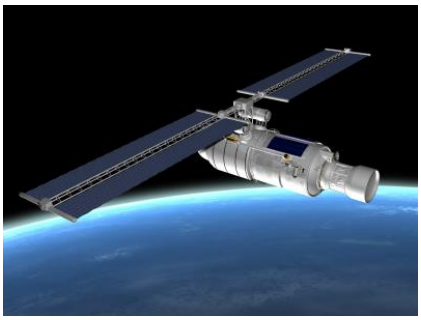
www.pipelinepub.com
Volume 17, Issue 9

Safeguarding Satellites for a Generation

By: Thorsten Stremlau



According to the Union of Concerned Scientists, there were over 3,300 operational satellites orbiting the earth at the start of 2021, with hundreds of others planned for launch. From supporting worldwide Internet of Things (IoT) deployments and geolocation capabilities to assisting with military intelligence, satellites are becoming an integral part of everyday life. This proliferation of satellites is only set to increase, with many firms planning to send whole fleets into the skies to meet the rising global demand for digitalization and connectivity.

As the popularity of satellite skyrockets, however, the concern around security is also heightening. Many of the world's global communication networks are now reliant on satellites and have become increasingly integrated with the Internet and many other networks. With this connectivity comes a growing attack surface, and cyber criminals are starting to take notice. As a result, it is imperative that security is made a priority right from the outset. With access to crucial networks and highly sensitive information, it is essential that vendors and manufacturers take the right steps to safeguard both satellites and ground infrastructure.

The growing need for satellites

Satellites have become extremely important. Not only do they support telecommunication networks, but they have also become vital for running global supply chains, worldwide logistics, and personal navigation. Private and government organizations now also depend heavily on them for important operations, such as remote sensing, imaging, mission-critical communications, and

weather monitoring. Similarly, electric grids, IoT devices, data centers, and GPS technologies all rely on satellites to work effectively.

It is particularly alarming to think that many of these organizations have no influence over the cybersecurity of the satellite system and lack a basic understanding of the risks facing them. As more satellites are deployed, they will become increasingly interconnected, which therefore opens the door to the vulnerabilities through which attacks can easily occur. Despite the reality that cyberattacks frequently have significant consequences, security is often an afterthought, as innovation takes priority. This leaves little room or time to think about implementing best practices that can protect against attacks.

As evidenced by the recent attack on SolarWinds, which saw sensitive information from federal governments, educational institutions, and other private companies compromised by hackers, breaches can have a detrimental impact. A recent Cybersecurity Ventures report noted that cybercrime is expected to cost the world $10.5 trillion every year by 2025. With so much depending on satellites, cyberattacks that target them can cause substantial damage, from financial losses to fines for failing to comply with data protection legislation. Any intentional or unintentional disruption is also highly likely to cause a ripple effect with severe economic impact or information leakage. With so much at stake, companies must get security right the first time.

Security threats

There are a variety of ways in which satellites and their systems can be attacked. One method that is used by hackers is accessing the downstream system by intercepting the signal of the satellite. Once this is complete, it is then relatively simple for them to invade the entire network, and the networks of any organizations using that system, by infiltrating one ground station. Another way is through the long-held practice of using long-range telemetry to communicate with any ground stations. Any downlink or uplink communication is managed via open network security protocols, which can be easily bypassed by cyber criminals. There are also many entry points offered by IoT devices, which can open a back door into the entire network. One single unprotected device can bring down an entire company—and potentially its customers and suppliers too.

This is worrisome for organizations of all sizes, especially those that need to protect highly sensitive data, such as militaries and governments. Satellite cybersecurity is hindered by a multitude of weaknesses, according to Major Stephen Bilcher of the US Air Force. During the manufacturing stage, several weaknesses have developed through years of neglect, leaving potential weak spots in satellite receivers, networks, and ground systems that cyber criminals can readily exploit. Each craft or system often requires a specific, custom solution, which is costly and time-consuming to implement. Additionally, the ground systems that support satellites are routinely saturated with Industrial Control Systems (ICS) and IoT devices, which are common targets for attacks. Hackers are always looking for security loopholes to gain access to the entire satellite system, and these ICS and IoT systems provide the best way in due to their many vulnerabilities.

Ensuring the best protection

As we become increasingly reliant on satellites, it is important that the satellite industry urgently reassesses cybersecurity and makes it a priority. The first step is for organizations to determine the vulnerabilities facing them and understand exactly how they could be exploited—for example, ensuring that their equipment can be updated and upgraded with the latest security measures. Because of its low security level and weak encryption, old IT equipment has often been used in the past to take control of entire satellite networks.

The next step is to implement industry-wide guidance and technologies that are designed to address not only the many security shortcomings present today, but also those that may crop up during the satellite's long service life. The Trusted Computing Group (TCG) has developed a series of specifications, standards, and technologies that are guaranteed to protect the entire satellite ecosystem throughout its long lifecycle. From verifying the authenticity and trustworthiness of a device to the implementation of network security, trusted computing provides a set of essential building blocks, which manufacturers and IT specialists must adopt for the complete protection of satellites and their ground-based infrastructure.

Network security, as defined by TCG, enables all communications to be authenticated before being sent up to the satellite. This enables ground-based infrastructure to become effective firewalls, capable of preventing the attacks that can prove deadly to satellite operations. Despite high volumes of traffic, the satellite will ignore any communication that remains unauthenticated. This prevents satellites from being taken control of by ingenuine traffic and ensures satellite networks meet compliance requirements, have access control, and offer orchestration. With encryption at a network level, all data is also protected while traveling around the satellite system.

Industry-wide protection

Practical solutions rely on a root of trust, which is a concept and component that has been developed by TCG. A root of trust provides a foundation for the device and can be used to keep the system secure for a wide range of applications. A root of trust allows for the device's authenticity and status to be comprehensively validated at any stage throughout the device's lifecycle. This measure is a key aspect needed for satellite security, as it is responsible for the protection, generation, and storage of a cryptographic device identity, which is essential for the authentication and validation process.

With the implementation of proper definitions, architectures and guidance, satellites can be protected throughout their entire lifetime. For example, the new Cyber Resilient Module and Building Block Requirements specification from TCG allows satellites, and any devices in the system, to protect themselves and be recovered following an attack. As the number of satellites in orbit rises, it will become extremely difficult to manually intervene when one has been compromised. Instead, satellites must have the ability to self-protect and respond to attacks

independently. With in-built resiliency using the steps outlined in the specification, the sector has another valuable tool with which to fight against any security risks.

As part of this, the Cyber Resilient Technologies Work Group (CyRes) at TCG has designed the concept of a Cyber Resilient Module. This can be implemented in many forms, either as part of a chip within the main hardware of the device, or as part of a subcomponent installed within a larger, more complex system. The module can recover successive layers of software and individual components within the device, through the servicing of code and the configuration of multiple layers sequentially. As a result, there are several options that can be used to assist with the recovery of a satellite and its infrastructure remotely. Not only does this reduce time and cost, it also provides a new level of assurance that will prove crucial for the satellite industry. It is currently impossible for manual intervention to be made to satellite craft once launched into the sky, but thanks to advancements in technology, this is no longer a limitation.

Satellite security must be a priority

Satellite cybersecurity is now an imperative, with the world dependent on thousands of satellites acting as the central system for governments, militaries, and businesses worldwide.

Satellites support thousands of networks globally and carry huge amounts of sensitive, personal data. As demand for more connectivity and bandwidth grows, we can expect to see the number of satellites deployed increase, too. This opens the door for more vulnerabilities to crop up and creates potential opportunities for hackers. In response, the satellite industry must step up its cybersecurity responsibilities and protect the multitude of systems and sensitive information now dependent on systems in the sky.

To do this effectively, organizations of all shapes and sizes must implement the security solutions, specifications, and technologies that offer the best way of securing, protecting, and recovering all devices within the satellite ecosystem. This will give businesses, governments, and militaries a great defense against hackers and help them to avoid the heavy financial losses or fines that are common due to data leakage and cyberattacks.