流量加密也沒用？
以阻斷攻擊拿下整片衛星RCE

Shenghao Ma, Team Lead
Jair Chen, Sr. Threat Researcher
PSIRT and Threat Research, TXOne Networks Inc.

April 22, 2025 @CYBERSEC 2025

TXOne Threat Researchers from TW

Team Lead, PSIRT and Threat Research at TXOne Networks Inc.

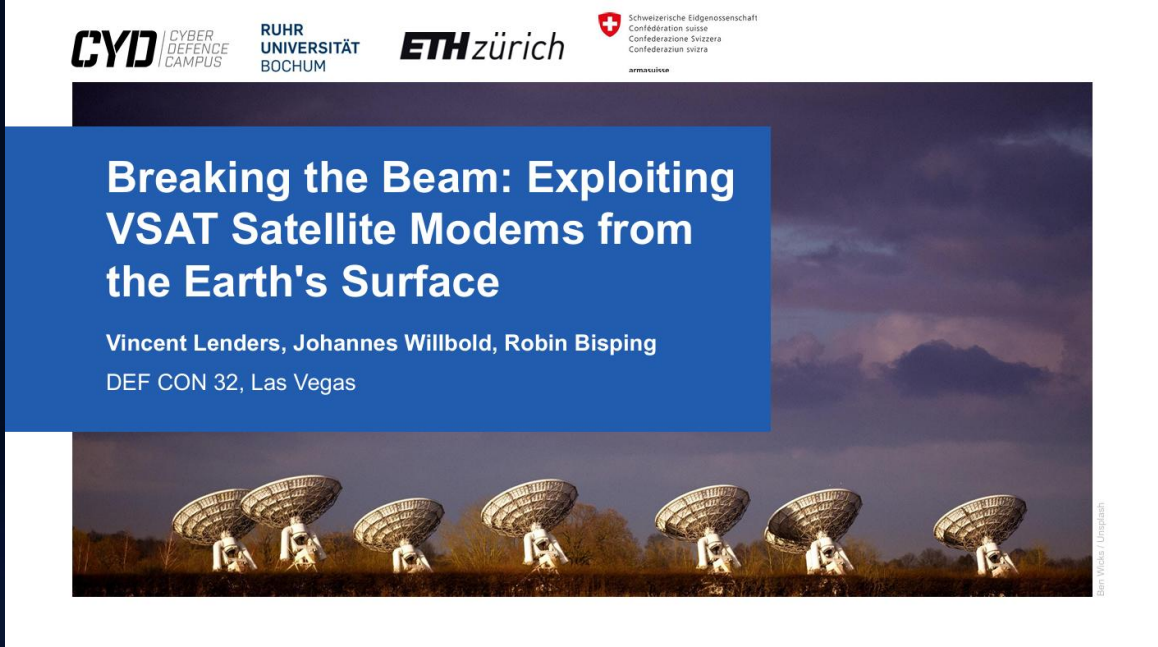
- Sheng-Hao Ma (@aaaddress1) is a team lead of TXOne Networks PSIRT and threat research team, responsible for coordinating product security and threat research. With over 15 years of expertise in reverse engineering, symbolic execution, malware analysis, and machine-learning, he is also part of CHROOT, a cybersecurity community in Taiwan.
- As a frequent speaker, trainer, and instructor, Sheng-Hao has contributed to numerous international conferences and organizations, including Black Hat USA, DEFCON, CODE BLUE, S4, SECTOR, HITB, VXCON, HITCON, and ROOTCON, as well as the Ministry of National Defense and the Ministry of Education. He is the author of "Windows APT Warfare: The Definitive Guide for Malware Researchers," a well-regarded cybersecurity book about reverse engineering of Windows.

Sr. Threat Researcher, PSIRT and Threat Research at TXOne Networks Inc.

- Jair Chen is a senior threat researcher of TXOne Networks PSIRT and Threat Research team. He specializes in building threat intelligence systems and tracking potential attack organizations as well as emerging attack techniques.
- Jair’s research spans the detection and defense against malicious behaviors in virtualization environments, on-premises systems, and cloud environments. Jair has developed an enterprise-grade APT behavior analysis engine that uncovers hidden hacker attacks by correlating suspicious behaviors across multiple dimensions.

Outline

- 通訊加密即安全？那可未必 - 當通訊韌性的先天寬鬆面臨真實攻擊
- 當抗雜訊產品顧慮成為攻擊破口？民用射頻裝置低成本達成阻斷攻擊
- 零知識狀態下行鏈路蓋台攻擊成為新前沿攻擊潮流
- 緩解措施與應對方案



txOne networks

加密即安全通訊？

那可未必 - 當通訊韌性的先天寬鬆面臨真實攻擊

Businessweek

The Satellite Hack Everyone Is Finally Talking About

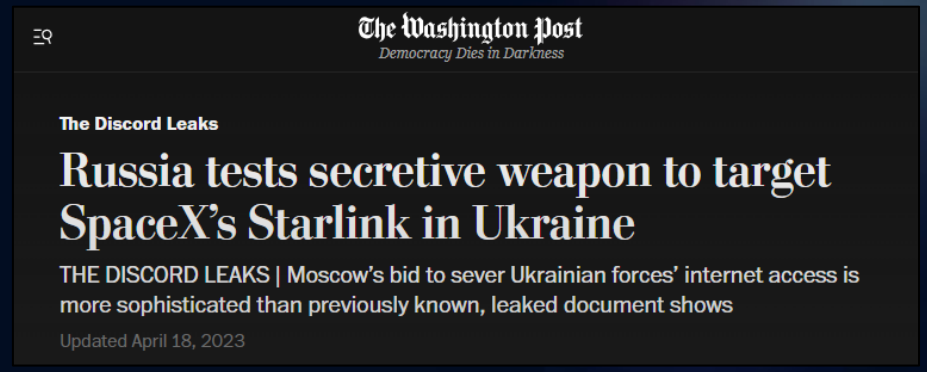
As Putin began his invasion of Ukraine, a network used throughout Europe—and by the Ukrainian military—faced an unprecedented cyberattack that doubled as an industrywide wake-up call.

By Katrina Manson
Illustrations by Jordan Speer

www.bloomberg.com/features/2023-russia-viasat-hack-ukraine

On the Ground Space Jam of Uplink

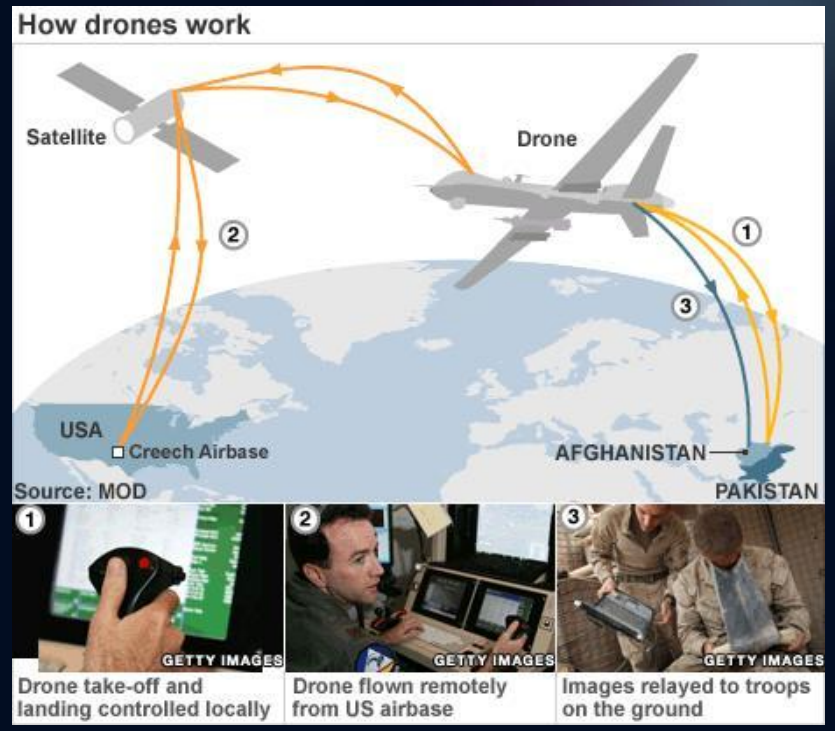
- **Russian Tobol-1: Space Jam Weapon**
  - *"The public documentation that we have talks about it being a defensive system, in that Tobol would be used to detect somebody else trying to jam or interfere with Russian satellites."*
  - *"It would analyze those interfering signals (Starlink)* ***and then broadcast a counter-signal that would try to negate the interference****"* director of the Secure World Foundation, Brian Weeden said.
- **(2023 IEEE S&P) "Space Odyssey" by CISPA**
  - Custom Ground Station ~ $10K
  - AWS Ground Station ~ $22 /min

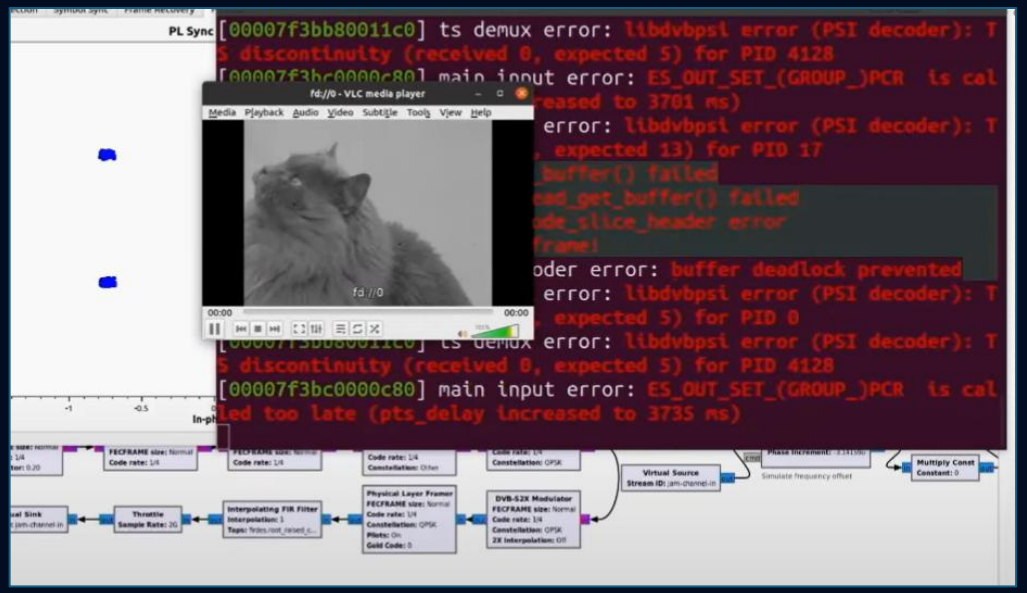


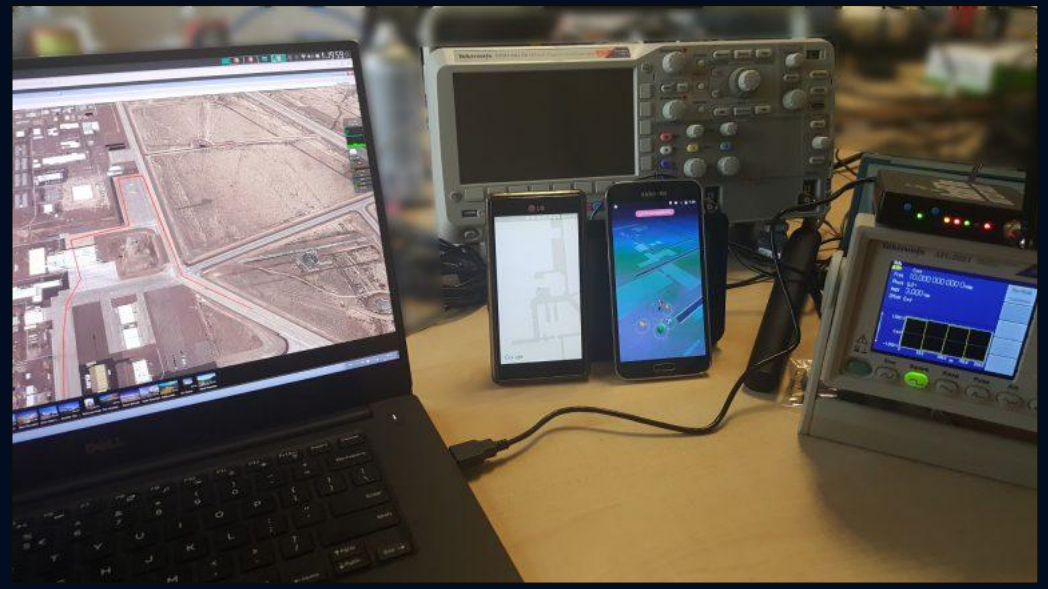
Ref: Willbold, Johannes, et al. "Space odyssey: An experimental software security analysis of satellites." 2023 IEEE Symposium on Security and Privacy (SP). IEEE, 2023.

SDR: Cheaper but Powerful. Possible?

- **(2011) BBC: Researchers use spoofing to 'hack' into a flying drone**
- **(2022) DVB-S2 Satellite Signal Hijacking on the Ground**
  - The U.S. Dept of Defense's Repo: github.com/deptofdefense/dc30-space-jam
- **Simple & Cheap even for None-National Hackers**
  - SDR hackers playing Pokémon Go with forged GPS
  - Affordable equipment: HackRF







Key Challenge: Off-the-shelf SDR Spoofing (1/2)

- 現存仍難以有個好的學術模型採用廉價射頻裝置對衛星級地面裝置攻擊
  - *“Despite these concerns, no current academic work has considered the feasibility of performing spoofing attacks on real world satellite downlink systems other than GNSS. Results from these attacks, which target cheap omnidirectional antennas in end-user devices designed to distinguish satellites on a shared channel, do not apply to other systems such as dedicated space-to-ground datalinks.”*
  - *“Rather, attacking these systems requires overshadowing a legitimate signal using a protocol not designed for multiple access, at a frequency not readily accessible with off-the-shelf hardware, and received by a large and highly directional antenna, potentially within a security perimeter. The wide variety of receiver systems have previously made presenting a detailed threat model difficult, as the attacker’s constraints are “strongly tied with the goals and security requirements of the target mission””*

Ref: Salkield, Edd, et al. "Satellite spoofing from a to z: on the requirements of satellite downlink overshadowing attacks." Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2023.

Key Challenge: Zero Knowledge Context (2/2)

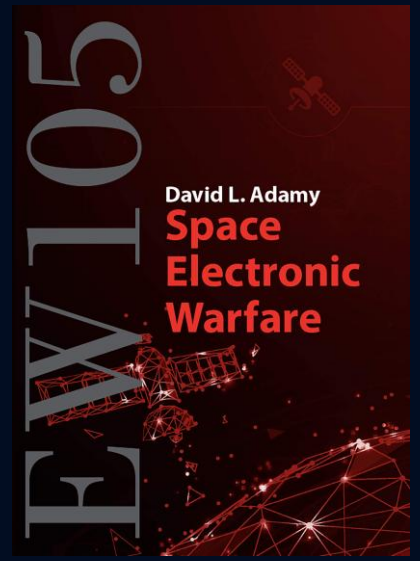
- 攻擊者的零前後文知識背景知識狀態難題（Zero Knowledge Context）
  - 在牛津大學此份研究中提出了在啟用端點加密的商用衛星通訊流量下進行 jamming Attack 具有攻擊者的零知識狀態難題，難以進行傳統的密碼學攻擊於既有存在的加密端點連線。
  - *“There are some known attacks on terrestrial systems which more closely match the satellite spoofing scenario, particularly in cellular networks. The AdaptOver attack system demonstrates the use of overshadowing on LTE to achieve arbitrary message injection, persistent denial of service, and leaking sensitive information for the LTE and 5G-NSA protocols”*
  - *“Additionally, the SigOverand SigUnder attacks demonstrate overshadowing attacks on LTE with a significantly reduced power budget. This is achieved by synchronizing with the carrier signal and taking advantage of error correcting codes present in the protocol, and by exploiting knowledge of the underlying data to flip individual bits in the signal rather than overshadowing the entire message. We build upon this work in Section 5, assessing these techniques in a zero-knowledge context (i.e. the message is not known and cannot be exploited to flip individual bits), with the added difficulty of **overshadowing signals on a highly directional dish**”*

Ref: Salkield, Edd, et al. "Satellite spoofing from a to z: on the requirements of satellite downlink overshadowing attacks." Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2023.

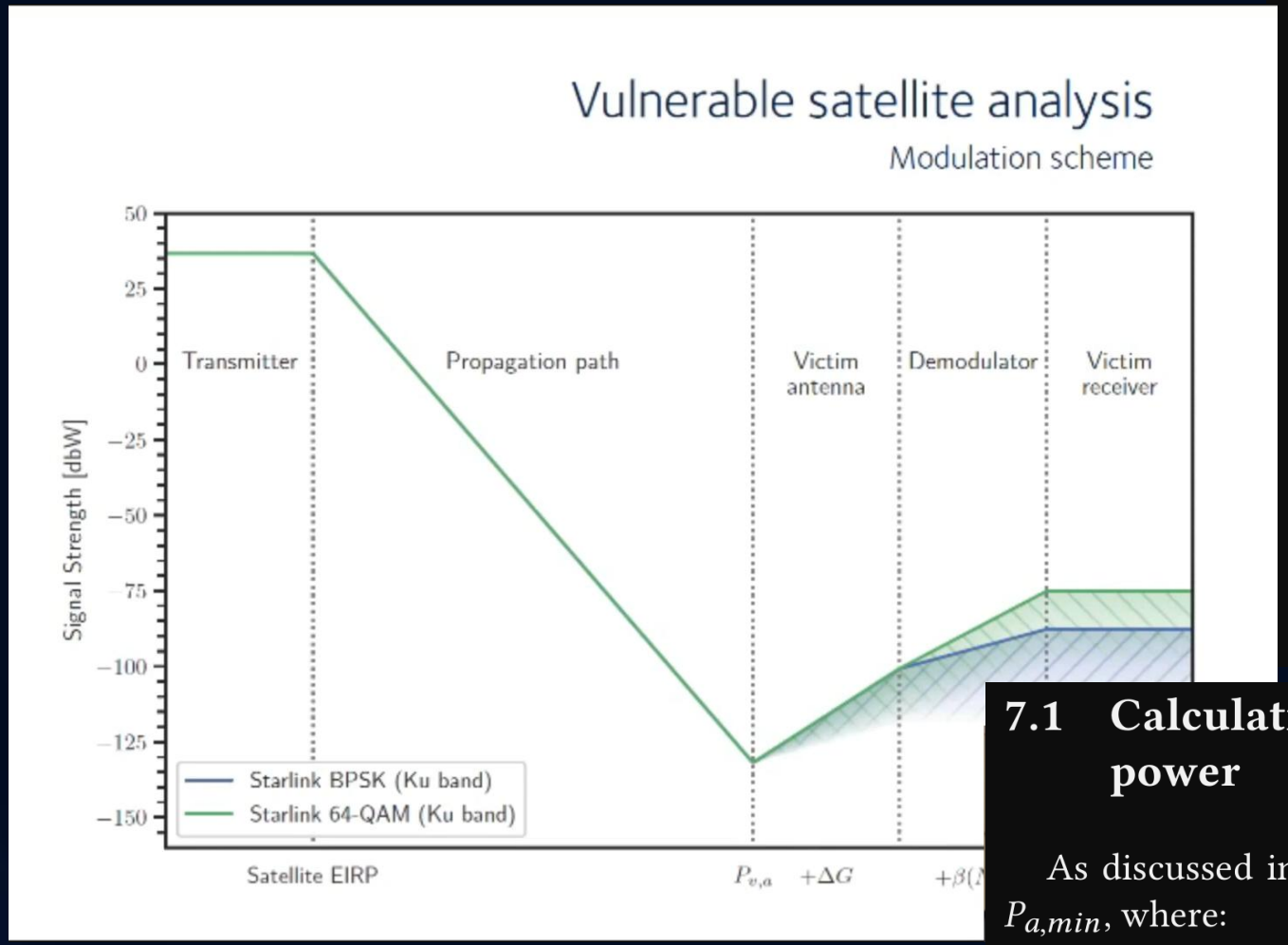
Challenge A
Off-the-shelf SDR Overshadowing

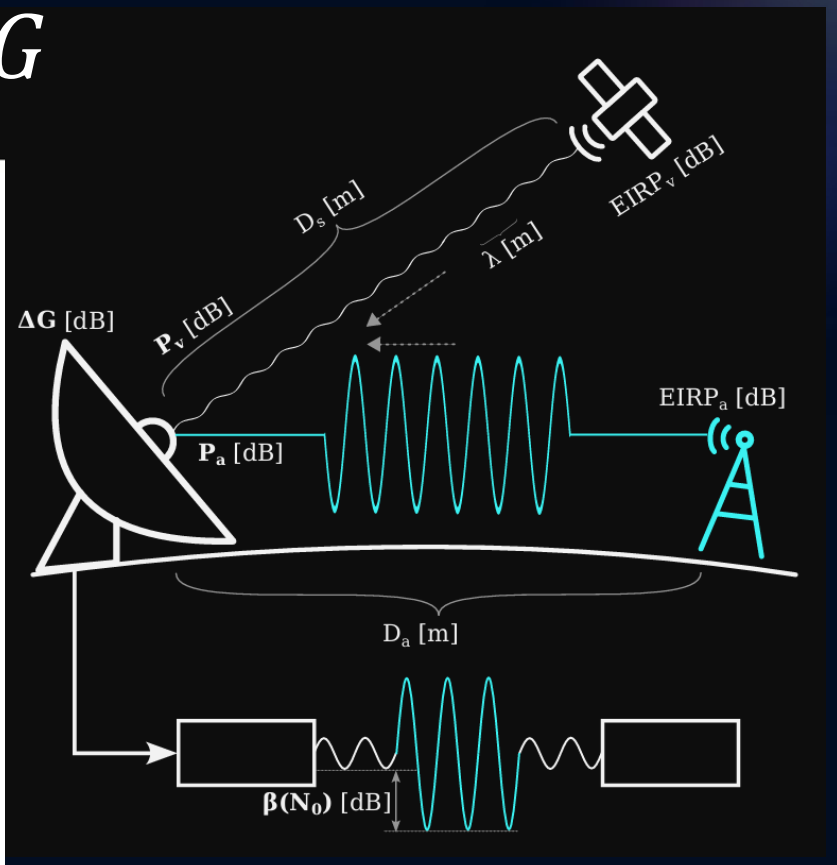
Challenge A

- David L. Adamy's publication, EW 105: Space Electronic Warfare as the following comment "*Unless the jamming transmitter is extremely close to the ground station, this can only be accomplished by looking down at the intercept site from an aircraft (perhaps unmanned) flying over the satellite's ground station*".
- **Oxford @ WiSec'23 ACM:** *Satellite Spoofing from A to Z: On the Requirements of Satellite Downlink Overshadowing Attacks*
- Oxford research: Challenge Accepted.



Threat Model - $P_a > P_v + \beta(N_0) + \Delta G$





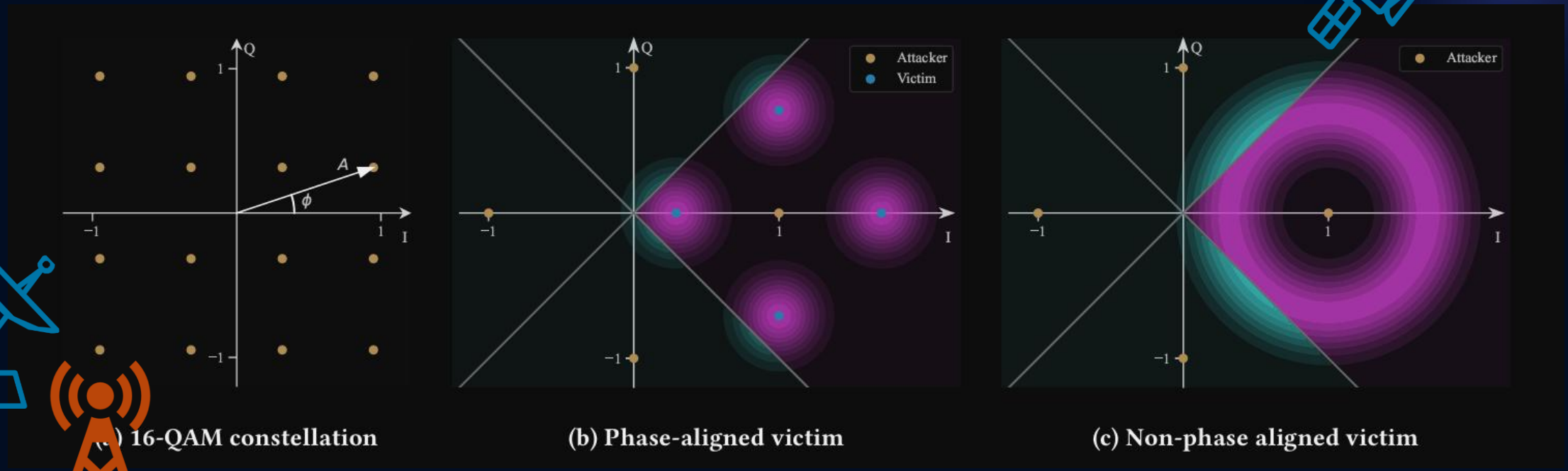
7.1 Calculating required attacker receiver power

As discussed in Section 6, the attack succeeds for any $P_a > P_{a,min}$, where:

$$P_{a,min} = P_v + \beta(N_0) + \Delta G$$

We calculate these values for a set of realistic satellites in Table 4.

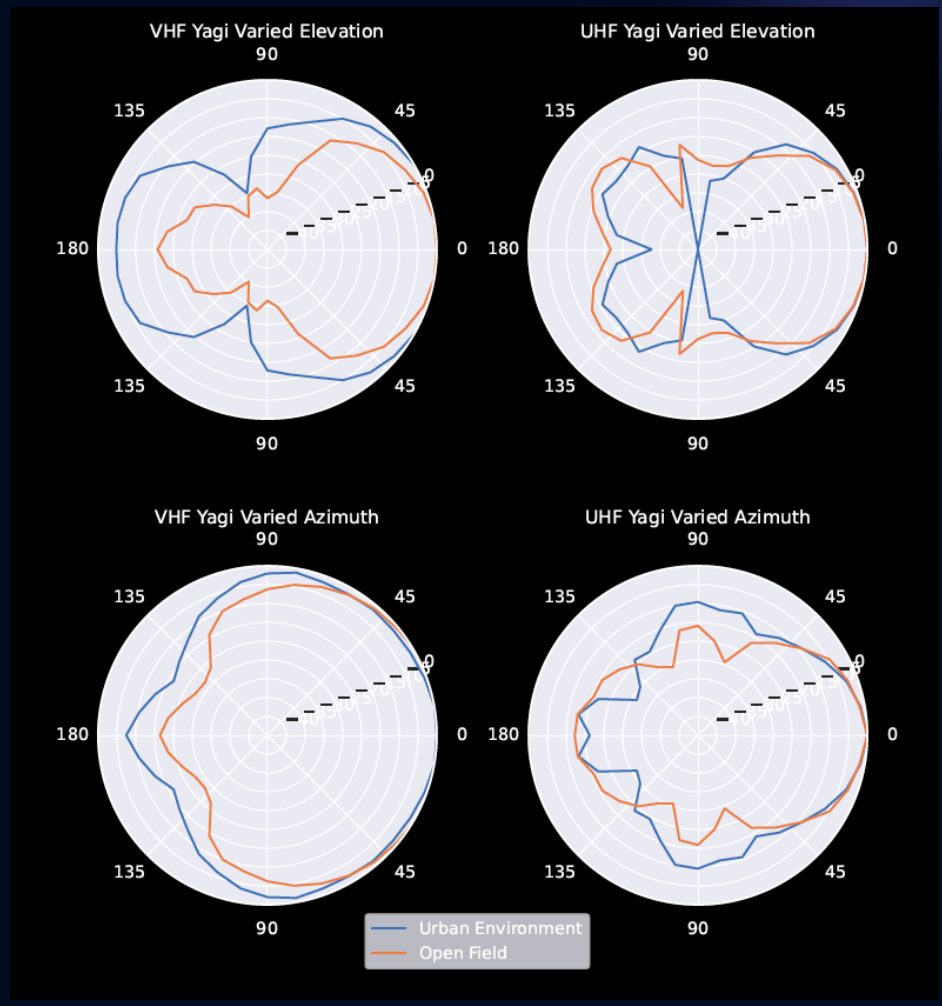
Overshadow Factor $\beta(N0)$ – Demodulator



When attackers inject their malicious signal into a weak legitimate one, the legitimate signal becomes background noise, resulting in a neat constellation that carries the wrong data.

Overshadow Factor ΔG – Victim Antenna

- Sidelobes can reduce out-of-beam attenuation on higher frequencies
- Due to the presence of nearby walls in the urban environment, significant multi-pathing occurs, increasing the gain.



Vulnerable Satellite Analysis

- L-band hardware, ~$254 e.g. Iridium-NEXT
- X-band hardware, ~$406 e.g. Terra/Aqua
  - *“the weakest equipment is capable of overshadowing the strongest signal with 40 dB to spare. Attackers can achieve overshadowing at a distance of over 8 km using only an SDR and very cheap amplifier.”*
- Ku-band hardware at 1km, ~$731 e.g. Starlink
  - Starlink will transmit in BPSK when the channel is very noisy
  - Starlink will transmit in 64-QAM when there's lots of capacity in the channel in order to get more data rates
  - *“Starlink in the Ku band demonstrates the large effect of modulation; BPSK is guaranteed overshadowable within 1 km, but 64-QAM only at very close range. The Ka band is similar, being overshadowable from 8 km in the best case, but within 1 km in the worst case”*

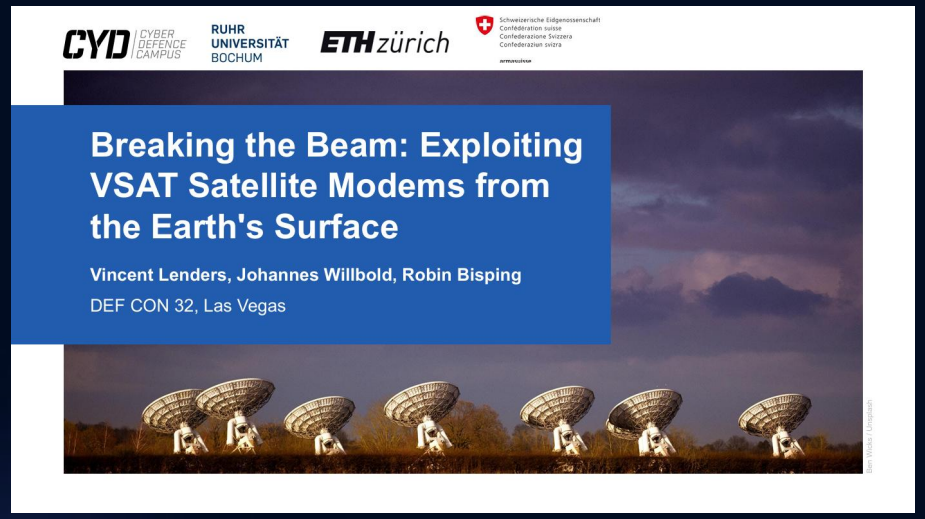
Satellite Class	Satellite	P_v [dBW]	$\beta(N_0)$ [dB]	ΔG [dB]	Required P_a [dBW]
GNSS (Navigation)	GPS L1	-155.8	3.0 – 13.60	0	-152.8 – -142.2
Telecommunication (Customer)	Iridium-NEXT	-145	3.0 – 13.60	0	-142 – -131.4
	Inmarsat 3	-138.1	-0.1 – 13.00	8.7 – 30	-129.5 – -95.1
	Alphasat	-117.1	-0.1 – 13.00	8.7 – 30	-108.5 – 74.1
	Starlink (64-QAM)	-131.9	19.90 – 25.60	13.25 – 31.15	-98.75 – -75.15
	Starlink (BPSK)	-131.9	-0.1 – 13.00	13.25 – 31.15	-118.75 – -87.75
Earth Observation	Terra/Aqua (Direct Broadcast)	-151.8	3.0 – 13.60	14.1 – 30	-134.7 – -108.2
	Planet Labs Dove (QPSK)	-156.5	3.0 – 13.60	14.1 – 30	-139.4 – -112.9
CubeSat	FUNcube	-135.3	-0.1 – 13.00	14.1 – 30	-121.1 – -92.3

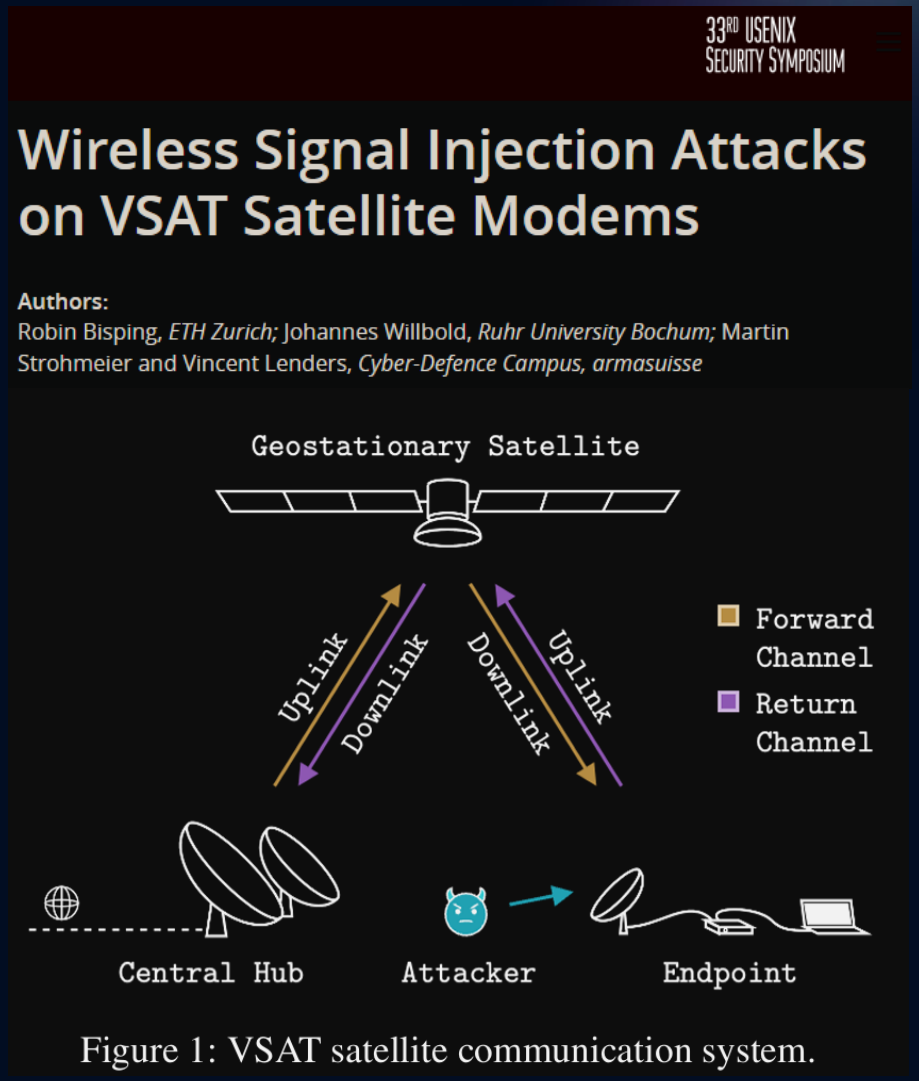
Ref: Salkield, Edd, et al. "Satellite spoofing from a to z: on the requirements of satellite downlink overshadowing attacks." Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 2023.

Challenge B
Zero Knowledge Context

From Space Jam to Practical Attack

- In order to better understand the risk of real-world VSAT satellite communication, they reverse-engineer the software (version 2.2.6.19) and hardware architecture of the popular Newtec MDM2200 satellite modem, which is #1 ranking solution adopted in several fields, as #1 ranking in maritime (oil & gas, and commercial shipping), 44% market share of aero in #1 ranking, and #1 ranking in U.S. DoD VSAT for critical infrastructures, 21 of28 EU nations, and 19 of 29 NATO member states.

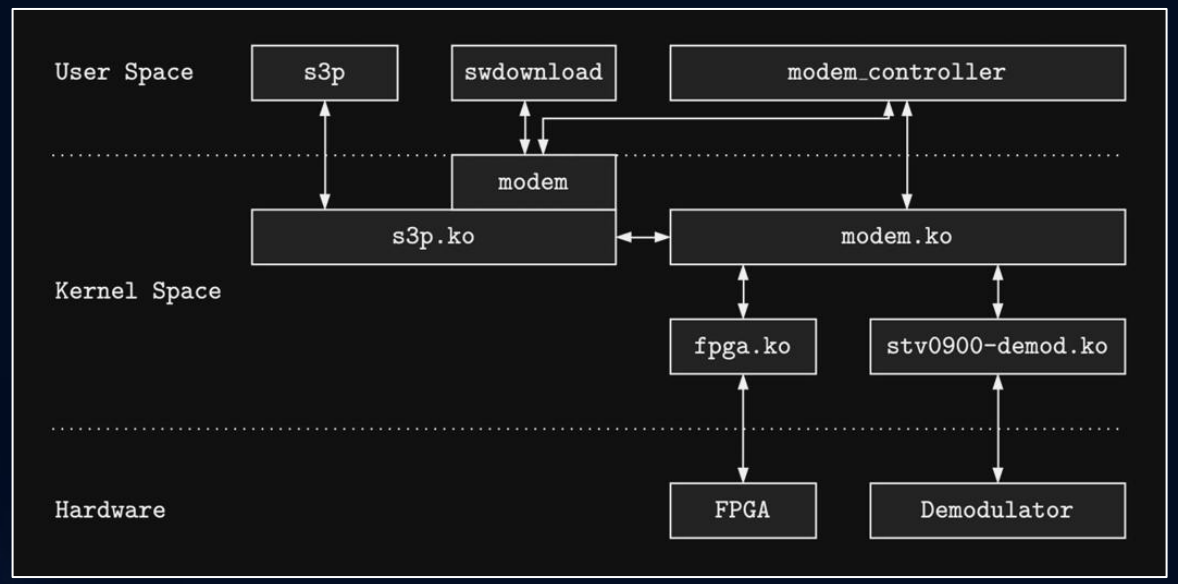




Ref: Bisping, Robin, et al. "Wireless Signal Injection Attacks on {VSAT} Satellite Modems." 33rd USENIX Security Symposium (USENIX Security 24). 2024.

From Space Jam to Practical Attack

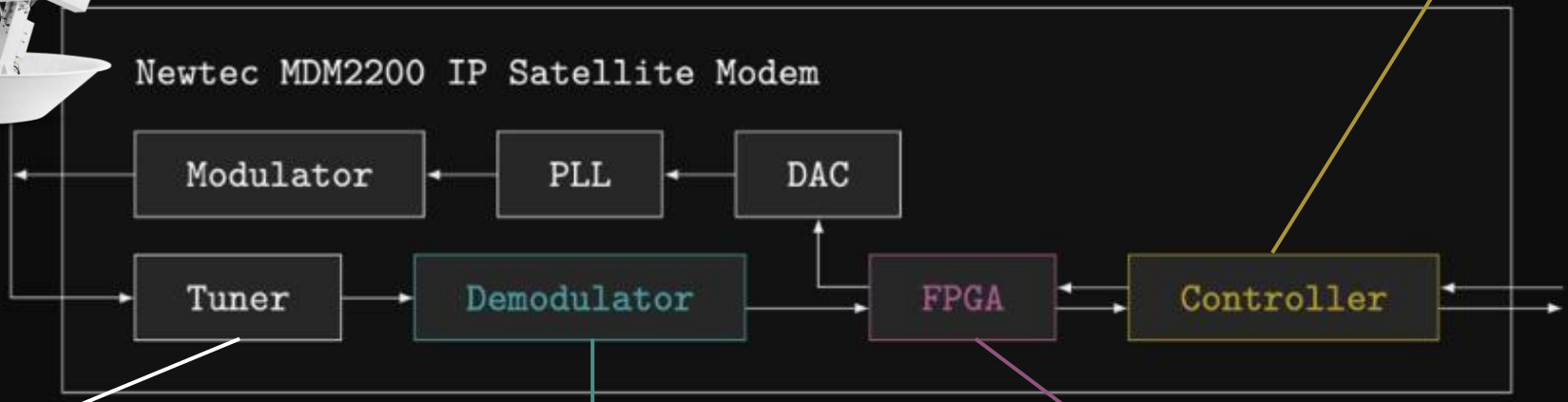
- **modem_controller:** designed to receive and demodulate the communication signals over satellite, to serve the user's network demand WITH a customized message envelope to secure the network traffic (which is powered by the modem_controller process.)
- **swdownload:** application software updater of Sat3Play (S3P)



Ref: Bisping, Robin, et al. "Wireless Signal Injection Attacks on {VSAT} Satellite Modems." 33rd USENIX Security Symposium (USENIX Security 24). 2024.

Forward Channel

The signal pipeline is abstracted behind a network interface: the received IP packets are fed into the IP network stack. Depending on their destination, they are either output to the LAN via the RJ-45 Ethernet port or routed to an internal process.

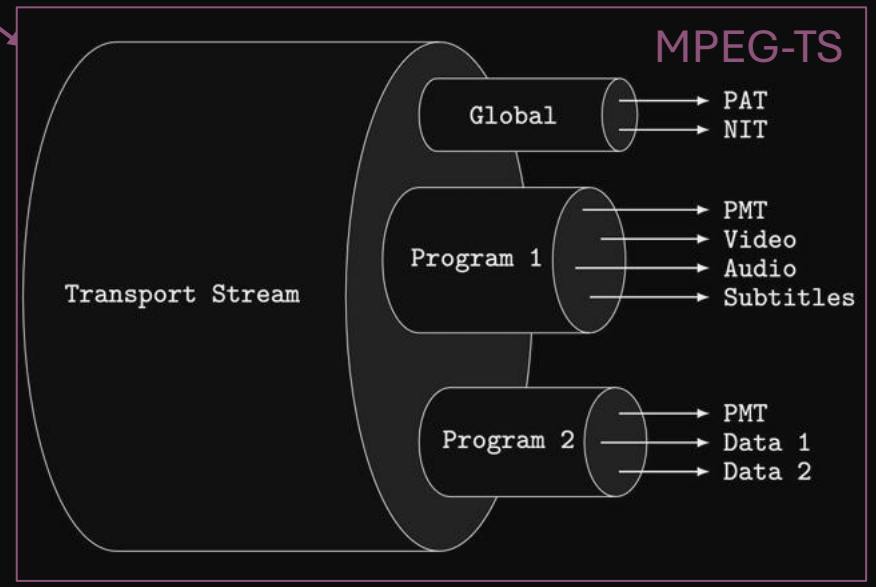


A satellite tuner IC, an STV6111, is used to tune to the correct frequency. It supports an L band frequency input in the range 950-2150 MHz.

[initial carrier] The frequency is configured statically in web interface, which is usually done by the vendor before sending the modem out to its customers.

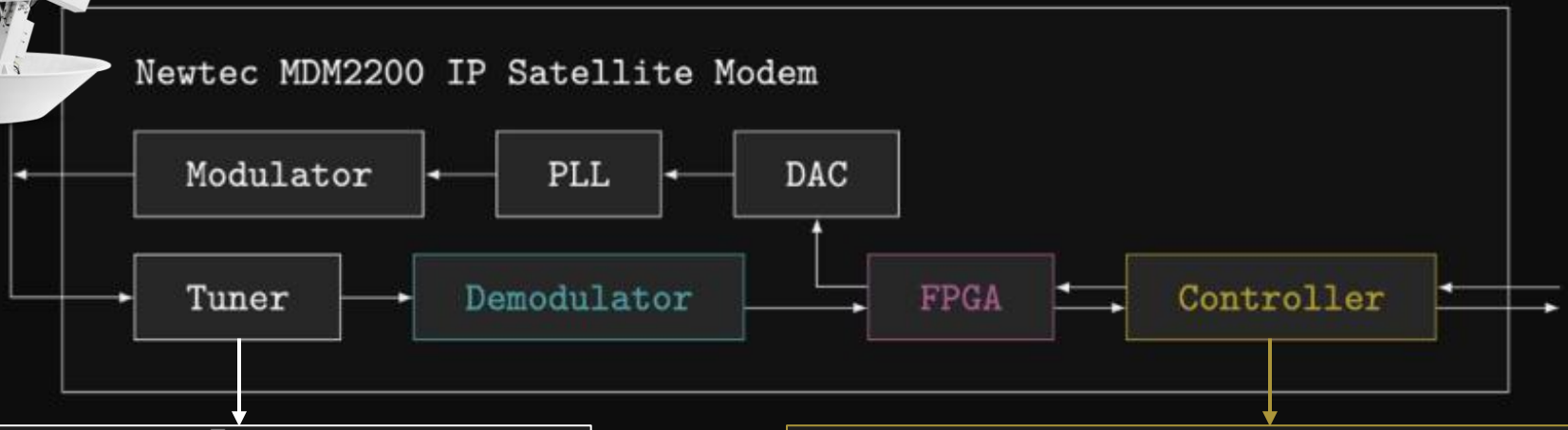
The parameters of the subsequent carriers are signaled via program-specific information and service information

Demodulator IC, anSTV0900A, this chip contains an analog-to-digital converter and supports both the DVB-S and DVB-S2 standards with all their modulation and coding schemes.



Ref: Bisping, Robin, et al. "Wireless Signal Injection Attacks on {VSAT} Satellite Modems." 33rd USENIX Security Symposium (USENIX Security 24). 2024.

Vulnerable Secure Envelop by Google ProtoBuf

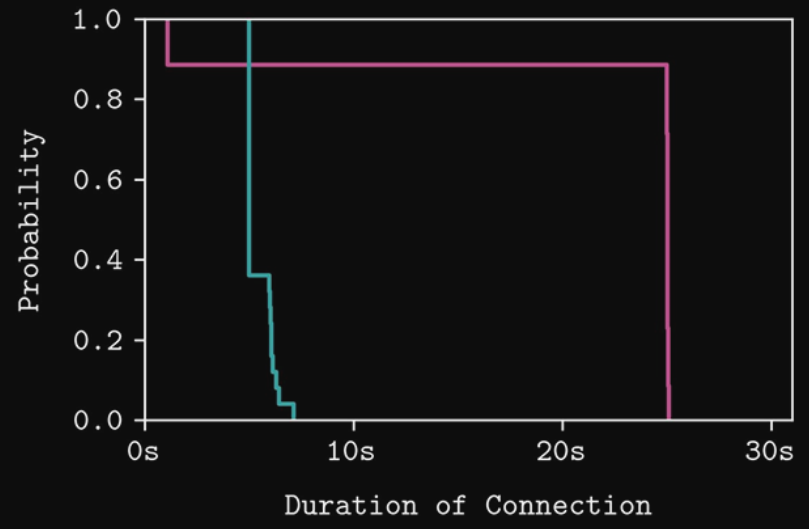



```
ModemController::init(ModemController *this) {
    std::string term_priv_key;
    ret = modem_crypt_init();
    if (ret == -1) log_printf(3, "Failed to init modem_crypt library\n");

    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->term_init_priv_key;
    HubInterfaceAPI::pushTerminalPrivateKey(term_priv_key);
}
```

```
    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
                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);
                return 1;
```

Ref: Bisping, Robin, et al. "Wireless Signal Injection Attacks on {VSAT} Satellite Modems." 33rd USENIX Security Symposium (USENIX Security 24). 2024.

Under jamming a deterioration in connection duration is noticeable; Under normal conditions the modem anticipates return channel configurations after 25 seconds.



?

```
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;
}
```

?

Ref: Bisping, Robin, et al. "Wireless Signal Injection Attacks on {VSAT} Satellite Modems." 33rd USENIX Security Symposium (USENIX Security 24). 2024.

Code Execution

- Process, sw_download run on Linux 2.6.35
  - No ASLR
  - No Stack Canaries
  - Buffer Overflow on parsing auth handshake traffic
- The other vulnerabilities
  - Web UI command injection
  - firmware update without signature (only CRC)

```
# $ 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!.
```

```c
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
…
```

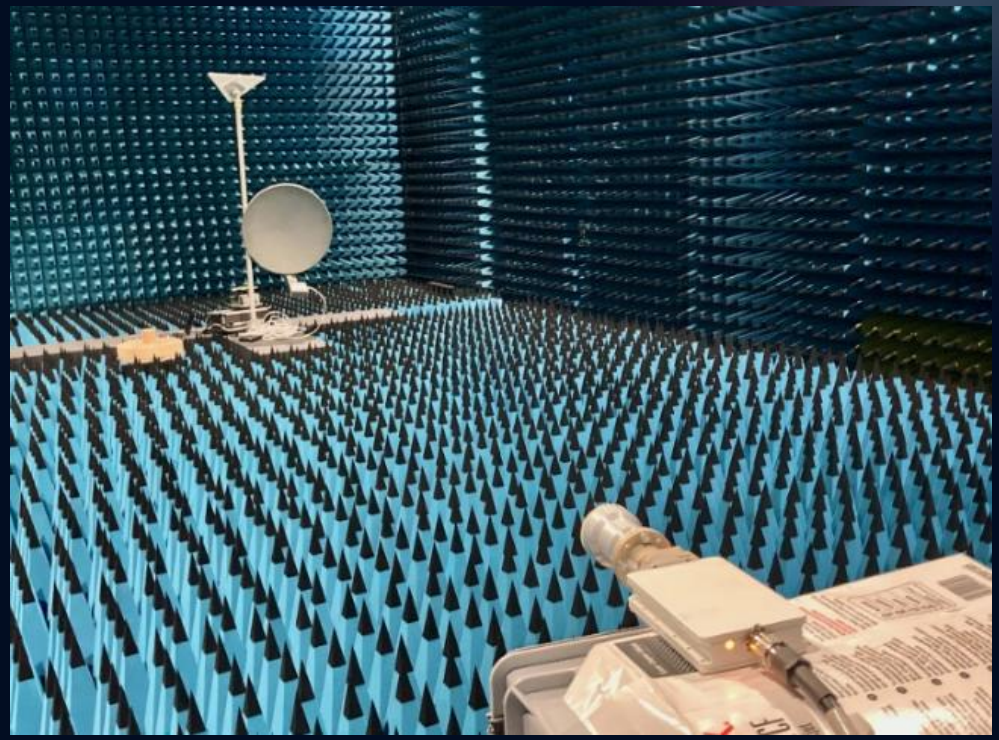
168	1.310934	172.18.19.81	239.1.0.1	UDP
169	1.320783	172.18.19.81	239.1.0.2	UDP
170	1.330876	172.18.18.35	239.1.0.1	UDP

```
> Frame 168: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: IPv4mcast_01
> Internet Protocol Version 4, Src: 172.18.19.81, Dst: 239.1.0.1
> User Datagram Protocol, Src Port: 44699, Dst Port: 49152
v Data (183 bytes)
    Data: 00ff75496d6167653032303230363046004f435445540062…
    [Length: 183]
```

Ref: Bisping, Robin, et al. "Wireless Signal Injection Attacks on {VSAT} Satellite Modems." 33rd USENIX Security Symposium (USENIX Security 24). 2024.

Remote Code Execution

- ~ $2000
  - 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



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

```
~
❯ nc -lvp 5000
Connection from 192.168.1.1:48282
uname -a
Linux S3P 2.6.35.14-s3pdx-svn13990 #1 PREEMPT Mon Oct 20
16:41:23 CEST 2014 armv5tel GNU/Linux
whoami
root
```

Ref: Bisping, Robin, et al. "Wireless Signal Injection Attacks on {VSAT} Satellite Modems." 33rd USENIX Security Symposium (USENIX Security 24). 2024.

Mitigation

- Physical layer
  - Spoofing detection
  - Signal fingerprinting
- Data link layer
  - MAC layer encryption
  - Source authentication
- Network layer
  - IPSec

8.2.1 Physical Layer

Several strategies have been proposed to detect spoofed signals at the physical layer. For instance, Jedermann et al. [20] advocate for the utilization of time difference of arrival measurements obtained from multiple receivers to compute the satellite's position and compare it with the satellite's actual position. In cases where these do not align, it can be concluded that the signal is spoofed.

In addition, Smailes et al. [36] advocate for employing fingerprints, which are derived from distinctive signal characteristics exhibited by the transmitter. To implement this, they propose an architecture for transforming satellite signals into unique fingerprints. If these deviate significantly from pre-recorded reference fingerprints, the system categorizes the signal as spoofed and rejects it.

8.2.2 Data Link Layer

The DVB-RCS [18] standard outlines encryption and authentication mechanisms that cryptographically scramble the transmission. However, the adoption of these measures is optional and contingent upon the specific implementation. The data necessary for the modem to discern if a packet is intended for it is retained in unauthenticated plaintext. Furthermore, these protective measures are only activated following the exchange of keying material. Consequently, they do not provide protection against spoofing during modem initialization, unless they keying material has previously been exchanged offline.

Ref: Bisping, Robin, et al. "Wireless Signal Injection Attacks on {VSAT} Satellite Modems." 33rd USENIX Security Symposium (USENIX Security 24). 2024.


txOne
networks