Exploring Radio Frequency Attacks in Outer Space

Dr. James Pavur
DOD Chief Digital and AI Office: Directorate for Digital Services*

* Opinions expressed are solely my own and do not express the views or opinions of my employer.
KA-SAT Coverage: European Spot Beams
February 24, 2022 - 5:00 am UTC

Space Cyber’s Escalatory Future...

Civil Infrastructure as Wartime Target
Space Cyber’s Escalatory Future...

Civil Infrastructure as Wartime Target

Collateral / Spillover Damage
Space Cyber’s Escalatory Future...

Civil Infrastructure as Wartime Target

Collateral / Spillover Damage

Cross-Border Disruption
Looking to the Past...

60 Years of Satellite Exploitation

Figure: Pavur & Martinovic, Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight, Journal of Cybersecurity, https://doi.org/10.1093/cybsec/tyac008
Signal Exploitation: >2/3 of Historical Satellite Attacks
1972: The Right to Jam

“One article appeared to give countries the right to jam electronically satellite relay transmissions - which would be relatively easy to do” - NYT; Aug 11, 1972
April 27, 1986: Captain Midnight Incident
Captain Midnight Attack
Early instance of satellite signal hijacking by an individual hacker.

And so it begins...
Captain Midnight Attack
Early instance of satellite signal hijacking by an individual hacker.

2002

Falun Gong Piracy Incidents
Early example of non-state actor engaged in satellite signal piracy.

And so it begins...
Captain Midnight Attack
Early instance of satellite signal hijacking by an individual hacker.

“Bolinha” Piracy Incident
Brazil cracks down on truckers hijacking US military FLTSAT-8 transponders for long-range comms.

Falun Gong Piracy Incidents
Early example of non-state actor engaged in satellite signal piracy.

Banned Falun Gong Movement Jammed Chinese Satellite Signal

And so it begins...
Captain Midnight Attack
Early instance of satellite signal hijacking by an individual hacker.

“Bolinha” Piracy Incident
Brazil cracks down on truckers hijacking US military FLTSAT-8 transponders for long-range comms.

2002
Falun Gong Piracy Incidents
Early example of non-state actor engaged in satellite signal piracy.

Banned Falun Gong Movement Jammed Chinese Satellite Signal

2009

2018
Trident Juncture GPS Interference
Norway and Finland accuse Russia of emitting GPS jamming signals from Kola Peninsula during joint military exercises.

And so it begins…
How?

A *Very* Short Introduction to Radio Interference
Jammed!
Hijacked!
What’s Special About Satellites?
Free Space Path Loss

\[ \left( \frac{4 \pi \times \text{distance}}{\text{wavelength}} \right)^2 \]
Free Space Path Loss

\[ \left( \frac{4 \pi \text{distance}^2}{\text{wavelength}} \right) \]
How is this possible?

FSPL -> Weak GPS Signals

$$26.5 - 10 \times \log_{10} \left( \frac{4 \times \pi \times 19000}{0.19} \right)^2 - 30$$

GPS Satellite Power in dBW

19,000 km

Legit GPS Power at Receiver: **-125.48 dBm**
Use That Distance Advantage!

Legit GPS Power at Receiver: \(-125.48\ \text{dBm}\)

Spoofed GPS Power at Receiver: \(-26.41\ \text{dBm}\)

Attacker Distance (km)

\[-20 - 10 \log_{10} \left( \frac{4\pi \cdot 0.01}{0.19} \right)^2 \approx -30\]

HackRF Power in dBW
Example: GPS Interference
Example: GPS Interference
Surely There are Rules?

CubeSat Design Specification (CDS)

AFSPCMAN 91-710 V3
# Safety Controls

<table>
<thead>
<tr>
<th>Safety Control</th>
<th>Primary Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment switches prevent power-on in deployer</td>
<td>CDS 3.3</td>
</tr>
<tr>
<td>Software timers prevent RF transmission for 45 minutes</td>
<td>CDS 3.4</td>
</tr>
<tr>
<td>Battery power limitation</td>
<td>CDS 3.1</td>
</tr>
<tr>
<td>Software Safety Guidance</td>
<td>AFSPCMAN A2.2.4.14</td>
</tr>
<tr>
<td>RF Emission Compatibility</td>
<td>AFSPCMAN A2.2.4.10.2, Launch Vehicle User’s Guide</td>
</tr>
<tr>
<td>Safety Control</td>
<td>Primary Reference</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Deployment switches prevent power-on in deployer</td>
<td>CDS 3.3</td>
</tr>
<tr>
<td>Software timers prevent RF transmission for 45 minutes</td>
<td>CDS 3.4</td>
</tr>
<tr>
<td>Battery power limitation</td>
<td>CDS 3.1</td>
</tr>
<tr>
<td>Software Safety Guidance</td>
<td>AFSPCMAN A2.2.4.14</td>
</tr>
<tr>
<td>RF Emission Compatibility</td>
<td>AFSPCMAN A2.2.4.10.2, Launch Vehicle User’s Guide</td>
</tr>
</tbody>
</table>
## Let’s Break Some Rules...

<table>
<thead>
<tr>
<th>Safety Control</th>
<th>Primary Reference</th>
<th>Responsible for Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment switches prevent power-on in deployer</td>
<td>CDS 3.3</td>
<td>CubeSat Developer (DITL, Electrical Diagrams)</td>
</tr>
<tr>
<td>Software timers prevent RF transmission for 45 minutes</td>
<td>CDS 3.4</td>
<td>CubeSat Developer (DITL)</td>
</tr>
<tr>
<td>Battery power limitation</td>
<td>CDS 3.1</td>
<td>CubeSat Developer (Battery Report, MSPSP)</td>
</tr>
<tr>
<td>Software Safety Guidance</td>
<td>AFSPCMAN A2.2.4.14</td>
<td>CubeSat Developer (MSPSP)</td>
</tr>
<tr>
<td>RF Emission Compatibility</td>
<td>AFSPCMAN A2.2.4.10.2, Launch Vehicle User’s Guide</td>
<td>CubeSat Developer (MSPSP) Range Safety (EMF testing)</td>
</tr>
</tbody>
</table>
### Attack Simulation

1. Integrate Malicious CubeSat On To Target Mission

<table>
<thead>
<tr>
<th>BadSat Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size &amp; Weight</td>
</tr>
<tr>
<td>Relevant RF Range</td>
</tr>
<tr>
<td>Attacker RF Tx Power</td>
</tr>
<tr>
<td>3U, 4kg</td>
</tr>
<tr>
<td>1.1–1.6 GHz (SDR)</td>
</tr>
<tr>
<td>1 – 10 W</td>
</tr>
</tbody>
</table>
Attack Simulation

2. Power On CubeSat Radio Immediately After Deployment from LV (Violates CDS 3.4)
Attack Simulation

3 Transmit Interference at 1575.42 MHz to Jam GPS Reception (Violates AFSPCMAN A2.2.4.10.2)
Attack Simulation

Profit???

Separation Model

CubeSat Separation over Time

Image: CCSWE, *The CSSWE CubeSat and PPOD just prior to integration*. Wikimedia Commons. CC-BY-SA-3.0
Separation Model

CubeSat Separation over Time

Image: CCSWE, The CSSWE CubeSat and PPOD just prior to integration. Wikimedia Commons. CC-BY-SA-3.0
Reception Quality Model

SINR at LV Receiver During Attack

![Graph showing SINR at LV Receiver during attack, with different lines representing various attack EIRP values.](Image)
Reception Quality Model

SINR at LV Receiver During Attack

Receiver SINR (dB)

Elapsed Time from Deployment (Minutes)

Attacker EIRP
- 1W
- 4W
- 7W
- 10W
Example: Signal Hijacking
How *most* Broadcast Satellites Work
How *most* Broadcast Satellites Work
How *(most)* Broadcast Satellites Work
How (most) Broadcast Satellites Work
Signal Piracy Attack

Satellite

Customers

Ground Station
Signal Piracy Attack

Customers → Satellite → Ground Station
What’s Next?
What’s Next?

Sophisticated RFI Attacks
What’s Next?

Sophisticated RFI Attacks

RFI Defenses & Mitigations
What’s Next?

Sophisticated RFI Attacks
RFI Defenses & Mitigations
Detection & Monitoring
What’s Next?

Sophisticated RFI Attacks
RFI Defenses & Mitigations
Detection & Monitoring
Policy & Norms
Key Takeaways

Space is Physical
Key Takeaways

- Space is Physical
- Space Cyber ≠ New
Key Takeaways

- Space is Physical
- Space Cyber != New
- Space Needs YOU
Questions/Ideas?
Email: james@pavursec.com (personal)
      james.pavur@dds.mil (work)
Twitter: @jamespavur

Resources & Further Reading
https://github.com/deptofdefense/dds-at-DEFCON

Jobs
https://www.dds.mil/join

Other DEFCON Stuff to Check Out
Kosher & Green - HACK THE HEMISPHERE
Wouters - Glitched on Earth
Aerospace Village
ICS Village