LEO Lessons from Hacking GEO Broadband

James Pavur, Oxford University

james.pavur@cs.ox.ac.uk / james@pavursec.com

What is Special About Space Cyber-Security?

How should we study it?

“RCMA” Method

1

Recognize

Unique physical needs affecting domain technology

2

Connect

Physical technology adaptations with their security implications

3

Motivate

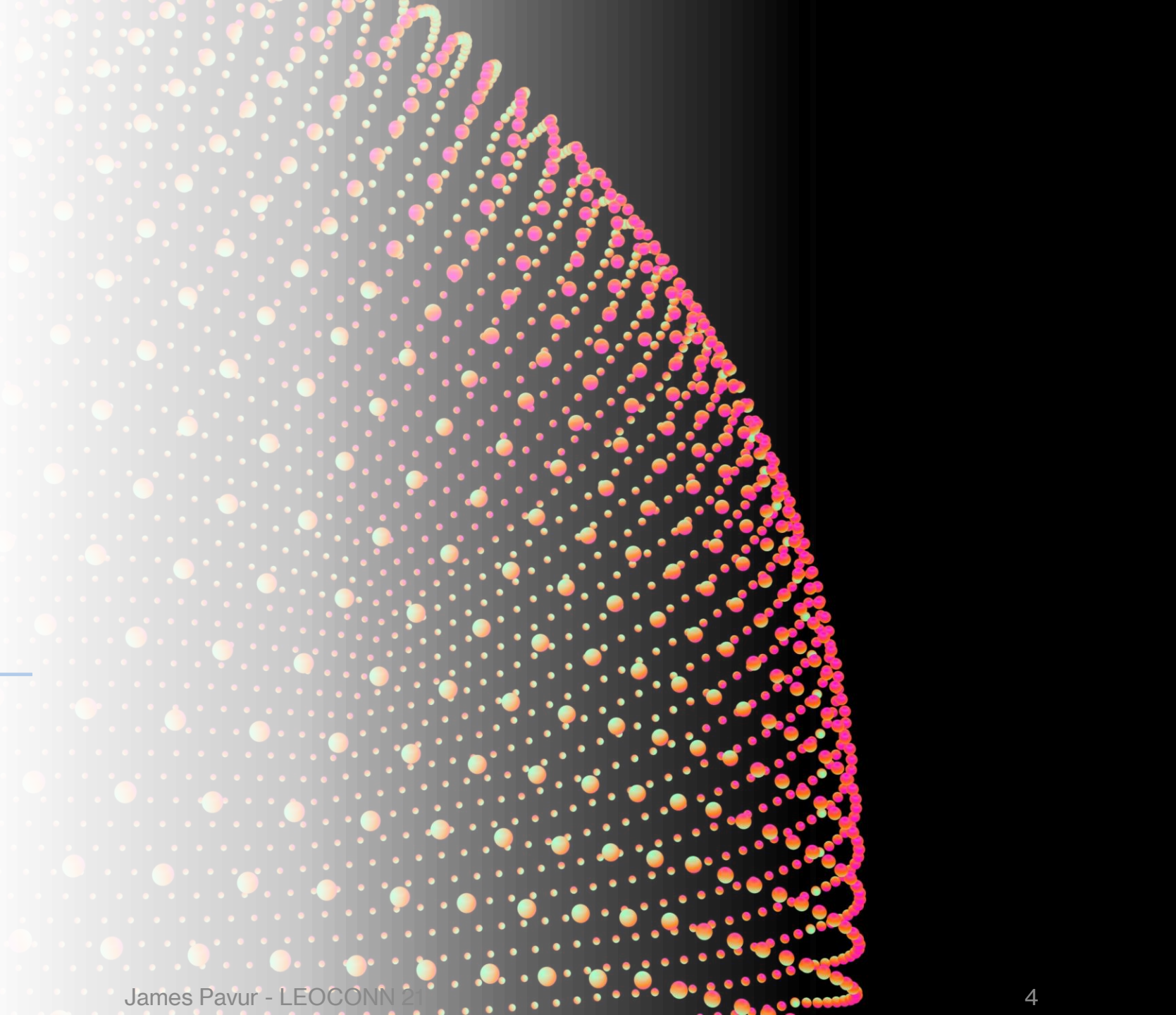
Security needs in context of operational requirements

4

Adapt

Existing security practices to unique domain properties

Case Study: GEO Broadband Security



1

Key Properties

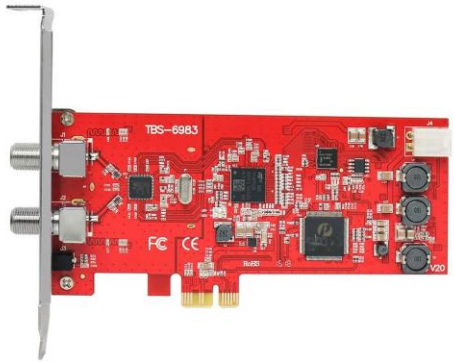
VAST COVERAGE

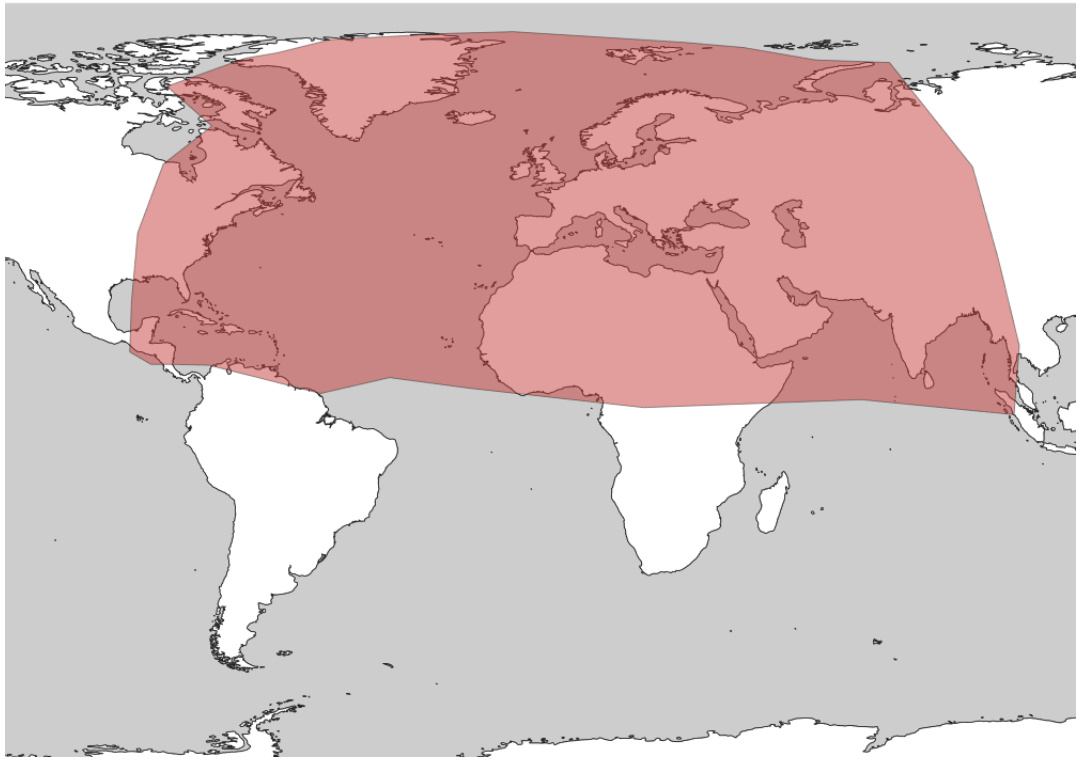
HIGH LATENCY

REGULATED SPECTRUM

The Experiments

2





Signal Challenges

2

- Proper Equipment = Expensive
- Our Equipment -> Signal Errors
  - Complex modulations
  - Proprietary protocol modifications
- Solution: GSExtract
  - github.com/ssloxford/gsextract
  - Focus on the “easy” bits
  - Brute force is cheap
  - Accuracy not *that* important

What's Inside?

3

9 FORTUNE GLOBAL 500 MEMBERS

6 OF 10 LARGEST AIRLINES

~40% MARITIME CARGO MARKET

GOVERNMENTAL AGENCIES

YOU?

Privacy

3

Email Communications

Subject: Microsoft account password reset
To: captain@[redacted].com
X-Priority: 3
X-MSAPipeline: MessageDispatcherEOP
Message-ID: [redacted]
X-MSAMetaData:
=?us-ascii?q?[redacted]
=?us-ascii?q?[redacted]
=?us-ascii?q?[redacted]
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="[redacted]"
Return-Path: account-security-noreply@accountprotection.microsoft.com
X-EOPAttributedMessage: 0
X-Forefront-Antispam-Report:

Crew Passport Data

CID Number [redacted] Rank: COFF Name: S[redacted]N
Passport: Z[redacted] Issued: 05[redacted] Expiry: 04[redacted]
Seaman book: [redacted] Issued: 04[redacted] Expiry: 03[redacted]
Nationality: [redacted] Date of birth: [redacted] Place of birth: [redacted]H

CID Number [redacted] Rank: 2OFF Name: [redacted]UL
Passport: R[redacted] Issued: 14[redacted] Expiry: 13[redacted]
Seaman book: [redacted] Issued: 24[redacted] Expiry: 23[redacted]br>
Nationality: [redacted] Date of birth: [redacted] Place of birth: [redacted]

IoT & Maritime

3


```
Transmission Control Protocol, Src Port: 21, Dst Port: 41573, S
File Transfer Protocol (FTP)
  257 "/Inbox/chartdelivery" is current directory.\r\n
      Response code: PATHNAME created (257)
      Response arg: "/Inbox/chartdelivery" is current directory.
```

Aviation

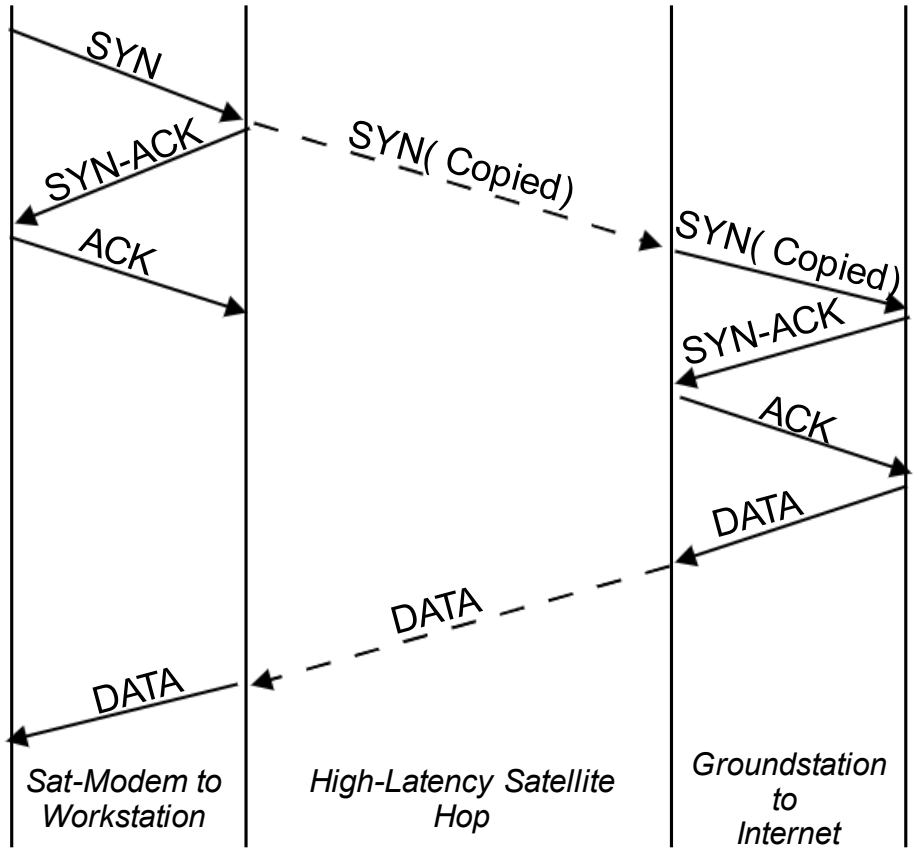
3

```
T [redacted] -> 10.48.[redacted]:50684 [AFP] #127
  HTTP/1.0 302 Moved Temporarily..Content-Type: text/html..Location:
  http://172.[redacted]:80?[redacted]&userurl=http
  ://efb.[redacted]/efb/api/v1/taskSheet/getUnsavedTsCaptains.do?soflSeqNrs=[redacted]
  [redacted]&fltNrs=[redacted]&schDepDts=[redacted]
  [redacted]&depCds=[redacted],PVG&arvCds=PVG,[redacted]

T [redacted]:80 -> 10.48.[redacted]:61044 [AFP] #913
  HTTP/1.0 302 Moved Temporarily..Content-Type: text/html..Location:
  http://172.[redacted]:80?[redacted]&userurl=http:
  //efb.[redacted]/efb/api/v1/flightPlan/getWayPoint.do?fltNr=[redacted]
  [redacted]&tailNr=[redacted]
  [redacted]&alnCd=[redacted]&depCd=[redacted]&arvCd=PEK&rescheduledFltDt=[redacted]&sofl
  SeqNr=[redacted]

T [redacted] -> [redacted]:55070 [AFP] #820
  HTTP/1.0 302 Moved Temporarily..Content-Type: text/html..Location:
  http://172[redacted]:80?[redacted]&userurl=http:/
  /efb.[redacted]/efb/api/v1/weather/sweatherquery.do?latitude=56.[redacted]&longi
  tude=[redacted]
```

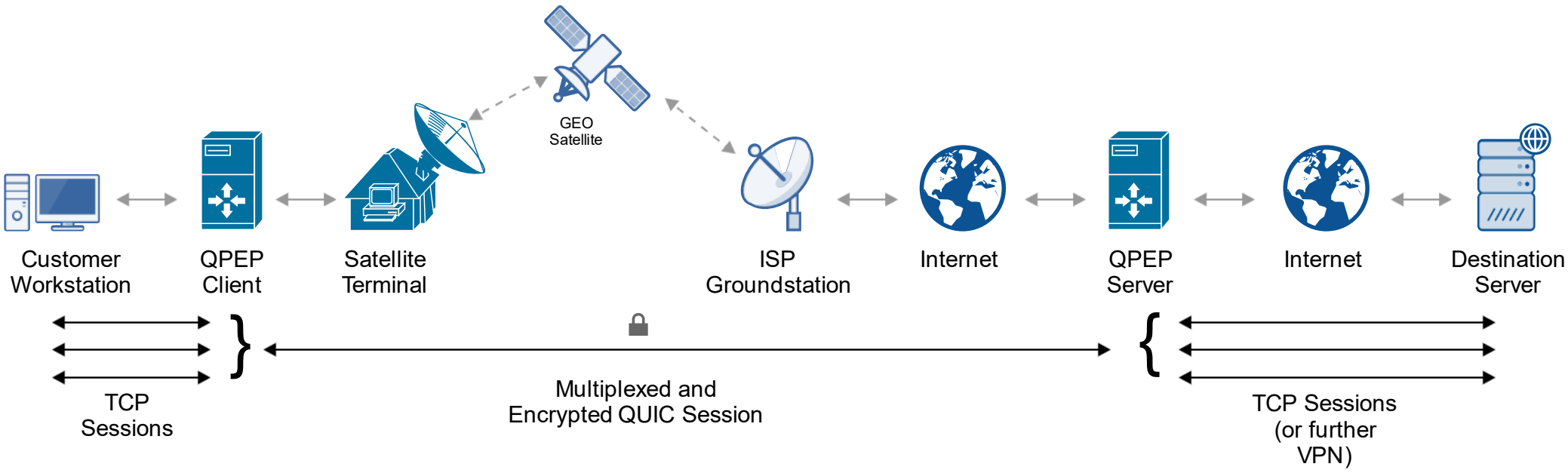
```
> UTRAN Iuh interface RUA signalling
> Radio Access Network Application Part
> GSM A-I/F DTAP - CP-DATA
> GSM A-I/F RP - RP-DATA (Network to MS)
v GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
    .1.. .... = TP-UDHI: The beginning of the TP UD field contains a Header in addition to the short message
    ..0. .... = TP-SRI: A status report shall not be returned to the SME
    .... 0... = TP-LP: The message has not been forwarded and is not a spawned message
    .... .0.. = TP-MMS: More messages are waiting for the MS in this SC
    .... ..00 = TP-MTI: SMS-DELIVER (0)
  > TP-Originating-Address - [redacted]
  > TP-PID: 0
  > TP-DCS: 8
  > TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (140) depends on Data-Coding-Scheme
  v TP-User-Data
    > User-Data Header
      SMS text: Name: [redacted]D\nTest Result: Negative - \nResult Date: [redacted]
```

Why does this happen?

- Space is *far* and round-trip times (RTT) to GEO are long
- TCP especially troublesome because of the 3-way handshake
- ISP = Benevolent “attacker” snooping on your traffic
  - But they can’t do this if you use a VPN



QPEP: Mitigation

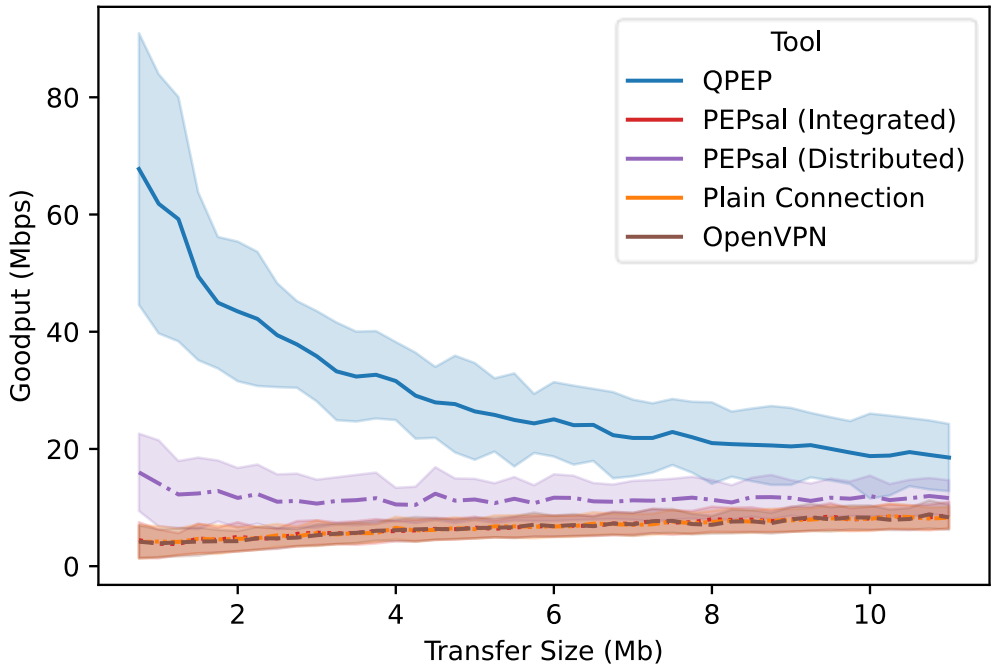


Contribute / Try It Out: https://github.com/ssloxford/qpep

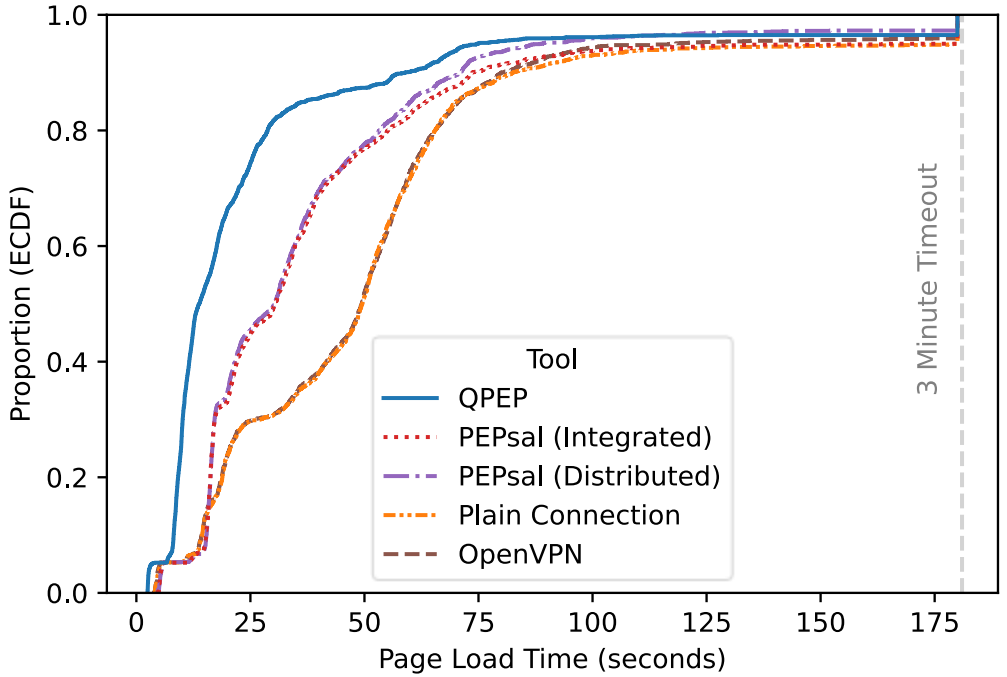
QPEP: Performance

4

IPERF Goodput vs. Transfer Size



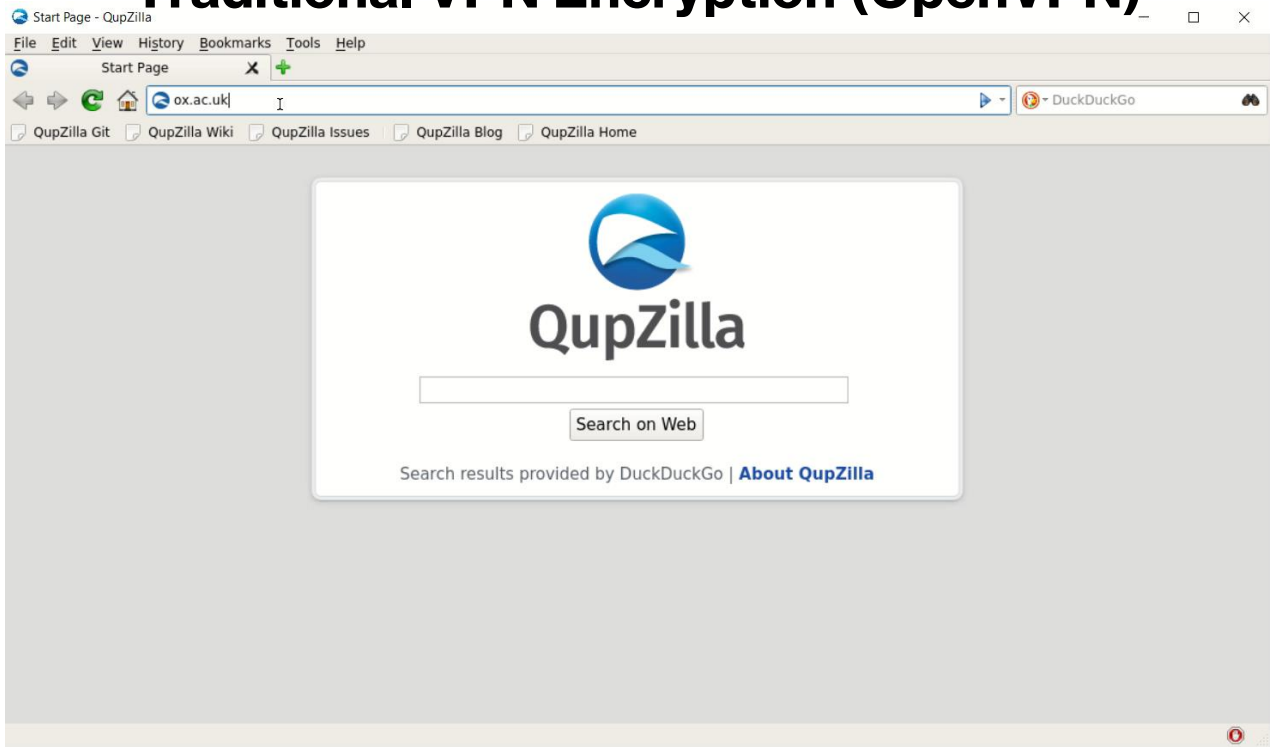
PLT over Alexa Top 20



Bottom Line

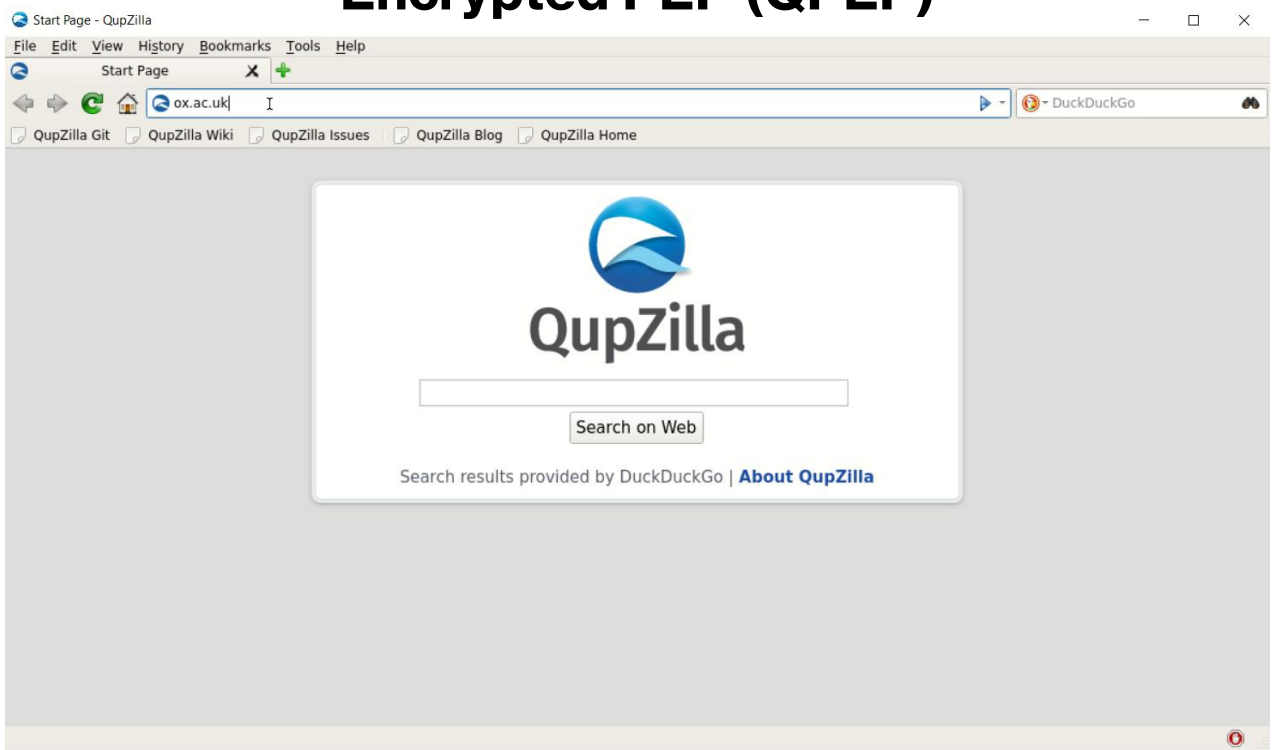
4

Traditional VPN Encryption (OpenVPN)



~25 seconds

Encrypted PEP (QPEP)



~14 seconds

VSAT Case Study Takeaways

1

Recognize

Physical aspects of GEO broadband have required adaptations in network design (PEPs)

2

Connect

PEPs discourage over-the-air encryption while physical coverage of GEO services benefits eavesdroppers

3

Motivate

Attackers can use inexpensive hardware to compromise sensitive infrastructure and transport networks

4

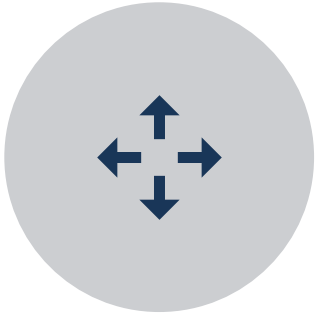
Adapt

Hybrid VPN+PEP model obviates security vs. performance tradeoff

Let’s Talk LEO

Properties of LEO Networks

1



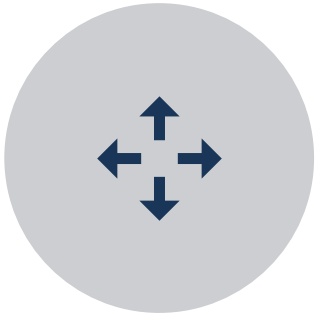
MOBILE FOOTPRINTS

INTER-SATELLITE LINKS

LOWER ALTITUDES

Security Connections

2

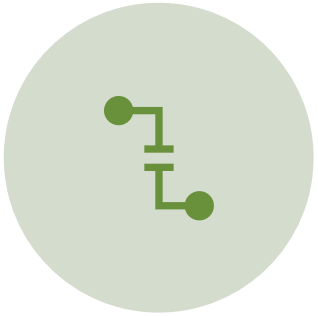


MOBILE FOOTPRINTS

INTER-SATELLITE LINKS

LOWER ALTITUDES

“ORPHAN” PERIODS



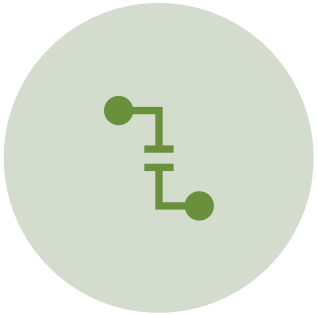
LINK SATURATION / DESTRUCTION

RADIO INTERFERENCE

Operational Motivations

3

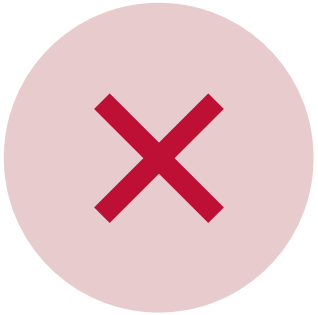
“ORPHAN” PERIODS



LINK SATURATION / DESTRUCTION

RADIO INTERFERENCE

DEVICE HIJACKING

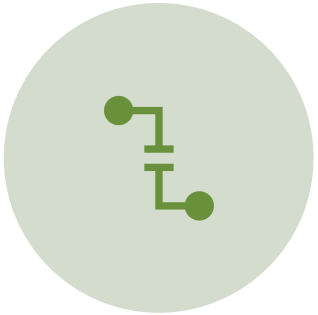


DENIAL OF SERVICE

CENSORSHIP

Possible Mitigations

“ORPHAN” PERIODS



LINK SATURATION / DESTRUCTION

RADIO INTERFERENCE

LOCATION-AWARE PERMISSIONS

RESILIENT ISL ROUTING

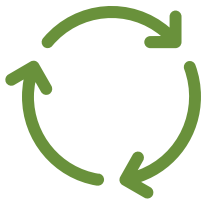
SPECTRUM POLICY AGREEMENTS

Concluding Thoughts

Themes for Effective Space Security

Physicality

Interdisciplinarity



Adaptability

Questions/Thoughts?:
james.pavur@cs.ox.ac.uk or james@pavursec.com