Are we safe in the “Internet from Space”?

Diogo Barradas

David R. Cheriton School of Computer Science
University of Waterloo

UNIVERSITY OF
WATERLOO

What is satellite Internet and how does it work?

- Internet access provided through communication satellites in space

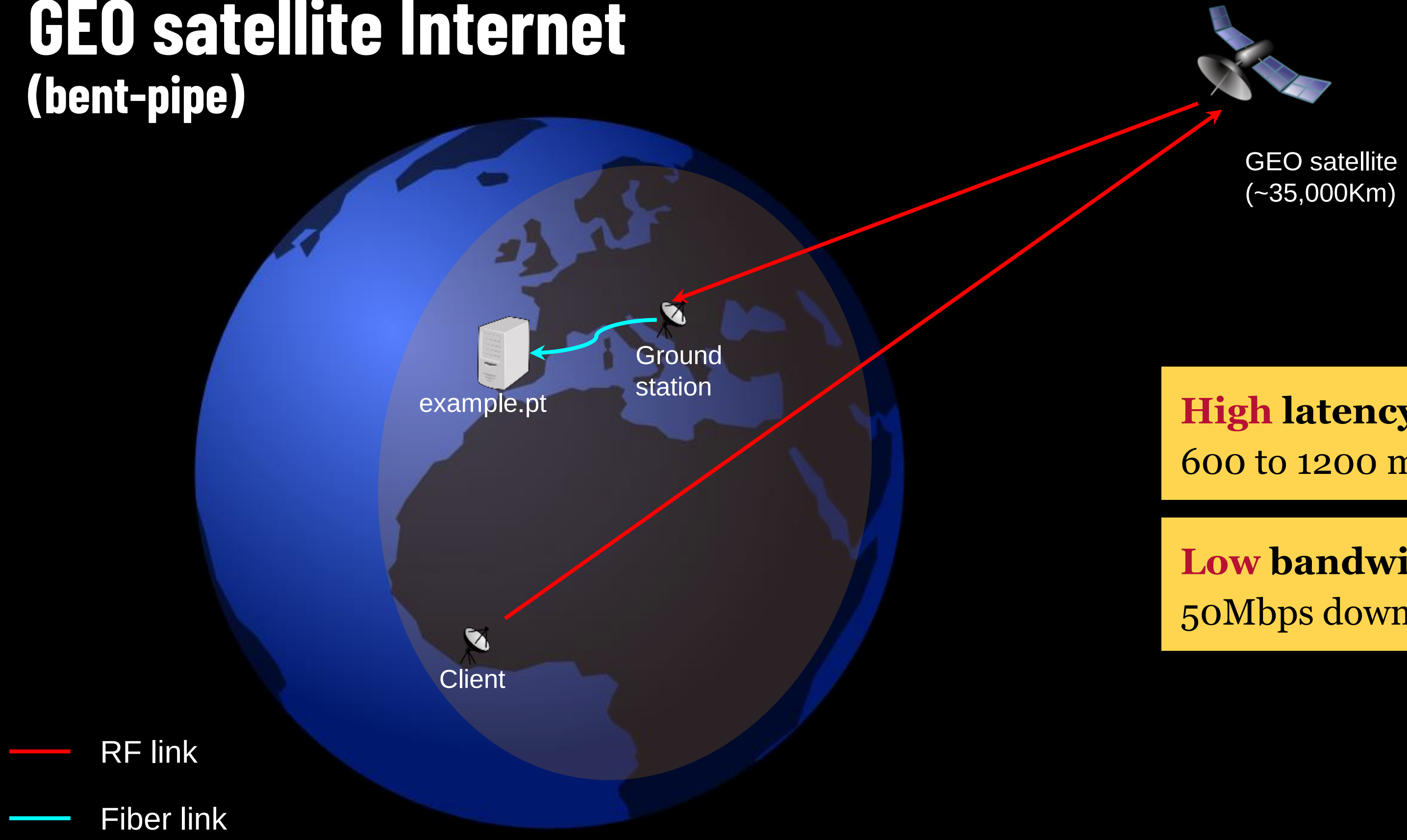
- Clients use a dish antenna to send and receive information from a satellite
  - No need for fiber or cabled connections

- Able to connect rural, remote, or indigenous communities in a cost-effective way
  - Helps bridge the digital divide

Do all satellite broadband connections work the same?

eutelsat

GEO satellite Internet
(bent-pipe)

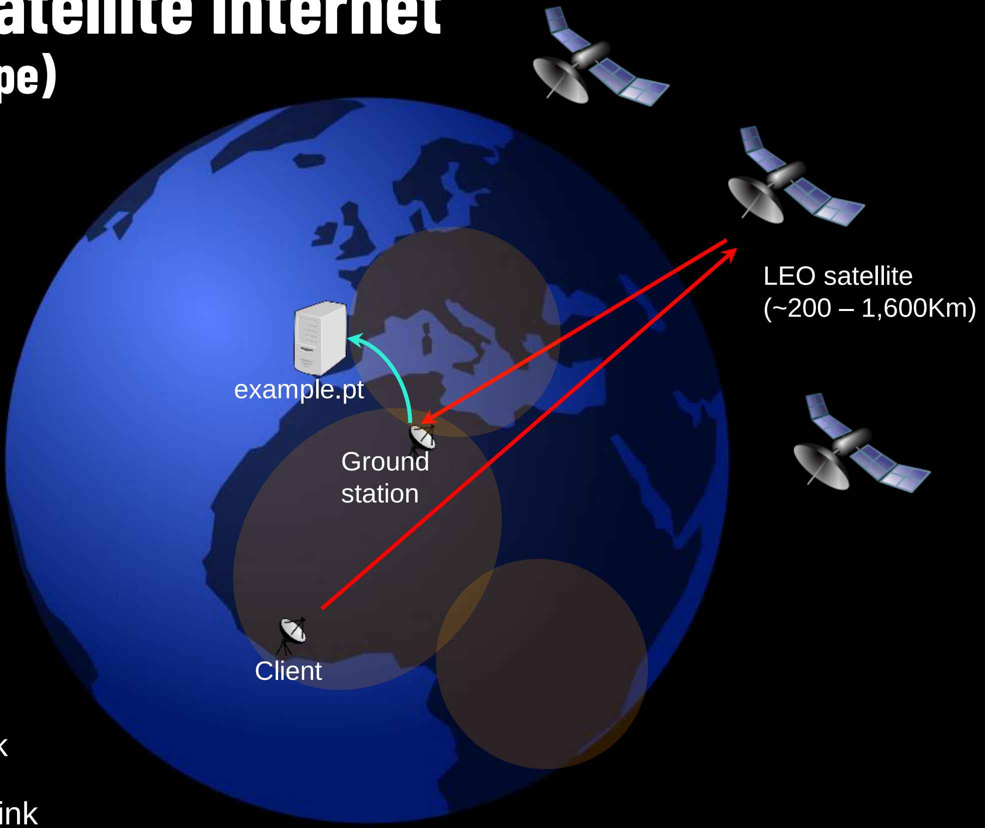


High latency:
600 to 1200 milliseconds

Low bandwidth:
50Mbps download / 6Mbps upload

LEO satellite Internet
(bent-pipe)

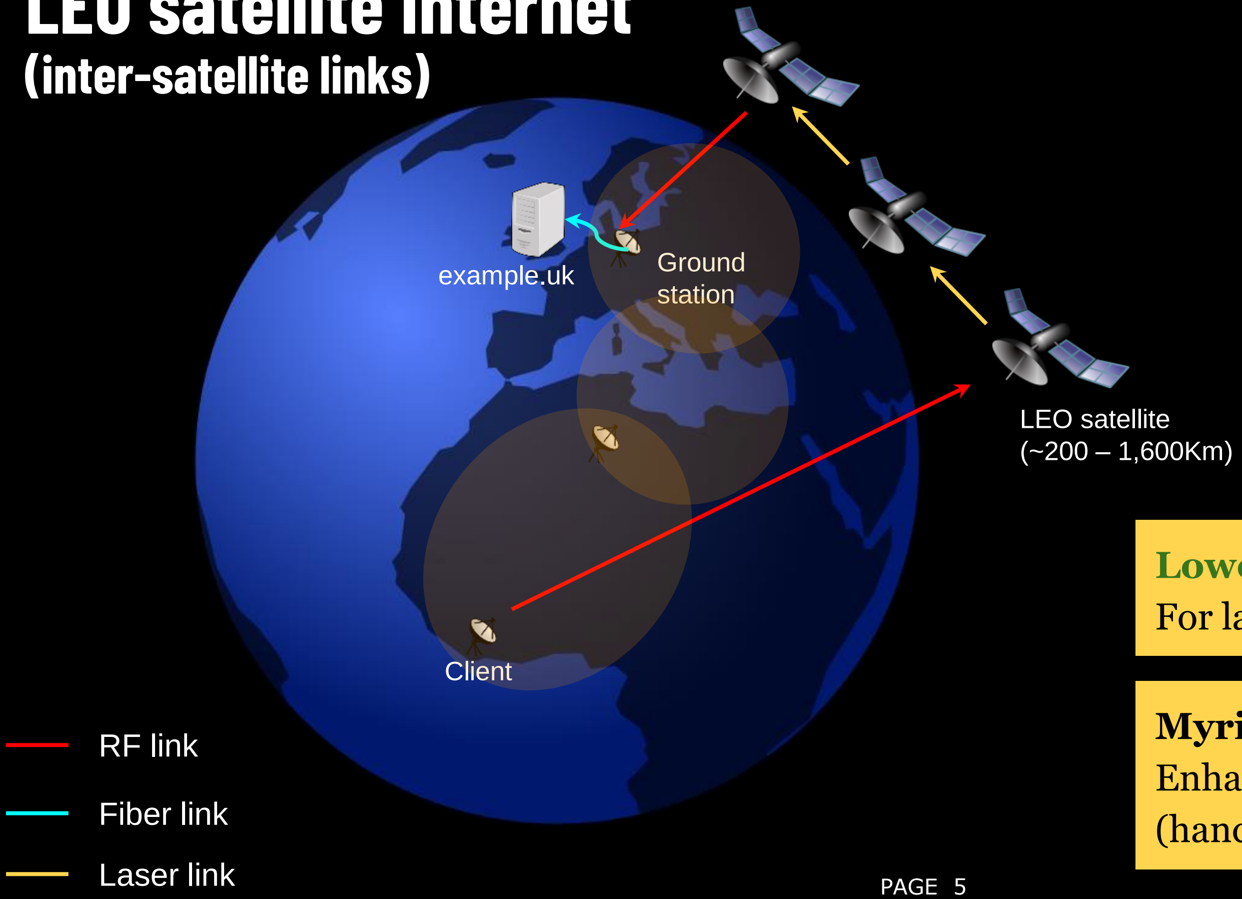
Globalstar



Low latency:
~10s to 100 milliseconds

High throughput:
~100s Mbit to Gbps speeds

LEO satellite Internet
(inter-satellite links)



Lower latency than fiber:
For large terrestrial routes

Myriad opportunities:
Enhanced routing, other optimizations (hand-off, service placement, etc.)

“Right, but this sounds a bit like science fiction”

However, it is very much real!

- Many companies are launching their own constellations
  - Low-cost satellite launches & COTS components
- Opportunities for new services and applications
  - Civilian & military usage (e.g., DARPA Blackjack)
  - Also fostering new research avenues

AALYRIA

OneWeb

Telesat Lightspeed™

STARLINK

amazon | project kuiper

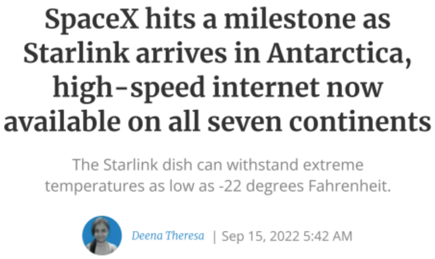
UNIVERSITY OF WATERLOO

Imagination is the limit

- High-speed satellite Internet
  - no more sluggish connections

- Geospatial data analysis
  - AI-powered data analytics for tracking and monitoring

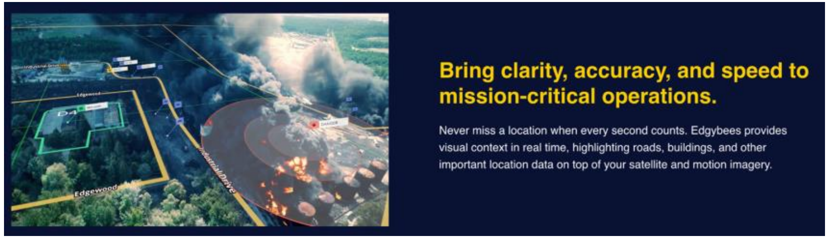
- Edge computing & micro datacenters
  - offload data and analytics, minimize bandwidth requirements



SpaceX hits a milestone as Starlink arrives in Antarctica, high-speed internet now available on all seven continents

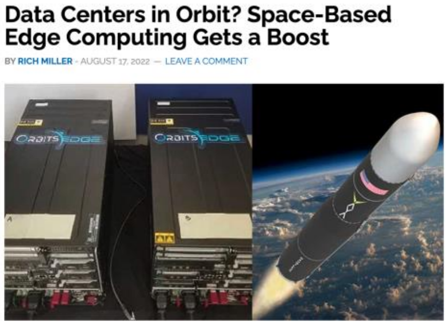
The Starlink dish can withstand extreme temperatures as low as -22 degrees Fahrenheit.

Deena Theresa | Sep 15, 2022 5:42 AM



Bring clarity, accuracy, and speed to mission-critical operations.

Never miss a location when every second counts. Edgybees provides visual context in real time, highlighting roads, buildings, and other important location data on top of your satellite and motion imagery.



Data Centers in Orbit? Space-Based Edge Computing Gets a Boost

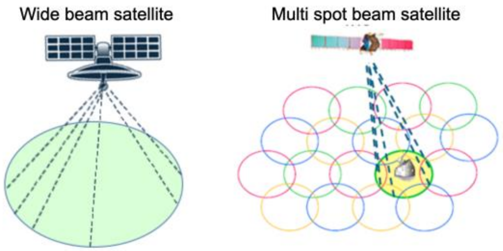
BY RICH MILLER - AUGUST 17, 2022 — LEAVE A COMMENT

This all sounds pretty cool! But how safe is my data?

There are three important **security concerns**:

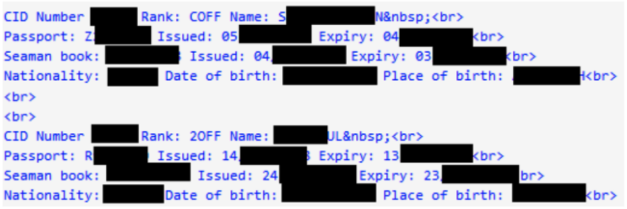
- Large beaming radius
- Easy to intercept
- (Often) no encryption

How can we secure our satellite Internet links?



$300 of TV Equipment
Selfsat H30D ~$90 (or any old satellite dish + LNB off Craigslist)
TBS-6983/6903 ~$200-$300 (or comparable PCIE DVB-S tuner, ideally with APSK support)

Crew Passport Data Transmitted to Port Authorities

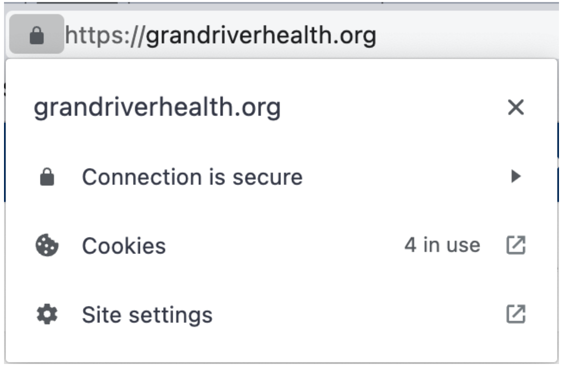


```
CID Number [redacted] Rank: COFF Name: S[redacted]N&nbsp;<br>
Passport: Z[redacted] Issued: 05[redacted] Expiry: 04[redacted]<br>
Seaman book: [redacted] Issued: 04[redacted] Expiry: 03[redacted]<br>
Nationality: [redacted] Date of birth: [redacted] Place of birth: [redacted]<br>
<br>
<br>
CID Number [redacted] Rank: 2OFF Name: [redacted]UL&nbsp;<br>
Passport: R[redacted] Issued: 14[redacted] Expiry: 13[redacted]<br>
Seaman book: [redacted] Issued: 24[redacted] Expiry: 23[redacted]br>
Nationality: [redacted]Date of birth: [redacted] Place of birth: [redacted]<br>
```

[Whispers Among the Stars, James Pavur, Oxford University, BlackHat 2020]

Satellite Internet is still the Internet

- Transport Layer Security (TLS) can be used to encrypt the content of communications
  - Widely adopted
  - Your browser can even do it for you



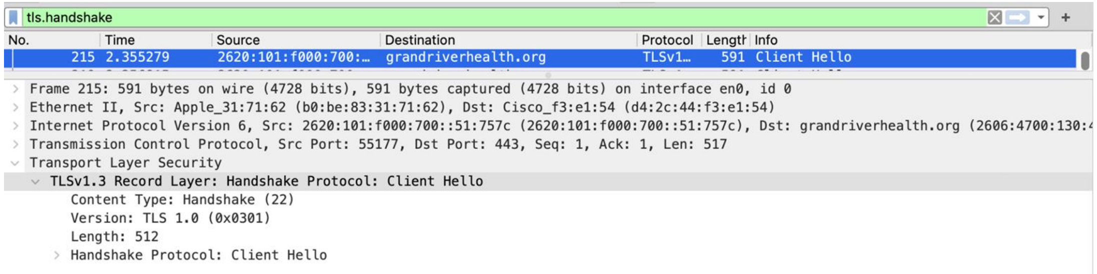
https://grandriverhealth.org

grandriverhealth.org ✕

Connection is secure ▸

Cookies 4 in use

Site settings

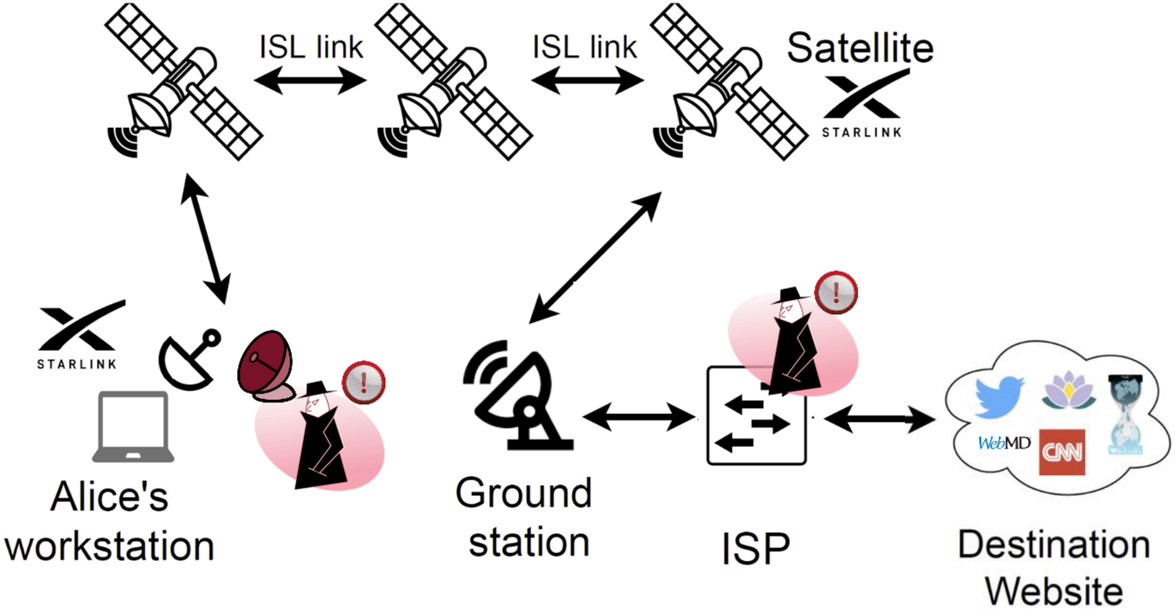


```
tls.handshake
No.        Time        Source                Destination               Protocol  Lengtŀ Info
      215  2.355279    2620:101:f000:700:…   grandriverhealth.org      TLSv1…      591  Client Hello

> Frame 215: 591 bytes on wire (4728 bits), 591 bytes captured (4728 bits) on interface en0, id 0
> Ethernet II, Src: Apple_31:71:62 (b0:be:83:31:71:62), Dst: Cisco_f3:e1:54 (d4:2c:44:f3:e1:54)
> Internet Protocol Version 6, Src: 2620:101:f000:700::51:757c (2620:101:f000:700::51:757c), Dst: grandriverhealth.org (2606:4700:130:4
> Transmission Control Protocol, Src Port: 55177, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    > Handshake Protocol: Client Hello
```

TLS does not hide everything!
e.g., destination, connection duration

Where is the adversary?

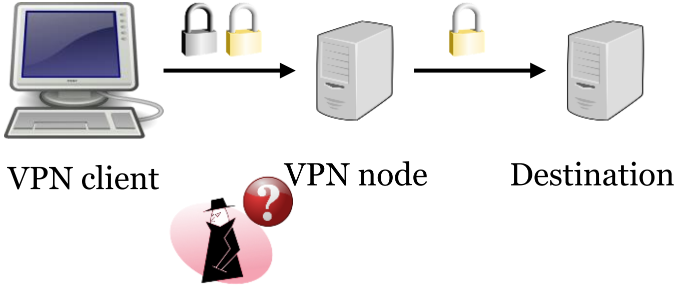


UNIVERSITY OF WATERLOO

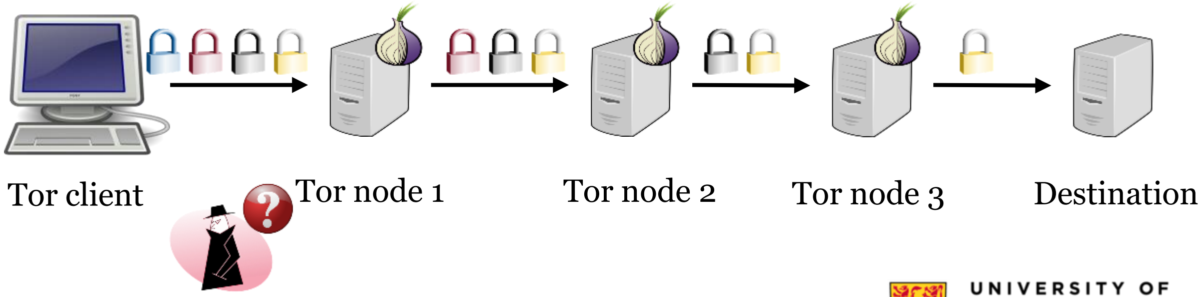
So what can I do to protect this information?

Key idea:
Hop around!

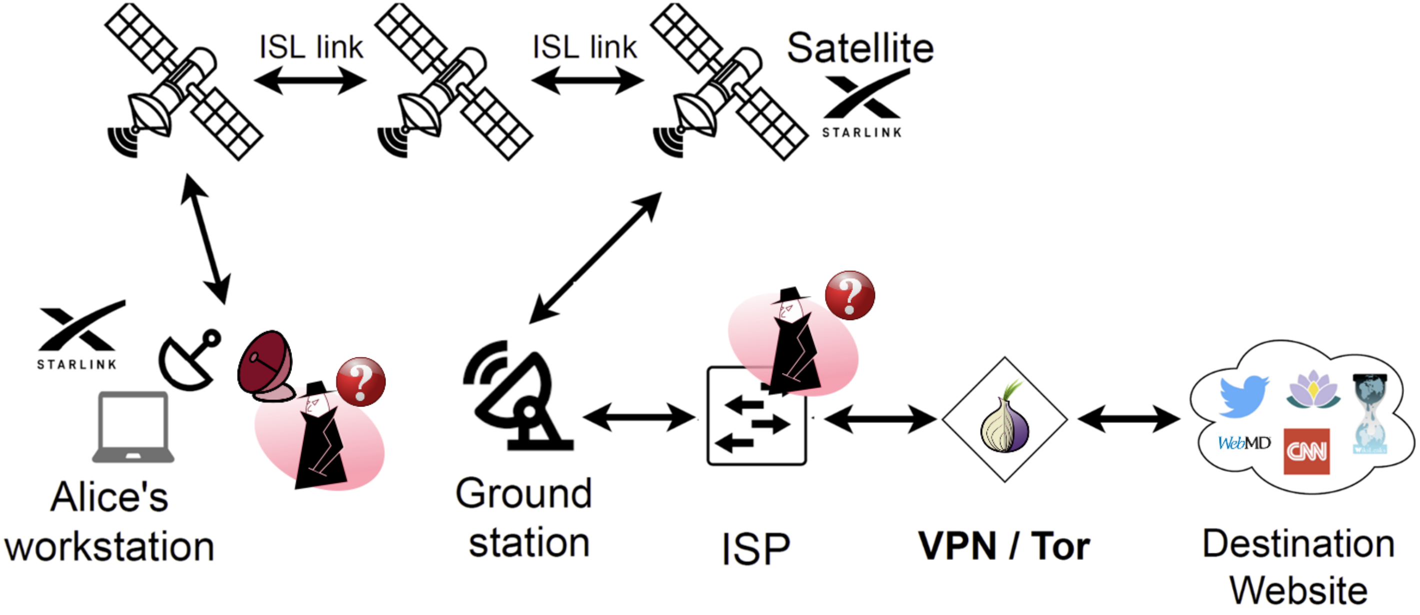
Virtual Private Networks



Anonymity networks
e.g., Tor

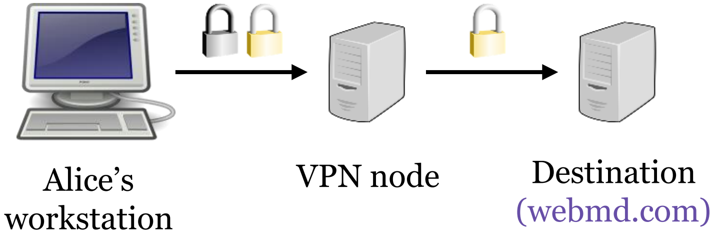


Satellite Internet users can also apply these mechanisms

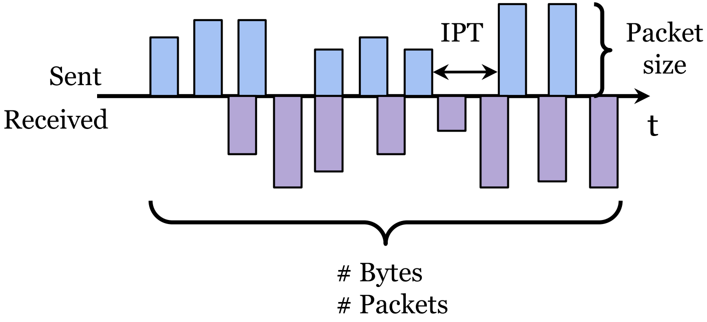


Game over for eavesdroppers, right?

There's actually more than meets the eye...



Packet flow:



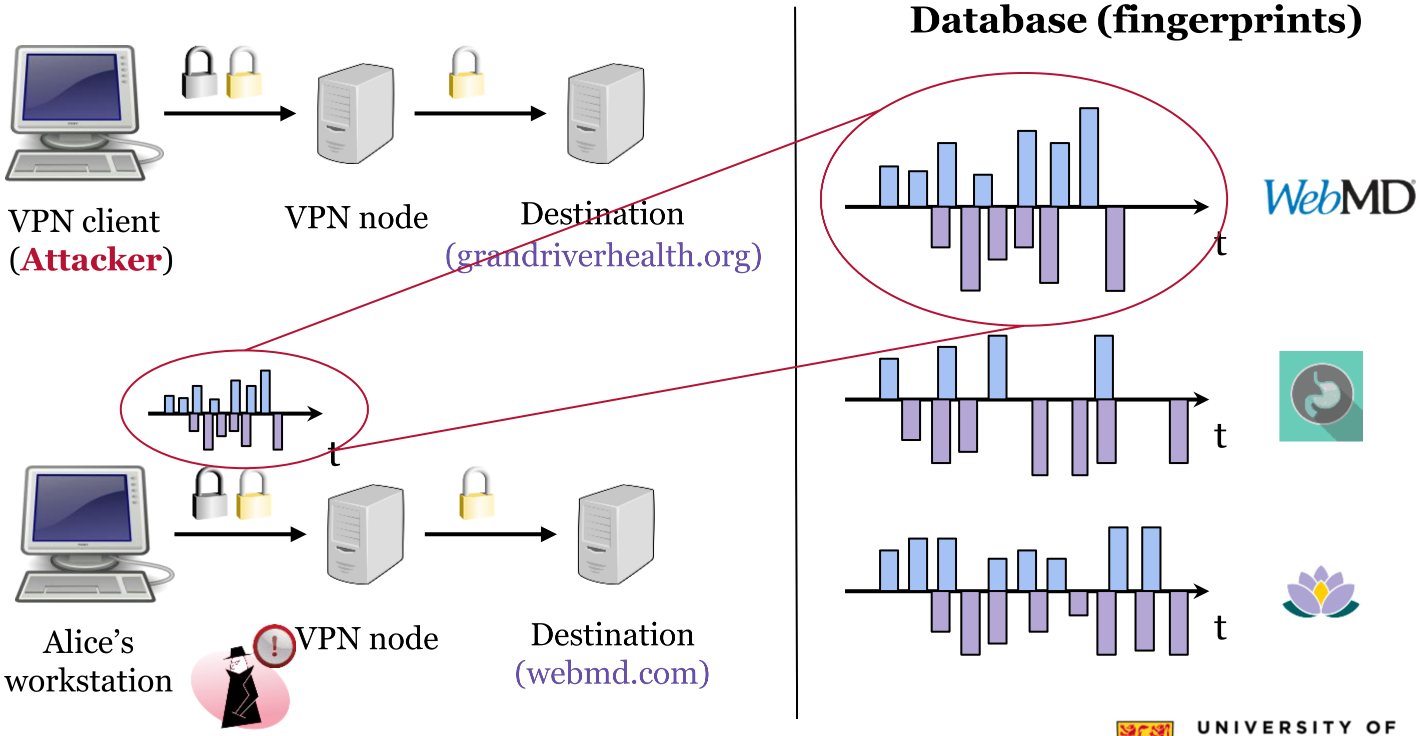
Observation:
VPNs and Tor **leak metadata** like the volume, direction, and timing information that characterize a given website

Website Fingerprinting attack:
Create a database of website traces and try to match Alice's traffic patterns

How does website fingerprinting work?

Step 1:
Build database

Step 2:
Match Alice’s traffic



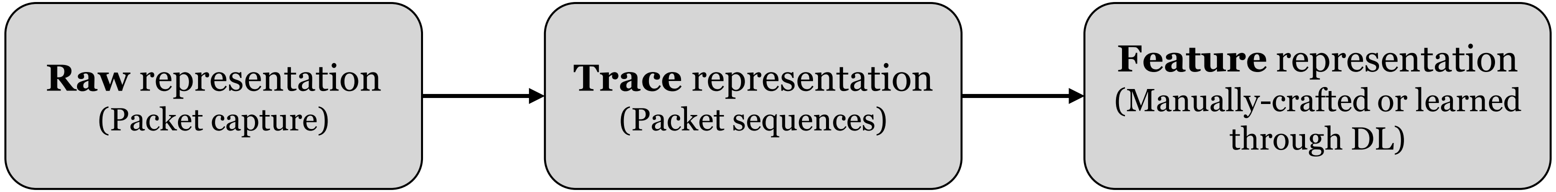
In practice, matching fingerprints is more difficult than that...

- No two website accesses are the same!
  - Users have **different** machines, browser configurations, etc.
  - Network conditions are **not static**

- This causes **uncertainty** when matching fingerprints

How do adversaries reduce this uncertainty?

Machine learning-assisted website fingerprinting pipeline:



Raw representation (Packet capture) → **Trace** representation (Packet sequences) → **Feature** representation (Manually-crafted or learned through DL)

Defences against website fingerprinting

(and prototyped over Tor)

Constant-rate padding
CS-BuFLO, Tamaraw

Supersequence
Glove, Walkie-Talkie

Adaptive Padding
WTF-PAD

Application-layer
LLaMA, ALPaCA

Traffic splitting
HyWF, TrafficSliver

Trace noise/merge
FRONT/Glue

Adversarial defences
Mockingbird, BLANKET

Synthetic traffic
Surakav

Some are impractical

Some are inefficient

None evaluated in satellite links

Challenges and Opportunities

- **How difficult is it** to fingerprint traffic over satellite links?
  - Different link properties than terrestrial links
  - Added **latency, jitter, packet drops**
  - Different transport protocol behaviour
- Can we **lower bound** an adversary's capabilities?
  - Different interception settings
    - At the backhaul, antenna placed close to clients, downlink only
- Can we build **enhanced defences**?
  - Existing WF defences impose severe performance overheads
  - A big issue assuming limited traffic plans

Takeaways

- We are facing a **rise in the adoption** of satellite Internet solutions
  - And a wealth of networked space-based services being designed

- Satellite Internet links are **susceptible** to traffic analysis
  - Just like the regular/terrestrial Internet

- We are working towards **assessing the security** of satellite Internet users
  - Against the analysis of communication metadata

Thank you!
Questions?