to **inject arbitrary IP packets** into the modem's network stack.

Implementation
Hardware Setup





- Software-defined Radio:
  Ettus Research USRP B200
- Power Injector:
  UMT-TV BUC-Ku002-10.6 v2.0
- Block Upconverter:
  UMT-TV DC Injector IDCI with IP Ctrl
- Antenna:
  UMT-TV Offset Feed

~ $2000

Attack 1
Connection Reset

- We emit a **jamming signal** consisting of random noise at the same frequency as the forward channel.

✓ Because the modem is no longer able to receive the synchronization packets, the **modem restarts the channel initialization process**.

Attack 2
Malicious Firmware Update

- We emit a signal, containing a packet indicating that an update is available, followed by malicious firmware update packets.
- Both packet types are **neither authenticated nor encrypted**.

```
Jan 1 00:00:38 S3P user.info swdownload[396]: All data received
Jan 1 00:00:38 S3P user.info swdownload[396]: All packets received
Jan 1 00:00:38 S3P user.info swdownload[396]: SW download finished
Jan 1 00:00:38 S3P user.err  swdownload[396]: CRC on the header was not correct!
Jan 1 00:00:38 S3P user.err  swdownload[396]: - Calculated=1972200246, expected=0n
Jan 1 00:00:38 S3P user.info swdownload[396]: CRC not correct!
```

✓ The modem confirms the **successful firmware reception**.

✓ Allows an attacker to **overwrite the firmware**.

Attack 3
Remote Code Execution

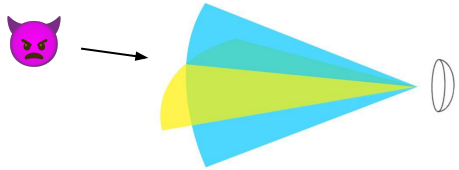
- We emit a signal that contains an **exploit of a buffer overflow vulnerability**.

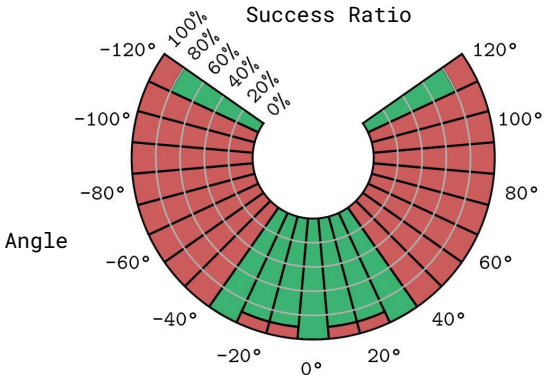
✓ We were able to execute commands with visibly verifiable results, for example by **turning on an LED**.

✓ We were able to open a **reverse shell to a host in the LAN**.

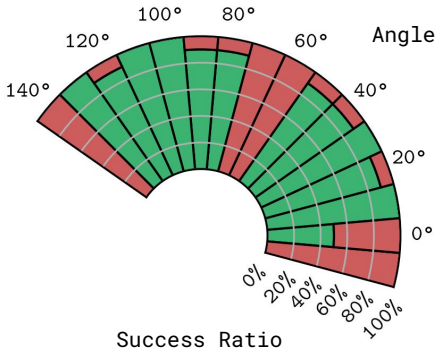
Evaluation
Sidelobe Injection

TX power: 9.5dBm
Environment: Anechoic





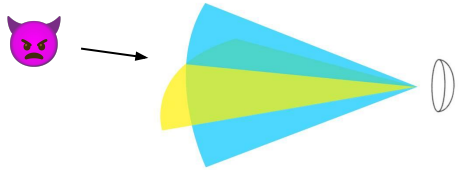
Horizontal plane
(yellow)

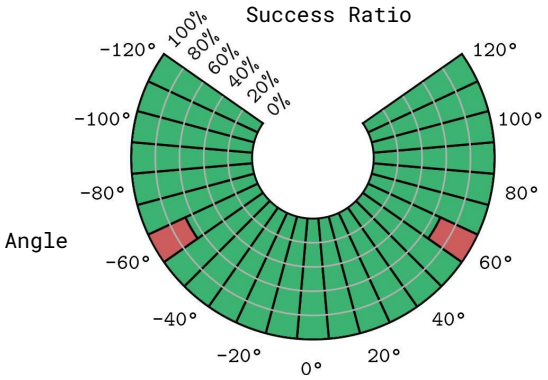


Vertical plane
(blue)

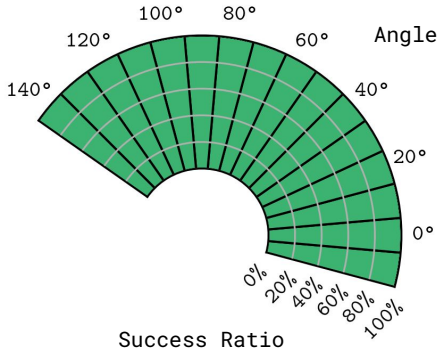
Evaluation
Sidelobe Injection

TX power: 9.5dBm
Environment: Multipath





Horizontal plane
(yellow)



Vertical plane
(blue)

Conclusion
Real-World Impact

- Attacks are expected to be effective on other modems utilizing **Sat3Play**.
- We believe the results of this study can be adapted to devices from other vendors based on **DVB-RCS** (e.g., Viasat, Hughes, Advantech, and Satlink).
- These solutions are estimated to hold a **10-20%** market share out of millions of deployed VSAT terminals.

Conclusion
Research Contributions

- We **reverse engineered the communication** stack of the Newtec MDM2200 modem.
- We implemented an **SDR attacker** with a budget of **$2000**.
- We demonstrated **three wireless attacks**:
  - Resetting the connection
  - Injecting malicious firmware updates
  - Obtaining a remote admin shell
- We found that signal injection attacks can be **successful from angles other than directly in front of the antenna**.
- We discussed the real-world impact and **potential mitigations**.

Robin Bisping, robin@bisping.ch
Johannes Willbold, johannes.willbold@rub.de
Martin Strohmeier, martin.strohmeier@armasuisse.ch
Vincent Lenders, vincent.lenders@armasuisse.ch

https://www.usenix.org/conference/usenixsecurity24/presentation/bisping