CYPHRE
a RigNet company

CYBERSECURITY IN SPACE: ENCRYPTING SATELLITE COMMUNICATIONS

Global satellite communications networks are a mission-critical part of infrastructure sectors, including broadcast networks, emergency services, national defense, navigation systems, maritime communications, and more. Cyber threats are evolving against satellites and the services they support, as cybercriminals, hacktivists, as well as state and non-state actors look to commit espionage, terrorism, or cyberwarfare disruptions – either for profit or to create chaos.

Attacks on satellite infrastructure can affect everything from GPS navigation, shipping command and control systems, defense signaling, and even the targeting of weapons systems. Corrupting satellite communications can have a cascading effect that impacts public safety, commerce, and national security. Attackers may focus on anything from manipulating IoT sensors to infusing ransomware into network operators, software solution providers, integrators, and hardware manufacturers.

The Satellite Industry's High Cyber IQ

In response to this growing threat, the satellite industry has already woven cybersecurity into its fabric, embracing best practices around encryption, subscriber management, access control, and overall system hardness. However, this has mostly been focused around supporting national security activities where they are already encrypting command uplinks and have begun to encrypt telemetry downlinks to safeguard information (e.g. the location of steerable military communications beams, which could signal the location of warfighters).

Since this level of security has, until now, been limited to militaries and governments, enterprises and industrial companies have been left without such hardened encryption technologies to protect their information.

In the face of these serious dangers to the security of information transiting networks and control systems that communicate, these corporations need a solution that can protect data from ships and offshore assets, as well as control access to subcontractors, technicians, and suppliers.

The rapid development of maritime broadband satellite coverage and sophisticated, computer-controlled systems has also heightened risks to vessels, which are no longer protected by an air-gap from external systems. Today, 30,000 vessels have constant internet access, a massive exploit vector for nearly all cyberattacks.

Advanced Encryption Is Vital to Guarding Satellite Infrastructure from Cyberattacks

Adopting cybersecurity solutions that does not begin and end with the satellite or the terrestrial teleport station is required in order to protect satelllites performing mission-critial communications. Cyphre Security Solutions offers hardware-driven, encryption-based data security services that protect data in-transit across virtually any network and when at-rest in data centers or the cloud.

Cyphre's comprehensive solution is built on a robust data encryption foundation. While standard encryption can provide basic protections, the way Cyphre encryption is achieved matters vitally. Cyphre's uniquely powerful hardware-based encryption adds a crucial layer of protection, providing deeper and stronger data security than conventional methods can. In Cyphre's solutions, encryption keys are stored in a hardware layer and are never exposed. Even if an attacker gains root access into the server, the keys are protected and remain isolated from the attacker.

Securing the Global Supply Chain

Ship operators, Maersk, BW Group, and BP Shipping have all been hacked in recent years. They readily admit that they are constantly under pressure from cyberattacks. When malware is introduced into a computer or ship system connected to the network, a common action of the malware is to establish a covert command communication that results in system encryption, exfiltration of data, and a number of other serious exploits.

On-board systems and devices, such as pumps, generators, valves, connected sensors, and many more, generate significant amounts of data that is often stored on the local network and then transmitted over satellite to a teleport or via cellular to the service provider network. Standard data encryption employed by these networks may be sufficient for consumer traffic but is inadequate protection against modern hacking techniques used by sophisticated for-profit hackers and nation-states looking to gain a competitive edge.

CyphreLink provides hardware-encrypted connections for data transmitted from on-board systems over satellite communications networks. CyphreLink is virtually unbreakable by man-in-the-middle attacks, making it an extremely resilient service that's simple to deploy and highly-extensible across an entire network. CyphreLink's hardened security solution protects data, certificates, keys, and connections from eavesdropping, surveillance, overt and covert interception, and man-in-the-middle attacks.

When data reaches corporate data centers or a cloud service, the Cyphre Encryption Gateway offers powerful encryption and key protection that is virtually unbreachable at the key generation and management level. Purpose-built for enterprise users who access, transmit, store, and retrieve data from cloud services and applications, the Cyphre Encryption Gateway serves as an integration point for consistent deployment of security policies for 'data in transit' and 'data at rest.'

Cyphre's BlackTIE® Technology Is the Key

Cyphre's BlackTIE® technology assigns chip-resident encryption keys (Black Keys) per file, rather than one key for many files. This establishes maximum protection for data at rest, limits the 'blast radius' of any breach, and protects traffic as it leaves the network. Cyphre's automatic protection of information in transit requires no proactive action by the teams moving the data. This establishes a "zero knowledge" stance for employees, eliminating them as a possible point of exposure.

Cyphre's uniquely powerful security solutions provide 360-degree data protection that is invisible to end users, highly scalable, device-resident, and cost effective for medium and large-scale environments.

About Cyphre

Headquartered in Austin, Texas, Cyphre cloud encryption technology provides the highest level of security for cloud data. Period. Product offerings include Encrypted Cloud Storage and Enterprise Collaboration services, Secure IoT Integration and the Enterprise Cloud Encryption Gateway.

www.cyphre.com   @getcyphre   Cyphre   /getcyphre