**Satellite Network Hacking and Security Analysis**

Satellites may be secure while they orbit around the Earth, but with recent use of cheaper high-powered antennas makes them prone to threats. It is only recently that satellite cyber security is being viewed as a serious concern, which may not be as difficult as generally perceived.

Many of the satellites in Low Earth Orbit were never looked at from a security perspective, as their designers never thought anyone would make an attempt from the ground to intercept satellite signals. Many of these satellites have no data encryption due to little memory and low processing power. For instance, Voyager 1 would need six days to crunch bits for setting up an SSL link. It not only has only 0.25 MB of storage, but also receives a signal after 20 hours. With low power satellite devices such as CubeSats becoming more common, Engineers are now more concerned than ever.

At an RSA conference last year, Bill Malik, VP of Infrastructure Strategies at Trend Micro, mentioned many attacks in the past on NASA systems, with some focusing on satellites. From TDRS to Sputnik, all satellites in NASA;s orbital network have had similar security vulnerabilities as devices on Earth. With unencrypted transmission, it was very easy and possible to listen to whatever communication was going on. Malik also talked about Hubble, which had its own vulnerabilities. The space telescope optics are covered by a hatch to save it from the sun, whereas the solar panels can be tuned according to the power received. Both the optics and solar panels could be exploited by pointing the Hubble in the sun’s direction to burn the optics, or to position the solar panels such that the power received would damage their batteries.

If hackers get control over these satellites, there can be dire consequences. They could simply shut down the satellites to deny their services or jam the satellite signals, thus creating a chaos for critical infrastructures such as transport systems, electricity grids or water networks. Some satellites consist of thrusters that enable them to change their direction in space, slow down or speed up. If hackers take controls of their network, they can create havoc by changing their orbits or crashing them into other satellites or the International Space Station.

**How Can we Ensure Satellite Security?**

Some immediate measures can address the current threats. For instance, jamming can be prevented if satellite operators hop their communications recurrently between frequencies and make it hard for a hacker to jam the communication. They can also be protected from natural disasters by hardening them against electromagnetic interference.

Ground systems that rely on satellite communications, for instance [Earthlink Internet](http://www.planetdish.com) and GPS, should increase the use of GPS authentication. This will help to measure the signal with confidence that its actually coming from a real satellite.

Furthermore, though new satellites use encrypted communication, we need seamless monitoring of transmission traffic and activity detection on the satellite. Some analysts are also of the belief that government should be actively involved in developing and regulating security standards for satellites. It needs to adopt and formulate a comprehensive framework for the commercial space assets such as, for instance, passing a legislation requiring all satellite manufacturers to formulate a mutual cybersecurity architecture.

It should also be made mandatory to report satellite cyber breaches and notify about critical space assets to prioritize cybersecurity of those assets. There should also be clear instructions on authorities responsible in case of a cyberattack on a satellite. This will ensure that those authorities take all possible steps for the security of satellites for which they are accountable.

**Conclusion**

Considering the conventional slow-pace of action at federal level, a better strategy to ensure the application of security standards would be the involvement of multiple stakeholders including public and private entities. It is imperative that together, government and industry take action now. Else it may be a mistake to leave it a at the disposal of hackers to hack a commercial satellite and misuse it for their criminal agenda, whether in space, or here on Earth.