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

James Pavur
james.pavur@cybersecurity.ox.ac.uk
Oxford University

Daniel Moser
daniel.moser@inf.ethz.ch
armasuisse / ETH Zurich

Vincent Lenders
vincent.lenders@armasuisse.ch
armasuisse

Ivan Martinovic
ivan.martinovic@cs.ox.ac.uk
Oxford University

## ABSTRACT

Demands for ubiquitous global connectivity have sparked a satellite broadband renaissance. Secure satellite broadband is vital to ensuring that this growth does not beget unanticipated harm. Motivated by this need, this paper presents an experimental security analysis of satellite broadband signals using the Digital Video Broadcasting for Satellite (DVB-S) protocol. This analysis comprises 14 geostationary platforms encompassing over 100 million square kilometers of combined coverage area.

Using less than €300 of widely available equipment, we demonstrate the ability to identify individual satellite customers, often down to full name and address, and their web browsing activities. Moreover, we find that these vulnerabilities may enable damaging attacks against critical infrastructure, including power plants and SCADA systems. The paper concludes with a discussion of possible confidentiality protections in satellite broadband environments and notes a need for further cryptographic research on link-layer encryption for DVB-S broadband.

**ACM Reference Format:**
James Pavur, Daniel Moser, Vincent Lenders, and Ivan Martinovic. 2019. Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband. In *WiSec '19: Conference on Security and Privacy in Wireless and Mobile Networks, May 15–17, 2019, Miami, FL, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3317549.3323418

## 1 INTRODUCTION

Satellite based internet communications have existed for nearly as long as the internet itself [1]. Today, satellite broadband is experiencing something of a market renaissance driven by demand in the developing world and the expected coverage demands of the Internet of Things and autonomous vehicle sectors [2, 3, 4]. Robust communications security is vital to ensuring these innovations do not endanger those who rely on them.

This paper focuses on the ability of low-resourced malicious actors to undermine privacy and security in one widely used satellite broadband protocol: DVB-S encapsulated IP traffic. Particular attention is paid to the ability of attackers to compromise consumer privacy and damage satellite-dependent critical infrastructure. This threat is tested experimentally using traffic captures from 14 geostationary satellites providing a combined signal footprint of more than 100 million square kilometers (Figure 1).

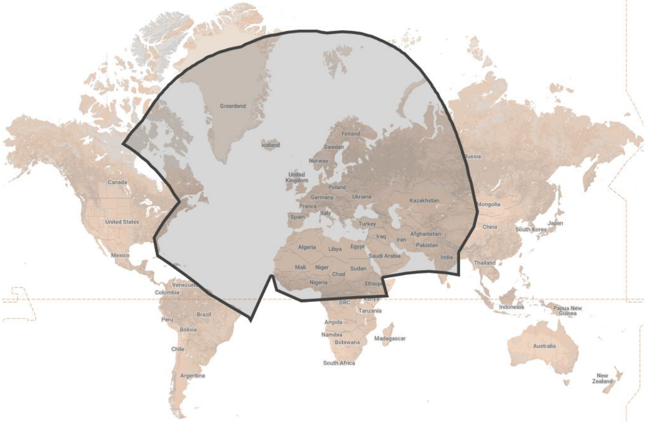


**Figure 1: Transmissions destined for locations covered by the polygon on this map were analyzed at our collection site in Europe.**

## 2 RELATED WORK

Most relevant academic work on satellite broadband security predates the emergence of smartphones and recent dramatic growth in the internet of things and connected infrastructure sectors. Prior work tends to focus on only individual satellites and as a result, identified issues may simply have been shortcomings of a single service provider.

In 2005, a team of researchers from Ruhr University Bochum published what appears to have been the first experimental security study of satellite broadband [5]. They collected traffic from a single Astra satellite (since depreciated) and

*WiSec '19, May 15–17, 2019, Miami, FL, USA*

ACM ISBN 978-1-4503-6726-4/19/05. . . $15.00
https://doi.org/10.1145/3317549.3323418

observed that the satellite transmitted DVB-S encapsulated web-browsing data in the clear. The researchers noted that these short-comings may have been the responsibility of end-users who relied on unencrypted protocols such as POP3 emails [5].

A few years later, at Black Hat 2009, private security researcher Adam Laurie presented on a traffic interception experiment which used modified equipment provided by a satellite ISP [6]. This was followed at Black Hat in 2010 by Leonardo Nve Egea, who demonstrated satellite internet sniffing using DVB PCI cards in the Ka-Band [7]. Some peripherally related academic work has emerged in the form of various standards revisions for satellite internet [8, 9, 10]. Moreover, some related non-academic work on other aspects of satellite systems (such as the security of software on satellite terminals) has taken place [11, 12]. However, the past eight years have seen very little study of satellite broadband transmissions and more than a decade has elapsed since major academic consideration of these networks.

Beyond academia and security conferences, hobbyist and criminal communities are the primary source of modern domain-specific research. For example, online communities dedicated to the receipt of free satellite television have developed various high-quality tools for scanning, intercepting, and interpreting DVB-S signals [13, 14]. Online forums dedicated to the illegal cracking and cloning of private keys associated with satellite television networks are active hotbeds of informal offensive security research [15]. Finally, criminal groups have demonstrated the usage of satellite internet connections for exfiltrating data to undetectable command-and-control stations [16].

In short, only a small body of high-quality but dated academic research exists. Researchers in the 2000s suggested severe security shortcomings in DVB-S broadband but no assessment has been performed to assess if the modern situation has improved or changed [5, 6, 7]. This paper updates and expands previous findings in the context of modern internet traffic. Unlike prior research, which focused on individual satellites and providers, we focus on a broad cross-section of the industry and present what we believe to be the first large-scale multi-satellite security study of DVB-S broadband.

## 3 DVB-S NETWORKS

The long distances in geostationary earth orbit (GEO) satellite networks (72,000 km from customer to ISP) have resulted in protocols designed specifically for satellite radio broadcasts. Among these is the widely used Digital Video Broadcasting-Satellite (DVB-S) and DVB-S version 2 (DVB-S2) protocols [17]. DVB-S is widely used in the provision of satellite television services. This has resulted in the emergence of a large number of free tools and protocol analyzers allowing individuals to receive satellite television without purchasing subscriptions. Moreover, DVB-S is the de facto global standard for satellite broadcast and IP services, particularly from GEO [18, 19]. When compared with more proprietary protocols for which comparatively little public tooling exists (e.g. Inmarsat's BGAN system), this makes DVB-S a particularly attractive target for attackers [20].

The DVB-S standard transmits data per the Moving Pictures Experts Group (MPEG) standards in the form of MPEG transport streams (MPEG-TS) [21]. While MPEG-TS is primarily used for media broadcasting, the standard has also been extended to support many other types of data. In particular, one such extension, called "Digital Storage Media Command and Control" (DSM-CC) was developed to provide interactive features on Video Cassette Recorders (VCR) [22]. As demands for interactive satellite broadband services grew, DSM-CC was repurposed to relay arbitrary packetized data to and from satellite internet customers via an additional encapsulation layer called Multiprotocol Encapsulation (MPE) [23]. A subsequent revision of the MPE method called Unidirectional Lightweight Encapsulation (ULE) has also been created which allows for the transmission of packetized data without the use of DSM-CC tables [23]. In both protocols, IP packets destined for many distinct customers are transmitted on the same stream and then extracted by customer equipment on the basis of address information in the IP header or ISP-assigned MAC addresses in the MPE/ULE headers.

### 3.1 Data Visibility

The specific topology of satellite networks can have significant impacts on an attacker's ability to understand broadband transmissions. Our threat model takes into account two of the most common network topologies.

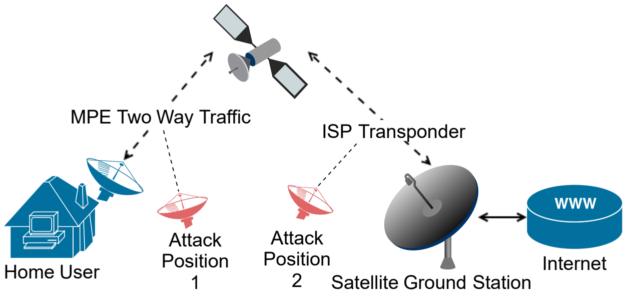


**Figure 2: A single-band two-way satellite internet setup. Attackers at position 1 and 2 will see downstream and upstream traffic respectively.**

The first configuration leverages two-way linkages from the customer's satellite dish and is ideal in remote locations (such as rural areas or naval vessels) where no terrestrial connectivity is available (Figure 2). The customer transmits a web request directly to a satellite which then relays these requests on another beam towards an ISP-controlled ground station. At the ground station, this request is relayed across the wider internet and the response is subsequently transmitted back the customer. An attacker listening to the downlink-to-consumer connection (Position 1 in Figure 2) could intercept responses from the internet while an attacker listening to the downlink-to-ISP connection (Position 2 in Figure 2) would be able to view requests made to the internet. Depending on the specific geographic location of the attacker in either scenario, additional traffic may also be visible through interception of signals emanating from antenna side lobes.

The second configuration offered by some specialized ISPs such as Broadsat's Opensky combines satellite and terrestrial linkages (Figure 3) [24]. Uplink requests are transmitted via a terrestrial connection, which typically has better latency (Position 1 in Figure 3). Requests are sent to a proxy operated by the satellite ISP (Position 2 in Figure 3) and responses relayed back to the user via satellite (Positions 3-5 in Figure 3). Such configurations are ideal in cases where uplink latency is of higher priority than uplink bandwidth and for customers with extant but inadequate terrestrial service. Here, an attacker would be incapable of observing uplink traffic over the air as it is transmitted via wire rather than radio.

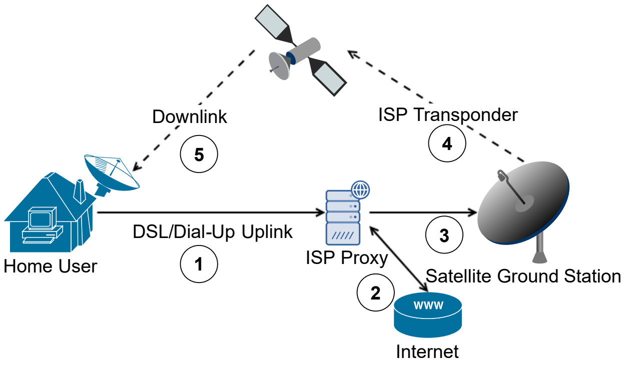


**Figure 3: A combined terrestrial uplink, space downlink satellite internet setup**

# 4 EXPERIMENTAL DESIGN

## 4.1 Attacker Equipment

For this study, we sought to discern the capabilities of a single malicious individual rather than a larger organization or nation state. As such, we restricted our equipment selection to hardware that was readily available for purchase online and only employed free software tools. The total cost of necessary equipment was under €300, as demonstrated by the budget in Table 1.

**Table 1: Hypothetical Attacker Budget**

| Equipment | Cost |
|---|---|
| Selfsat H30D Satellite Dish | €85 |
| TBS 6983 Satellite PCI-E Card | €197 |
| 3-Meter Coaxial Cable | €3 |
| Total | €285 |

It is worth noting that equipment quality can have a meaningful impact on capabilities. For legitimate customers, specialized hardware targeted to their ISP is used in the form of a satellite receiver/modem. Relying on generic equipment can increase processing errors – especially for complex modulation modes such as 16 and 32-APSK.

## 4.2 Deployment

Two inexpensive satellite receiver assemblies (of the sort intended for RV-camping) were deployed to simulate this threat model. One consisted of a 75 cm, flat-panel satellite receiver dish and a TBS-6983 DVB-S receiver. The other consisted of a 60 cm flat-panel dish, a motorized targeting assembly, and a TBS-6903 DVB-S receiver. The 75 cm dish remained in a fixed position while the 60 cm dish was repositioned to target many satellites over the duration of the study. The panels were configured to receive Ku-band transmissions between 10,700 MHz and 12,750 MHz with both vertical and horizontal polarizations. Both assemblies were located in Europe and, due to environmental constraints, could observe geostationary satellites positioned between 40°East and 37°West.

A set of 14 geostationary satellites were selected based on signal quality at the collection site. From these satellites over 350 transponders were identified using existing "Blind Scan" tools.

A collection of Python utilities developed for the purpose of this study was used to analyze each of these transponders for signs of DVB-based internet transmissions on the basis of three criteria. First, a stream was deemed more likely to carry internet traffic if DSM-CC (MPE) services were listed in the stream's program table. Second, streams which contained valid UDP or TCP packets, based on existing MPEG-TS dissectors in Wireshark, were flagged as candidates. Finally, streams were parsed against a list of regular expressions commonly seen in internet traffic. A total of 19 streams met at least two of these criteria and 4 additional matches were identified on the basis of the regular expression engine alone. From these 23 transponders, streams which appeared to carry IP-TV traffic or simple device firmware update services were discarded, along with streams with extremely low signal quality and throughput (anything less than 5 kb/s). This left 13 transponders for further study.

# 5 DATA COLLECTION

In June, 2018, approximately five hours of traffic were recorded on each of the 13 selected transponders. These recordings were initiated automatically in sequence over the course of three days. Each recording was processed to remove NULL packets and irrelevant program data (such as programme data related to satellite television). After this process we were left with 50 gigabytes of satellite internet traffic. Depending on location, radio conditions, and transmission modes, the amount of data collected per transponder ranged from as low as 8 megabytes to as high as 10 gigabytes (see Figure 4).

As anticipated in Section 4.1, recordings included many data errors resulting from our use of general-purpose hobbyist equipment. Nevertheless, sufficient information could be

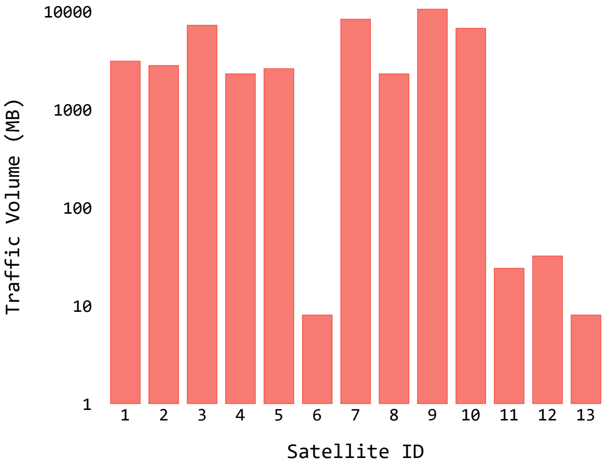


**Figure 4: Volume of internet traffic on each targeted transponder during the five-hour analysis window.**

extracted despite this corruption to give a general characterization of security concerns.

*5.0.1 Ethics, Data Privacy, and Legal Considerations.* Prior to our experiment, it was unclear what sort of information would be uncovered. As such, we assumed a worst-case scenario and treated all recorded radio signals as if they might contain sensitive information. Data was stored at the collection site in Europe and both physical and electronic access was restricted. Local laws relating to the interception and analysis of radio traffic were strictly adhered to. We also made plans to responsibly disclose any security issues which warranted it to the appropriate authorities. After the study all collected data was deleted.

## 6 FINDINGS

Across all thirteen frequencies included in the final phase of our study, broadband traffic was transmitted in plaintext. Of course, well-encrypted transmissions would not have been distinguishable from non-internet traffic and it is thus unclear to what extent these thirteen service providers are representative of the industry as a whole. Nevertheless, having the same issues appear over many distinct providers suggests that the earlier single-provider studies discussed in Section 2 were not merely anecdotal and the problems they identified have not yet been addressed.

The dangers of unencrypted wireless transmissions are well understood and, to some degree, academically uninteresting. However, unique properties of satellite broadband act as novel risk-multipliers.

The principle differentiator is scale. Our experiment included data from a coverage footprint of more than 110 million square kilometers (Figure 1). A handful of strategically located satellite dishes, would allow an attacker to intercept broadband signals encompassing most of the globe. Furthermore, satellite interception offers a privileged ISP-esque vantage-point and enables eavesdropping on the entirety of a target's traffic.

### 6.1 Privacy

A surprising amount of sensitive information appeared in the collected data. Indeed, many of the same categories identified over a decade ago still appear in modern satellite traffic.

One significant improvement since the mid-2000s has been increased adoption of SSL/TLS encryption. While this protects against certain types of eavesdropping attacks, the very process of requesting and exchanging SSL certificates leaks potentially revealing information. Our data included over 52,000 SSL "wildcard" certificates from around 1,200 distinct domains (Figure 5). Information a user might consider deeply private – such as TLS certificates or DNS responses from various adult websites – is, in fact, being broadcast across an entire continent. With collating data, such as knowledge of a user's IP address, this risk becomes particularly severe.

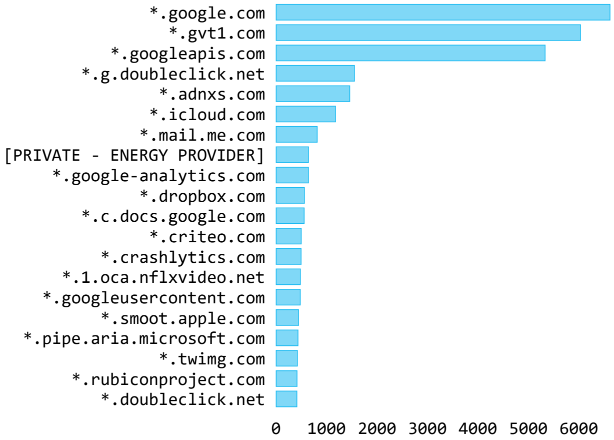


**Figure 5: The top 20 domains identified on a basis of SSL certificates. Number 8 has been hidden as it is a private subdomain range for a major energy provider.**

While SSL usage is widespread, our naive string-matching analysis nevertheless uncovered thousands of unencrypted HTTP requests, file downloads, FTP sessions, torrent connections, VoIP conversations and emails. The chart in Table 2 indicates which of these general classes of sensitive information were identified on each of the 13 transponders. Due to the sensitive nature of our findings, specific service providers and satellite names have been withheld. These findings raise legal and business concerns regarding whether it is the responsibility of satellite service providers to protect customers using insecure protocols over DVB-S or if responsibility for encryption in transit falls to end-users.

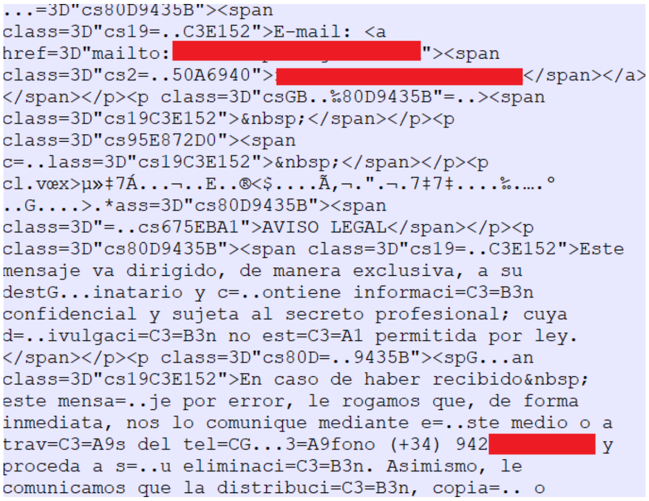
*6.1.1 Demonstrative Cases.* Beyond this broad sense of information leakage, a number of individual "narratives" emerged

**Table 2: Observed Traffic Contents**

| 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 |

during manual analysis. Although anecdotal, these incidents provide perspective on the need for communications security improvements. These incidents ranged from individuals who shared national identification numbers with hotels via plaintext email messages to online shoppers submitting payment details in clear-text.

One such case relates to an individual who connected his iPhone to a wifi network and synced his email client over IMAP. From the information he downloaded we were able to determine the specific town in northern Spain where he lived, his full name, phone number, and both his office and personal addresses. If this were not concerning enough, the individual proved to be a defense lawyer. Included in the traffic were specific and confidential communications between him and his clients regarding ongoing cases and the preparation of evidence for an upcoming trial (Figure 6). The data could have been intercepted by nearly anyone in Europe or Northern and Western Africa. Our ability to intercept it raises serious concerns for attorney-client privilege.



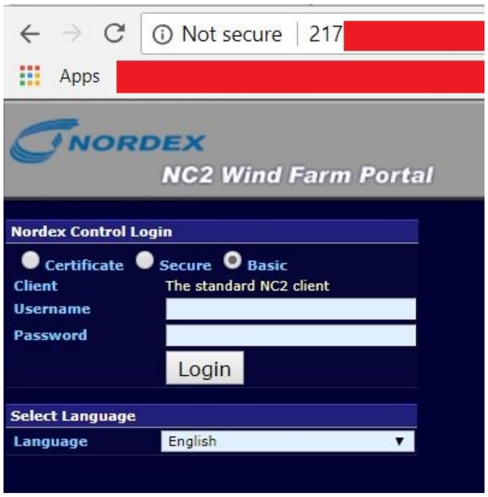
```
...=3D"cs80D9435B"><span
class=3D"cs19=..C3E152">E-mail: <a
href=3D"mailto:[redacted]"><span
class=3D"cs2=..50A6940">[redacted]</span></a>
</span></p><p class=3D"csGB..%80D9435B"=..><span
class=3D"cs19C3E152">&nbsp;</span></p><p
class=3D"cs95E872D0"><span
c=..lass=3D"cs19C3E152">&nbsp;</span></p><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
```

**Figure 6: The footer of one email from a lawyer to his client which was sent in plaintext via satellite internet. Sensitive information has been censored.**

## 6.2 Infrastructure

Through manual inspection of intercepted traffic, we detected flows associated with electrical power generation facilities. The majority of these were wind and solar farms but we also encountered facilities associated with the oil and gas industry. These were not isolated to a single provider but appeared both across several satellite internet services and terrestrial infrastructure operators.

While in some cases, such as an American solar power provider, TLS encryption was employed to protect infrastructure traffic, a large number of operators used unencrypted HTTP and FTP connections. In the case of one specific software platform commonly used in wind-power generation industry, over 5,000 plaintext requests were observed to various facilities and administration pages (Figure 7). Inside these requests we found credentials in the form of either HTTP Basic Authorization tokens or as session cookies that could be used to gain unauthorized access to the plants. Moreover, Credentials belonging to a company which operates almost a fifth of the world's installed wind energy base appeared frequently in unencrypted FTP control flows. Vulnerable systems administration pages and FTP servers were publicly routable from the open internet. This means that an attacker could sniff a session token from a satellite connection, open a web browser, and login to the plant's control panel.



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 ▼

**Figure 7: The login page for one vulnerable wind farm we encountered in our traffic. Credentials to access this site were readily identified in satellite transmissions.**

Beyond electrical plants, other infrastructure traffic also appeared in our dataset. For example, on a handful of transponders we identified Modbus traffic – a popular serial protocol widely used in SCADA systems and PLCs. In another instance, a satellite transponder appears to have been reserved for the national postal service of a sizeable Eastern European country and several of their intranet credentials were transmitted in plain text. References to maritime products appeared in the streams, but an in-depth analysis of maritime communications protocols was well beyond the project scope.

## 7 POTENTIAL SOLUTIONS

Our findings suggest a need for improved communications privacy in satellite broadband. The current state of industry has resulted in the leakage of sensitive information from both individual and industrial satellite broadband customers.

The application of terrestrial encryption techniques to satellite environments is non-trivial. Satellite transmissions cover vast distances and are subject to speed-of-light latency effects (upwards of 500ms for a round-trip transmission to GEO) and packet loss which can impair the function of encryption schemes designed for high-reliability terrestrial environments (e.g. by requiring re-transmission of corrupted key materials) [25, 26]. Moreover, satellites themselves are limited in terms of computing capabilities and any on-board cryptographic operation risks trading off with other mission functionality [26].

In television networks, "scrambling" algorithms which apply encryption to an entire MPEG-TS programme are widely used to prevent piracy of premium television channels. However, these techniques are, at present, not well suited to internet traffic for two reasons. First, many of the dominant algorithms in this space (e.g. the Common Scrambling Algorithm or PowerVu) have been demonstrated to have severe cryptographic weaknesses [27, 28, 29]. While these may be acceptable for low sensitivity TV broadcasts, where the principle goal is often to simply increase the complexity of piracy, internet traffic and sensitive data may merit more robust protections. Moreover, because these scrambling algorithms apply at the level of entire streams, customers necessarily share access to a "master key" (often updated at regular intervals) which could be used to compromise the privacy of other customers whose traffic is multiplexed into the same transmission [29]. Future work which builds on these scrambling techniques with a focus on the needs of internet customers may represent a possible avenue for developing more robust DVB-S protections.

One alternative approach would be the use of tunneling mechanisms such as IPSec. In the short term, this is likely the best approach for individual customers and infrastructure operators. However, terrestrial tunneling technologies impose significant performance constraints over satellite connections [8]. Due to the significant latency in GEO broadcasting, satellite service operators have adopted connection acceleration techniques which help minimize these effects. Specifically, broadband providers widely make use of Performance Enhancing Proxies (PEPs) to simulate artificial TCP acknowledgments and TCP features which misinterpret satellite latency as network congestion [26, 30]. Moreover, although TLS functions over satellite networks, plain-text HTTP requests will often appear more performant to users due to the heavy application of HTTP accelerators [26]. Tunneling and end-to-end encryption prevents satellite operators from inspecting the necessary packet headers to continue providing these services.

In the early 2000s, several solutions to these issues emerged, ranging from decrypting traffic at the satellite ISP ground station and re-encrypting for transmission over the internet to implementing revisions to the IPSec protocol itself to extract TCP headers needed for PEP usage, however these have gained little traction [9, 26, 31]. While promising standards proposals exist for encrypted satellite data links in scientific missions, additional work adapting these to multi-user broadband ecosystems is needed [32].

Beyond work to bolster satellite internet encryption, future work characterizing these vulnerabilities may prove useful. While broader than previous research, our study still only studied a handful of operators in the Ku-band and was restricted to the DVB-S protocol. Moreover, our experimentation was limited to passive eavesdropping attacks only. Research on the capabilities of an attacker to compromise not just the confidentiality but also the integrity of satellite broadcasts may uncover additional status quo risks. For example, attacks against the layer-two routing protocols used in satellite networks may facilitate sophisticated session spoofing and hijacking attacks.

## 8 CONCLUSION

Our experimental analysis raises significant concerns for the security of DVB-S broadband. Severe confidentiality shortcomings were identified across more than a dozen service operators and several gigabytes of potentially sensitive web traffic were collected in a matter of hours. An attacker with cheaply available hobbyist equipment may compromise the security and privacy of individuals in an area encompassing hundreds of millions of square kilometers. Moreover, satellite eavesdropping provides a potential route to harming many connected critical infrastructure systems such as power-generation facilities.

We suggest that future cryptographic work which finds a balance between satellite network performance and robust encryption represents a critical step towards resolving these issues. This work might build off of progress in stream-level scrambling techniques or in revisions to terrestrial encryption protocols that account for unique characteristics of satellite networks.

Secure satellite internet is vital to reaping the rewards of a connected future. In light of growth in the infrastructure and IoT space, the security community and satellite industry must cooperate to make satellite broadband private, reliable, and secure.

## REFERENCES

[1] H. D. Clausen, H. Linder, and B. Collini-Nocker. 1999. Internet over direct broadcast satellites. *IEEE Communications Magazine*, 37, 6, (June 1999), 146–151. ISSN: 0163-6804. DOI: 10.1109/35.769289.

[2] Olivier Anstett. Internet Broadband: A New Source of Growth. (2015). https://www.eutelsat.com/files/

contributed/investors/pdf/Capital-Markets-Day-2015/Internet%20broadband_a_new%20_source_of_growth.pdf.

[3] David Grossman. 2018. The Race for Space-Based Internet Is On. (January 3, 2018). Retrieved 05/31/2018 from https://www.popularmechanics.com/technology/infrastructure/a14539476/the-race-for-space-based-internet-is-on/.

[4] Mohammad Marashi. 2017. Satellites are critical for IoT sector to reach its full potential. (June 8, 2017). Retrieved 05/31/2018 from http://social.techcrunch.com/2017/06/08/satellites-are-critical-for-iot-sector-to-reach-its-full-potential/.

[5] André Adelsbach and Ulrich Greveler. 2005. Satellite Communication without Privacy - Attacker's Paradise. In *Sicherheit*.

[6] Adam Laurie. $atellite Hacking for Fun & Pr0fit! (2009). http://www.blackhat.com/presentations/bh-dc-09/Laurie/BlackHat-DC-09-Laurie-Satellite-Hacking.pdf.

[7] Leonardo Egea. Playing in a Satellite environment 1.2. (2010). http://www.blackhat.com/presentations/bh-dc-10/Nve_Leonardo/BlackHat-DC-2010-Nve-Playing-with-SAT-1.2-wp.pdf.

[8] S. Iyengar, H. Cruickshank, P. Pillai, G. Fairhurst, and L. Duquerroy. 2007. Security requirements for IP over satellite DVB networks. In *2007 16th IST Mobile and Wireless Communications Summit*. 2007 16th IST Mobile and Wireless Communications Summit. (July 2007), 1–6. DOI: 10.1109/ISTMWC.2007.4299224.

[9] Laurence Duquerroy, Sebastien Josset, O. Alphand, P. Berthou, and T. Gayraud. 2004. SatiPSec : An Optimized Solution for Securing Multicast and Unicast Satellite Transmissions. In *22nd AIAA International Communications Satellite Systems Conference & Exhibit 2004 (ICSSC)*. American Institute of Aeronautics and Astronautics, (May 2004). DOI: 10.2514/6.2004-3177. Retrieved 01/18/2019 from https://arc.aiaa.org/doi/abs/10.2514/6.2004-3177.

[10] H. Cruickshank, M. P. Howarth, S. Iyengar, Zhili Sun, and L. Claverotte. 2005. Securing multicast in DVB-RCS satellite systems. *IEEE Wireless Communications*, 12, 5, (October 2005), 38–45. ISSN: 1536-1284. DOI: 10.1109/MWC.2005.1522103.

[11] Ruben Santamarta. 2014. SATCOM Terminals: Hacking by Air, Sea, and Land. DEFCOM White Paper, 26. https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf.

[12] Ruben Santamarta. 2018. Last Call for SATCOM Security. Blackhat Whitepaper 2018, (August 2018). https://i.blackhat.com/us-18/Thu-August-9/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf.

[13] Cjcr-Software. 2016. EBSpro. Retrieved 06/20/2018 from http://ebspro.net/.

[14] crazycat69. 2018. CrazyScan: Satellite/terrestrial/cable scan software. Retrieved 06/20/2018 from https://sourceforge.net/projects/crazyscan/.

[15] World-Satellite. 2018. World-Satellite Forum. Retrieved 06/20/2018 from http://www.world-satellite.net/.

[16] Stefan Tanase. 2015. Satellite Turla: APT Command and Control in the Sky. (September 9, 2015). Retrieved 06/20/2018 from https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.

[17] ETSI. 2014. Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications. Retrieved 06/01/2018 from https://www.dvb.org/standards/dvb-s2.

[18] Koen Williams. 2014. DVB-S2X Demystified. White Paper. Newtec, (March 2014). https://www.newtec.eu/frontend/files/userfiles/files/Whitepaper%20DVB_S2X.pdf.

[19] Comsys. [n. d.] VSAT Network Types. Retrieved 03/07/2019 from https://www.comsys.co.uk/wvr_nets.htm.

[20] Inmarsat. [n. d.] BGAN Voice and Broadband Service. Retrieved 04/01/2019 from https://www.inmarsat.com/service/bgan/.

[21] International Telecommunication Union. 2014. H.222.0 Information technology – Generic coding of moving pictures and associated audio information: Systems. (October 2014). https://www.itu.int/rec/T-REC-H.222.0-201410-S/en.

[22] Vahe Balabanian, Liam Casey, Nancy Greene, and Chris Adams. 1996. An Introduction to DSM-CC. (November 1996). Retrieved 06/01/2018 from http://www.iuma.ulpgc.es/~nunez/procmultimedia98-00/cselt/mpeg/documents/dsmcc/dsmcc.htm.

[23] Teh Chee Hong, Wan Tat Chee, and R. Budiarto. 2005. A Comparison of IP Datagrams Transmission using MPE and ULE over Mpeg-2/DVB Networks. In *2005 5th International Conference on Information Communications Signal Processing*. 2005 5th International Conference on Information Communications Signal Processing, 1173–1177. DOI: 10.1109/ICICS.2005.1689239.

[24] Broadsat. [n. d.] OPENSKY - One way satellite internet. Retrieved 06/01/2018 from https://www.broadsat.com/en/opensky/.

[25] Dan Lester and Harley Thronson. 2011. Human space exploration and human spaceflight: Latency and the cognitive scale of the universe. *Space Policy*, 27, 2, (May 1, 2011), 89–93. ISSN: 0265-9646. DOI: 10.1016/j.spacepol.2011.02.002. Retrieved 06/15/2018 from http://www.sciencedirect.com/science/article/pii/S0265964611000348.

[26] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou. 2005. Security issues in hybrid networks with a satellite component. *IEEE Wireless Communications*, 12, 6, (December 2005), 50–61. ISSN: 1536-1284. DOI: 10.1109/MWC.2005.1561945.

[27] W. Li and D. Gu. 2007. Security Analysis of DVB Common Scrambling Algorithm. In *The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007)*. The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007). (November 2007), 271–273. DOI: 10.1109/ISDPE.2007.63.

[28] Erik Tews, Julian Wälde, and Michael Weiner. 2011. Breaking DVB-CSA. In *Research in Cryptology* (Lecture Notes in Computer Science). Western European Workshop on Research in Cryptology. Springer, Berlin, Heidelberg, (July 20, 2011), 45–61. ISBN: 978-3-642-34158-8 978-3-642-34159-5. DOI: 10.1007/978-3-642-34159-5_4. Retrieved 06/15/2018 from https://link.springer.com/chapter/10.1007/978-3-642-34159-5_4.

[29] Colibri. 2014. PowerVu Management Keys Hacked. (December 5, 2014).

[30] A. J. H. Fidler, G. Hernandez, M. Lalovic, T. Pell, and I. G. Rose. 2002. Satellite — A New Opportunity for Broadband Applications. *BT Technology Journal*, 20, 1, (January 1, 2002), 29–37. ISSN: 1573-1995. DOI: 10.1023/A:1014561823985. https://doi.org/10.1023/A:1014561823985.

[31] M. P. Howarth, S. Iyengar, Z. Sun, and H. Cruickshank. 2004. Dynamics of key management in secure satellite multicast. *IEEE Journal on Selected Areas in Communications*, 22, 2, (February 2004), 308–319. ISSN: 0733-8716. DOI: 10.1109/JSAC.2003.819978.

[32] CCSDS. 2018. Space Data Link Security Protocol - Summary of Concept and Rationale. Green Book. (June 2018). https://public.ccsds.org/Pubs/350x5g1.pdf.