SpaceSec

Workshop on Satellite and Space Systems Security

Co-Chairs
Martin Strohmeier - Armasuisse, Cyber-Defence Campus
Johannes Willbold - Ruhr University Bochum

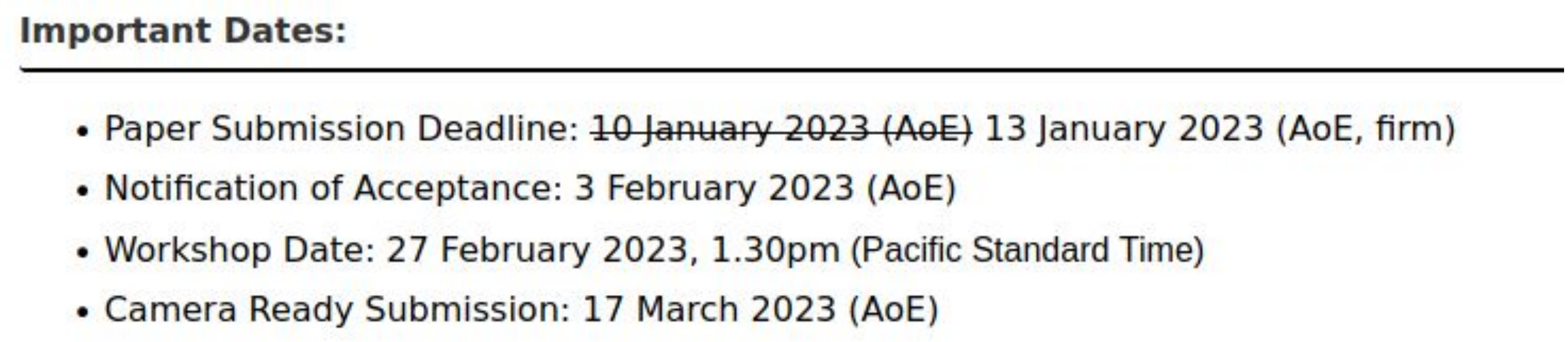
Numbers

First time workshop
Half-day
27th February

19 Submissions
10 Accepts
3-4 Reviews/Paper

Full Room
~60 In-Person
~15 Virtual

Workshop Proceedings



Important Dates:

- Paper Submission Deadline: ~~10 January 2023 (AoE)~~ 13 January 2023 (AoE, firm)
- Notification of Acceptance: 3 February 2023 (AoE)
- Workshop Date: 27 February 2023, 1.30pm (Pacific Standard Time)
- Camera Ready Submission: 17 March 2023 (AoE)

How did it go?

Traditional Workshop Format
Extended Discussions

Research/WIP/Position Papers

Traditionally Inaccessible
Merge Space & Sec Research
Fuse Different Research Institutions

Presentation Topics

4+1 topics on the final frontier of security

CDAO

DIRECTORATE FOR DIGITAL SERVICES

SECURING THE COSMOS

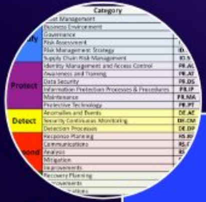
ON THE FUTURE OF SPACE SYSTEMS SECURITY RESEARCH

James Pavur, PhD.

Digital Service Expert, Directorate for Digital Services
Chief Digital and Artificial Intelligence Office, DoD
james.pavur@dds.mil | james@pavursec.com

WHAT'S DIFFERENT ABOUT SPACE SECURITY?

Defenses/Attacks Derive from Adaptations



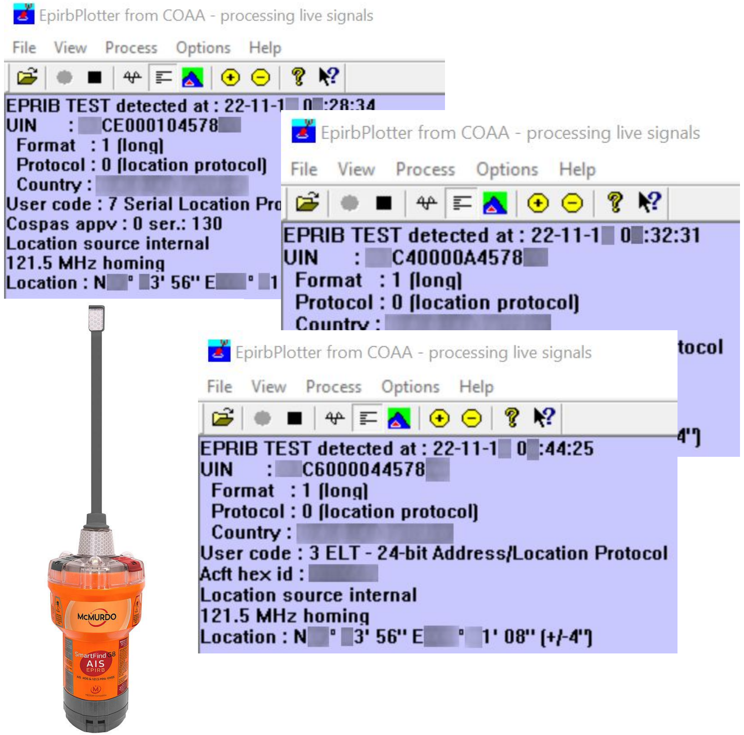
	Category	
	et Management	
ify	Business Environment	
	Governance	
	Risk Assessment	
	Risk Management Strategy	ID.
	Supply Chain Risk Management	ID.S
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
ond	Response Planning	RS.RP
	Communications	RS.C
	Analysis	RS
	Mitigation	
	Improvements	
	Recovery Planning	
	rovements	

Adaptations confound security practices

Tech adapts to domain

Space is *weird*

Session 1: Threat Modelling


EpirbPlotter from COAA - processing live signals
File View Process Options Help
McMURDO
SmartFind G8
AIS
EPIRB

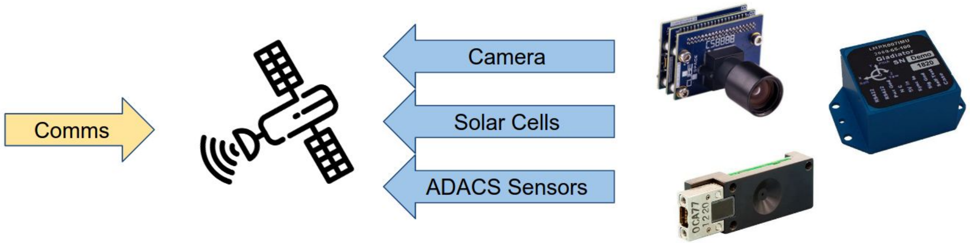
```
EPRIB TEST detected at : 22-11-1[redacted] 0[redacted]:28:34
UIN      : [redacted]CE000104578[redacted]
  Format   : 1 (long)
  Protocol : 0 (location protocol)
  Country : [redacted]
User code : 7 Serial Location Pro
Cospas appv : 0 ser.: 130
Location source internal
121.5 MHz homing
Location : N[redacted]° [redacted]3' 56" E[redacted]° [redacted]1
```

```
EPRIB TEST detected at : 22-11-1[redacted] 0[redacted]:32:31
UIN      : [redacted]C40000A4578[redacted]
  Format   : 1 (long)
  Protocol : 0 (location protocol)
  Country : [redacted]
tocol
4")
```

```
EPRIB TEST detected at : 22-11-1[redacted] 0[redacted]:44:25
UIN      : [redacted]C6000044578[redacted]
  Format   : 1 (long)
  Protocol : 0 (location protocol)
  Country : [redacted]
User code : 3 ELT - 24-bit Address/Location Protocol
Acft hex id : [redacted]
Location source internal
121.5 MHz homing
Location : N[redacted]° [redacted]3' 56" E[redacted]° [redacted]1' 08" (+/-4")
```

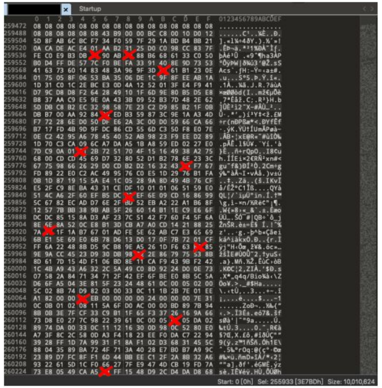
Sensors in Space

- Communication systems are a high priority
  - Primary Input, Inherently Sensitive
- But how about other inputs?
- How can sensors be influenced in unexpected ways?

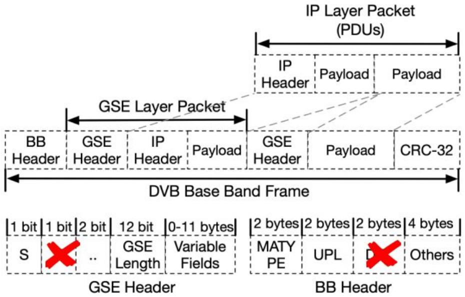


Session 2: Link Segment Security (1)

Eavesdropped Satellite Streams are Corrupted

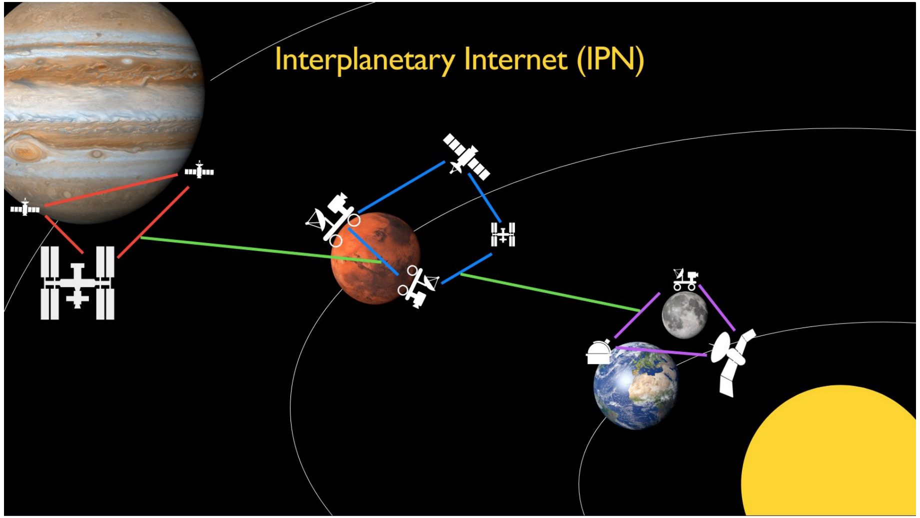


```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
259472  08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08  ................
259488  08 08 08 08 08 08 43 B9 00 00 BC C8 00 10 D0 12  ......C¹..¼È..Ð.
259504  5D 8F AB 6C BC F7 34 F0 59 7F 29 1A BD B4 BB 21  ].«l¼÷4ðY.).½´»!
259520  0A CA DE AC E4 01 AA B2 31 25 D0 C0 98 CC 83 7F  .ÊÞ¬ä.ª²1%ÐÀ˜Ìƒ.
259536  FE C0 E9 B3 DB ✗  90 AB ✗  88 B6 68 61 33 C0 50  þÀé³Û .«9ˆ¶ha3ÀP
259552  B0 D4 FF DE 57 7C F0 BE FA 33 91 40 8E 9D 73 53  °ÔÿÞW|ð¾ú3'@Ž.sS
259568  41 63 73 60 14 83 48 3A 96 9F 3D ✗  61 B1 23 0E  Acs`.ƒH:–Ÿ=‹a±#.
259584  01 75 05 8F 06 53 BA 35 06 DE 1C 9F 8F EE AB 1A  .u...Sº5.Þ.Ÿ.î«.
259600  1D 31 C0 1C 2E BC E3 0D 4A 12 52 01 3F E4 F9 41  .1À..¼ã.J.R.?äùA
259616  D7 9C D8 D8 F2 64 28 49 10 1F 6D 9E 80 B5 D5 E8  ×œØØòd(I..mž€µÕè
259632  B8 37 AA C9 E5 9E 0A 43 3B 09 52 B3 7D 48 2E 62  ¸7ªÉåž.C;.R³}H.b
259648  5D DB C8 B2 EC 32 98 58 7E 23 C2 D9 85 B2 1F 0B  ]ÛÈ²ì2˜X~#ÂÙ…²..
259664  DB B7 00 AA 92 84 ✗  ED B3 59 87 3C 9E 1A A3 4D  Û·.ª'„)í³Y‡<ž.£M
259680  F7 72 28 6E D0 50 DF E6 2A 3C 00 D0 59 66 CA 66  ÷r(nÐPßæ*<.ÐYfÊf
259696  B7 17 FD 4B 9D 9F DC 86 CD 55 6D C3 50 F8 E0 7E  ·.ýK.ŸÜ†ÍUmÃPøà~
259712  0E C2 42 95 A6 78 45 40 52 AB 98 23 F9 EE D2 89  .ÂB•¦xE@R«˜#ùîÒ‰
259728  1D 70 C3 CA 09 6C A7 DA A5 1B A8 59 ED 02 27 E0  .pÃÊ.l§Ú¥.¨Yí.'à
259744  7D C9 0A 01 ✗  2B 72 51 70 4F 15 16 49 38 A2 75  }É..ñ+rQpO..I8¢u
259760  68 00 CD CD 45 69 D7 32 80 52 D1 B2 78 6E 23 3C  h.ÍÍEi×2€RÑ²xn#<
259776  67 75 98 66 26 29 D0 CD B2 D2 16 32 43 ✗  F7 67  gu˜f&)ÐÍ²Ò.2C÷g
259792  FD 89 22 E0 C2 AC 49 95 76 C0 E5 1D 29 76 B1 FA  ý‰"àÂ¬I•vÀå.)v±ú
259808  0B 1D 87 19 15 5A E4 1C 05 28 9A 8D 49 4B 76 CF  ..‡..Zä..(š.IKvÏ
259824  E5 2F C9 8E BA 43 31 CE DF 10 01 01 06 51 59 E0  å/ÉŽºC1Îß....QYà
259840  51 4C A6 2F 60 EF B5 DC ✗  EF 6E 09 CD 16 86 99  QL¦/`ïµÜ"ïn.Í.†™
259856  5C 67 82 EC AD D7 6E 2F BD 52 EB A2 22 A1 B6 8F  \g‚ì×n/½Rë¢"¡¶.
259872  12 57 7B BB 38 9B AB 5F 26 60 14 B1 1E C9 E6 6F  .W{»8›«_&`.±.Éæo
259888  DC DC 85 15 8A D3 AF 23 7C 51 42 F7 60 F4 5F 6A  ÜÜ….ŠÓ¯#|QB÷`ô_j
259904  8E 6E 8A 52 0C E8 B1 3D CB A7 A0 CD 14 21 88 25  ŽnŠR.è±=Ë§ Í.!ˆ%
259920  7A ✗  1F 1A B7 67 01 AD FE 5E 62 AB C7 E3 65 69  z'...·g.þ^b«Çãei
259936  6B E1 5E 69 E0 6B 78 D6 13 D0 17 0F 7B 72 01 CF  ká^iàkxÖ.Ð..{r.Ï
259952  FF 6A 22 48 8B D5 9C B8 9E A5 26 1D F6 63 ✗  85  ÿj"H‹Õœ¸ž¥&.öc»…
259968  9E 9A CC 45 23 D9 30 DB 98 ✗  2E 86 79 75 53 8B  žšÌE#Ù0Û˜".†yuS‹
259984  8D 61 7D 15 4D F1 06 BD 8E 11 CA F9 43 9B F2 42  .a}.Mñ.½Ž.ÊùC›òB
260000  1C 4B A9 43 A6 32 2C 5A 49 C0 8D 92 24 D0 0E 73  .K©C¦2,ZIÀ.'$Ð.s
260016  07 58 2A 84 71 34 71 2F 42 EF 6F BE E0 8B 5C 5A  .X*„q4q/Bïo¾à‹\Z
260032  D6 6F A5 04 3E 81 5F 23 24 48 61 0C 00 05 02 00  Öo¥.>._#$Ha.....
260048  5C 02 8B 74 D9 82 03 00 33 0C 11 1B 2B 7E 01 EE  \.‹tÙ,..3...+~.î
260064  A1 82 00 00 ✗  EB 00 00 00 00 24 00 00 00 7E 31  ¡,....ë....$...~1
260080  0C 0B 01 02 08 11 5A 6F D0 AC 00 00 BD 89 7B 94  ......ZoÐ¬..½‰{"
260096  8B 0B 3E 7F CF 33 C9 B1 1F 65 F3 37 26 16 9A 66  ‹.>.Ï3É±.eó7&.šf
260112  73 D8 E0 27 7C 98 22 39 61 0C 00 05 ✗  05 DA 02  sØà'|˜"9a.....Ú.
260128  89 74 DA 00 33 0C 11 12 16 30 0D 98 0C 52 80 E0  ‰tÚ.3....0.˜.R€à
260144  A7 3F 8C 2C 58 0D A3 F4 18 23 EE F0 DA C7 22 94  §?Œ,X.£ô.#îðÚÇ""
260160  39 28 FF 1D 7A 99 31 F1 8A F1 02 D3 68 31 45 5C  9(ÿ.z™1ñŠñ.Óh1E\
260176  88 04 35 89 BA 72 4F 71 3A 40 28 E7 B0 B7 A9 9C  ˆ.5‰ºrOq:@(ç°·©œ
260192  23 89 D7 FC 8F F1 6D 44 BB EE C1 2F 2A 8B 32 A6  #‰×ü.ñmD»îÁ/*‹2¦
260208  93 22 61 5D 1C F0 66 27 7F E9 47 4D CB 19 FD 7A  ""a].ðf'.éGMË.ýz
260224  73 E8 05 49 CA A5 ✗  FF 15 48 D9 2C D4 DA D8 68  sè.IÊ¥ÿ.HÙ,ÔÚØh
                                      Start: 0 [0h]   Sel: 255933 [3E7BDh]   Size: 10,010,624
```



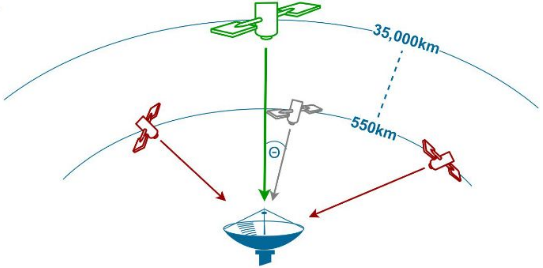
→ We know the steam is corrupted but we don't know which bytes are corrupted and their correct value

Session 2: Link Segment Security (2)

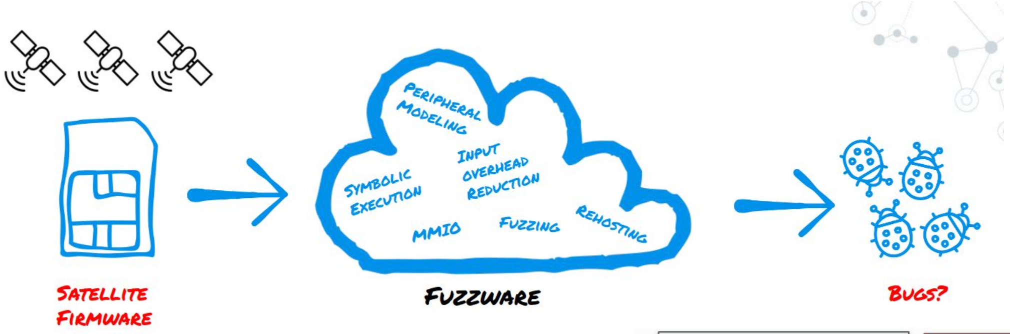


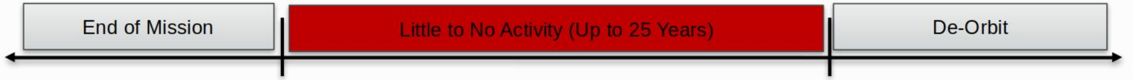
The Attack

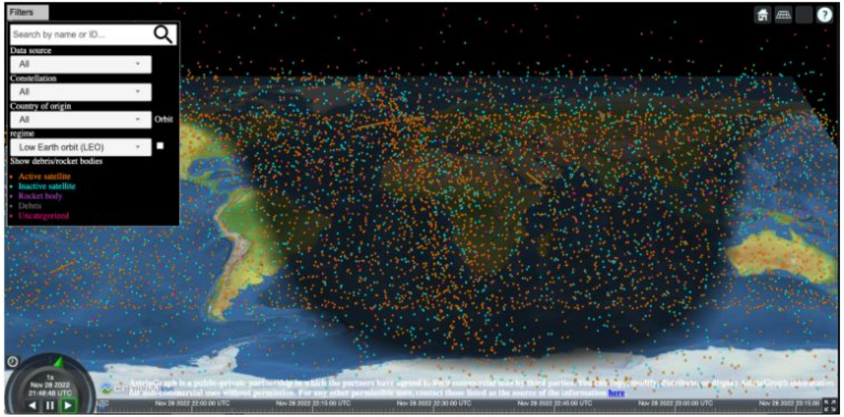
- Override disabling of small-angle satellite broadcasting
- Match known frequency band
- Broadcast noise (additive)
- Accumulate weaker off-angle signals



Session 3: Space Segment Security

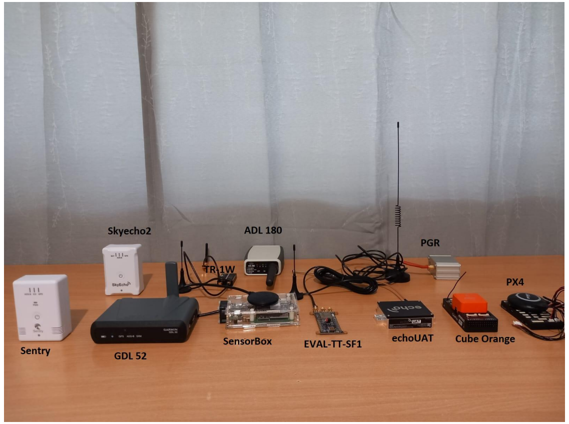


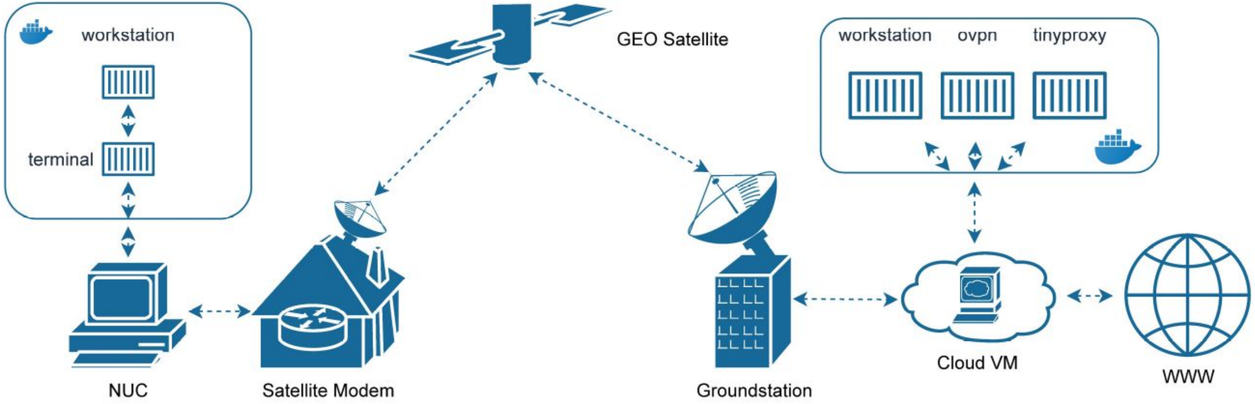




AstriaGraph is a public-private partnership in which the partners have agreed [illegible] commercial use by third parties. You can copy, modify, distribute, or display AstriaGraph information for non-commercial uses without permission. For any other permissible uses, contact those listed as the source of the information here.

Session 4: Test Beds




workstation
terminal
GEO Satellite
workstation
ovpn
tinyproxy
NUC
Satellite Modem
Groundstation
Cloud VM
WWW