Outline

Intro Paragraph – Line up the main points

Main Point -> Space is insecure though the attack vectors are limited this will soon change with the rise of private satellites which will cause a much more dangerous space.

Evidence:

Tesla Starlink Planet and Hawkeye 360 are private companies who are creating satellite constellations and have been attacked.

Iridium Satellites can already be hacked and methodologies for finding vulnerabilities have been an active topic. Hack-A-Sat

NIST Acknowledges the inevitability of Cyber Space dangers – Risk Management Framework for Space, Dangers of TDRS etc.

Paragraph 1 – Current issues with Satellites

Breaking into a satellite can be done as there are cyber threats in each aspect of satellite communication and operation such as ground communication, satellite communication, and satellite software/hardware.

Find Source:

There are no cybersecurity standards for Satellites. <https://www.satellitetoday.com/cybersecurity/2019/11/14/satellite-providers-stymied-by-lack-of-cyber-standards/>

Ground Communications are susceptible to attacks

Satelite to satellite communication is susceptible to attacks

Satelites themselves are vulnerable though one would need to break through the other two to take over a satellite.

<https://link.springer.com/article/10.1007/s10207-020-00503-w#Sec8>

Paragraph 2 – Commercial evidence past to Now

Networks can be very insecure and the solution is not to move the network into space.

As of April 2021 there are 7,389 satellites in space which is an increase of 27.97% compared to the year prior. There have been a total of 11,139 satellites that have been launched but only 7,389 remain in space. <https://www.geospatialworld.net/blogs/how-many-satellites-are-orbiting-the-earth-in-2021/>

The changes of losing a satellite to a cyber attack can be very high considering the number of commercial vehicles. Government space crafts have been hacked in the past like the US German ROSAT X-Ray satellite - where hackers were able to control the direction of the satellite’s solar panels and effectively destroy its only power source. <https://gcn.com/cybersecurity/2020/02/hackers-could-shut-down-satellites-or-turn-them-into-weapons/291164/>

Paragraph 3 – Future of Satellites

A Cyber Physical Power System (CPPS) is a system that combines and coordinates the internet and physical power system elements. These systems are distributed networks executing in unpredictable environments and built from control systems and embedded systems to monitor and regulate the physical power system in real time. CPPSs are designed as a structure of interacting elements with physical input and output. <https://ieeexplore.ieee.org/document/9167203/authors#authors>

These are systems that have cyber integrated into the hardware to monitor the network as part of the ongoing push to secure space. This is not a working solution, though it can mitigate the vulnerabilities of a satellite it can still prove to be vulnerable.

Fortunately, due to the low orbit (550 km altitude) and fast transmission speed in vacuum, the propagation delay difference between the SpaceX’s Phase I Starlink constellation and the terrestrial optical fiber network is small, and the delay of space propagation could be even smaller when the hop distance is longer than 2500 km [3]. Therefore, the Starlink network could be exploited in the CPPS for wide area measurement, protection and control (WAMPAC) applications in the areas with weak network connections.

Starlink Space Network-Enhanced Cyber–Physical Power System

Tong Duan , *Graduate Student Member, IEEE*, and Venkata Dinavahi , *Fellow, IEEE*

Though there is innovations in the building of secure commercial space vehicles, the rate at which security is maturing is very slow. Due to the slow rate of improvement, vulnerabilities which can circumnavigate the

NIST framework history and the acknowledgement that NIST is about mitigation not prevention or immunity

Conclusion