Insecure satellite Internet is threatening ship and plane safety



reader comments

36 with 30 posters participating, including story author

Share this story

More than a decade has passed since researchers demonstrated serious privacy and and security holes in satellite-based Internet services. The weaknesses allowed attackers to snoop on and sometimes tamper with data received by millions of users thousands of miles away. You might expect that in 2020—as satellite Internet has grown more popular—providers would have fixed those shortcomings, but you'd be wrong.

In a briefing delivered on Wednesday at the Black Hat security conference online, researcher and Oxford Ph.D. candidate James

Pavur presented findings that show that satellite-based Internet is putting millions of people at risk, despite providers adopting new technologies that are supposed to be more advanced.

Over the course of several years, he has used his vantage point in mainland Europe to intercept the signals of 18 satellites beaming Internet data to people, ships, and planes in a 100 million-square-kilometer swath that stretches from the United States, Caribbean, China, and India. What he found is concerning. A small sampling of the things he observed include:

- A Chinese airliner receiving unencrypted navigational information and other avionics data. Equally worrisome, that data came from the same connection passengers used to send email and browse webpages, raising the possibility of hacks from passengers.
- A system administrator logging into a wind turbine in southern France, some 600 kilometers away from Pavur, and in the process exposing a session cookie used for authentication.
- The interception of communications from an Egyptian oil tanker reporting a malfunctioning alternator as the vessel entered a port in Tunisia. Not only did the transmission allow Pavur to know the ship would be out of commission for a month or more, he also obtained the name and passport number of the engineer set to fix the problem.
- A cruise ship broadcasting sensitive information about its Windows-based local area network, including the log-in information stored in the Lightweight Directory Access Protocol database
- Email a lawyer in Spain sent a client about an upcoming case.
- The account reset password for accessing the network of a Greek billionaire’s yacht.

Hacking satellite communications at scale

While researchers such as Adam Laurie and Leonardo Nve demonstrated the insecurity of satellite Internet in 2009 and 2010, respectively, Pavur has examined the communications at scale, with the interception of more than 4 terabytes of data from the 18 satellites he tapped. He has also analyzed newer protocols, such as Generic Stream Encapsulation and complex modulations including 32-Ary Amplitude and Phase Shift Keying (APSK). At the same time, he has brought down the interception cost of those new protocols from as much as $50,000 to about $300.

“There are still many satellite Internet services operating today which are vulnerable to their [the previous researchers’] exact attacks and methods—despite these attacks having been public knowledge for more than 15 years at this point,” Pavur told me ahead of Wednesday’s talk. “We also found that some newer types of satellite broadband had issues with eavesdropping vulnerabilities as well.”

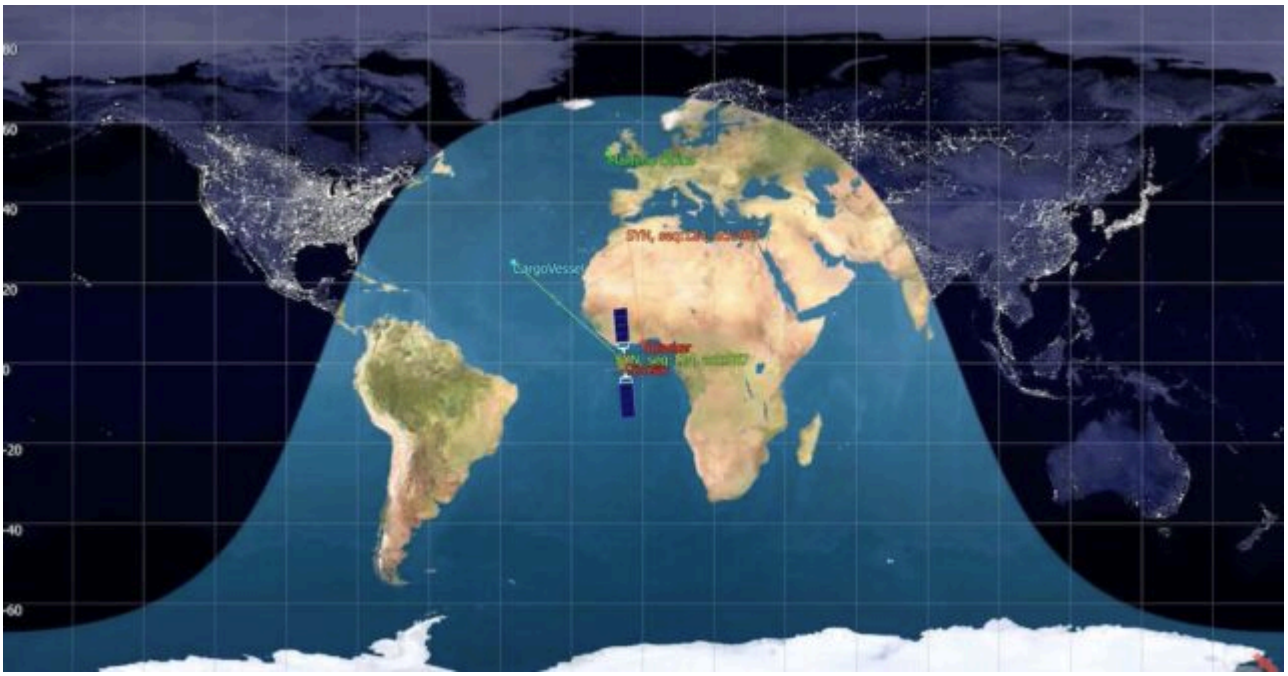
The equipment Pavur used consisted of a TBS 6983/6903 PCIe card/DVB-S tuner, which allows people to watch satellite TV feeds from a computer. The second piece was a flat-panel dish, although he said any dish that receives satellite TV will work. The cost for both: about $300.

Using public information showing the location of geostationary satellites used for Internet transmission, Pavur pointed the dish at them and then scanned the k_u band of the radio spectrum until he found a signal hiding in the massive amount of noise. From there, he directed the PCIe card to interpret the signal and record it as a normal TV signal. He would then look through raw binary files for strings such as “http” and those corresponding to standard programming interfaces to identify Internet traffic.

All unencrypted comms are mine

The setup allows Pavur to intercept just about every transmission an ISP sends to a user via satellite, but monitoring signals the other way (from the user to the ISP) is much more limited. As a result, Pavur could reliably see the contents of HTTP sites a user was browsing or of an unencrypted email the user downloaded, but he couldn't obtain customers' "GET" requests or the passwords they sent to the mail server.

Even though the customer may be located in the Atlantic off the coast of Africa and is communicating with an ISP in Ireland, the signal it sends is easily intercepted from anywhere within tens of millions of square kilometers, since the high cost of satellites requires providers to beam signals over a wide area.



Enlarge / An attacker from anywhere within tens of millions of square kilometers can hijack the connection between a ship off the coast of Africa and a ground station in Ireland.

Pavur explained:

> *There are a few reasons the other direction is harder to capture. The first is that the beam connecting a satellite to*

> *an ISP's ground station is often more narrow and focused (meaning you have to be within a few dozen miles of the ISP's system to pick up radio waves in that direction). In some cases, ISP's will use a different frequency band to transmit these signals for bandwidth and performance reasons—this means an attack might need equipment that is much harder to pick up commercially and affordably. Finally, even if an ISP just uses a normal wide-beam K>$_u$-band signal, they will normally transmit on a different frequency in each direction. This means an attacker would need a second set of antennas (not too difficult) and would also need to combine the two feeds correctly (slightly more difficulty).*

Et tu, Avionics?

In past years, Pavur focused on transmissions sent to everyday users on land and large ships at sea. This year, he turned his attention to planes. With the onset of the COVID-19 pandemic causing passenger flying to plummet, the researcher had less opportunity than he planned to analyze passenger communications from entertainment systems, in-flight Internet services, and onboard femtocells used to send and receive mobile signals. (He did, however, see a text message providing a passenger with a coronavirus test.)

But it turned out that the decrease in passenger traffic made it easier to focus on traffic sent to crew members in the cockpit. When one of the crew fat fingered a login to what's known as an electronic flight bag, the flightdeck equipment repeatedly got an HTTP 302 Redirect error to the Wi-Fi service login page. The redirect format included the URL of the original request showing the GET parameters of the flight bag API. The parameters described the specific flight number and its coordinates, information that gave Pavur a good feel for what the device was doing aboard the plane.



Enlarge / An electronic flight bag sending sensitive avionics information through HTTP.
James Pavur

The flight-bag data passed through the same network-address-translation router as entertainment and Internet traffic from passengers. In other words, the same physical satellite antenna and modem were delivering Internet traffic to both the flight bag and passengers. This suggests that any network segregation that may exist was performed by software rather than through physical hardware separation, which is less prone to hacking.

Session hijacking: The attacker always wins

The use of satellite-based Internet to receive the navigational data puts the crew and passengers at risk of an attack Pavur developed that allows an attacker to impersonate the aircraft with which the ground station is communicating. The hack uses TCP session hijacking, a technique in which the attacker sends the ISP the metadata customers use to authenticate themselves.

Because users' traffic is bounced off a satellite 30,000 kilometers above Earth—a route that typically results in signal latency of about 700 milliseconds—and the attacker's

data isn’t, the attacker will always beat customers in reaching the ISP.

The session hijacking can be used to cause planes or ships to report incorrect locations or fuel levels, false readings for heating, ventilation, and air conditioning systems, or transmit other sensitive data that’s falsified. It can also be used to create denials of service that prevent the vessel from receiving data that’s crucial to safe operations.



Enlarge / Capabilities and limitations of TCP session hijacking of satellite Internet.
James Pavur
Pavur explained the hijacking methodology this way:

> *We can convert the bytes from the recording in real-time at the IP-packet layer. Essentially, we wait until we record an entire IP packet from the stream (a matter of milliseconds normally) and then immediately write that packet to disk. As an attacker, you do need to know what kind of data you want to extract from the “noise” of people visiting Facebook and so forth. To do that, you can use IP addresses or other traffic signatures to identify just the most relevant traffic to respond to programmatically.*

A problem in search of a solution

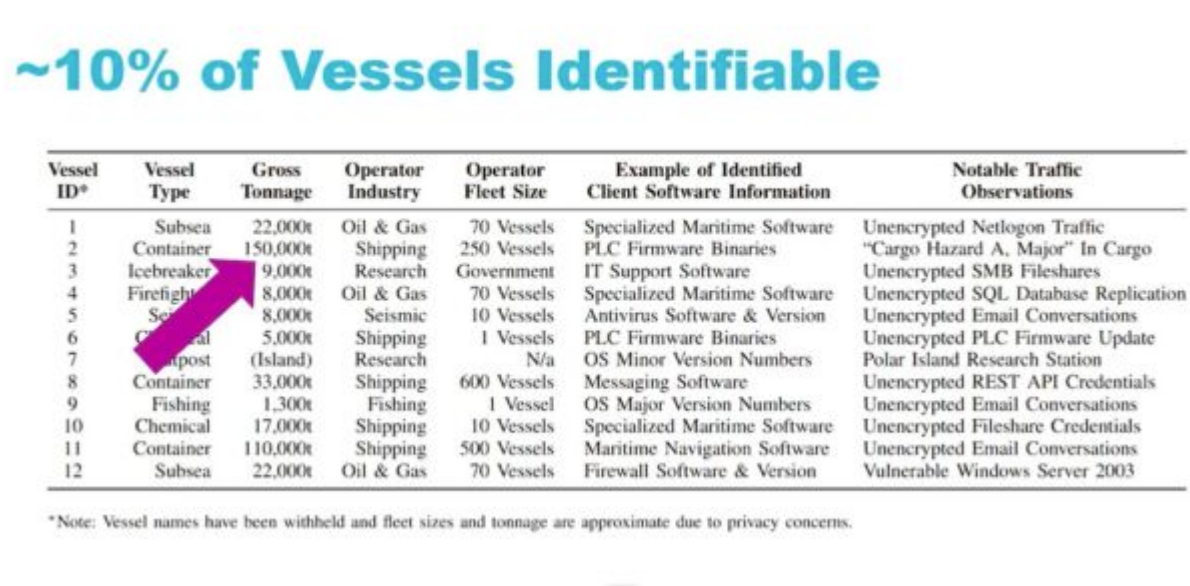
The common reaction Pavur gets after he shares his findings is that satellite-based Internet users should simply use a VPN to prevent attackers from reading or tampering with any data sent. Unfortunately, he said, the handshakes required for each endpoint to authenticate itself to the other results in a slow-down of about 90 percent. The overhead increases the already-large 700 millisecond latency to a wait that renders satellite Internet almost completely unusable.

And while HTTPS and transport-level encryption for email prevent attackers from reading the body of pages and messages, most domain-lookup queries continue to be unencrypted. Attackers can learn plenty by scrutinizing the data. HTTPS certificates allow attackers to fingerprint servers customers connect to.



Enlarge / Left: an unencrypted DNS response shows a satellite Internet user is visiting Dropbox. Right: a breakdown of the most commonly visited domains.
James Pavur

That information allows attackers to identify users who are worthy of more targeted attacks. Out of 100 ships Pavur pseudo-randomly looked at, he was able to deanonymize about 10 and tie them to specific vessels.



Vessel ID*	Vessel Type	Gross Tonnage	Operator Industry	Operator Fleet Size	Example of Identified Client Software Information	Notable Traffic Observations
1	Subsea	22,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted Netlogon Traffic
2	Container	150,000t	Shipping	250 Vessels	PLC Firmware Binaries	"Cargo Hazard A, Major" In Cargo
3	Icebreaker	9,000t	Research	Government	IT Support Software	Unencrypted SMB Fileshares
4	Firefight	8,000t	Oil & Gas	70 Vessels	Specialized Maritime Software	Unencrypted SQL Database Replication
5	Se	8,000t	Seismic	10 Vessels	Antivirus Software & Version	Unencrypted Email Conversations
6	C al	5,000t	Shipping	1 Vessels	PLC Firmware Binaries	Unencrypted PLC Firmware Update
7	post	(Island)	Research	N/a	OS Minor Version Numbers	Polar Island Research Station
8	Container	33,000t	Shipping	600 Vessels	Messaging Software	Unencrypted REST API Credentials
9	Fishing	1,300t	Fishing	1 Vessel	OS Major Version Numbers	Unencrypted Email Conversations
10	Chemical	17,000t	Shipping	10 Vessels	Specialized Maritime Software	Unencrypted Fileshare Credentials
11	Container	110,000t	Shipping	500 Vessels	Maritime Navigation Software	Unencrypted Email Conversations
12	Subsea	22,000t	Oil & Gas	70 Vessels	Firewall Software & Version	Vulnerable Windows Server 2003

*Note: Vessel names have been withheld and fleet sizes and tonnage are approximate due to privacy concerns.

Enlarge / Ships Pavur deanonymized.
James Pavur

The interception of unencrypted navigational charts, equipment failures in the open sea, and the use of vulnerability-riddled Windows 2003 servers also puts users at considerable risk. Combined with the use of insecure channels such as FTP, an attacker might be able to tamper with maritime data to hide a sandbar or use the data to plan physical intrusions.

The sheer scale of the problem put the researcher in a quandary. With tens of thousands of users affected, Pavur was unable to privately notify the vast majority of them. He settled on contacting the largest companies who were transmitting particularly sensitive data in the clear. He ultimately chose not to identify any of the affected users or companies because, he said, the crux of the problem is the result of industrywide protocols that are insecure.

“The goal of my research is to bring out these unique dynamics that the physical properties of space create for cybersecurity, and it’s an area that’s been underexplored,” he said. “A lot of people think that satellites are just normal computers that are a little bit further away, but there’s a lot that’s different about satellites. If we highlight those differences, we can better build security to protect the systems.”

https://arstechnica.com/?p=1696924