30th Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America
Presented on May 21, 2014

MEETING GLOBAL DEMAND FOR ASSURED MOBILE SATELLITE SERVICES

Rodrigo J. Gomez
TrustComm, Inc., Rodrigo.Gomez@TrustComm.com

ABSTRACT

In today's environment of constrained budgets, the demand for COMSATCOM remains high. The DoD has an ever-expanding need for both fixed and mobile SATCOM services, to operate on the strictest operational security requirements. Therefore, the industry must maintain the highest standards of security for its SATCOM deployments – regardless of the hardware solutions chosen by end users.

Among U.S. government agencies and commercial organizations with global missions, there is increasing demand for resilient, assured communications infrastructures that have a demarcation point in the United States. To address concerns of possible interception or interruption of sensitive voice and data traffic, and sensitive operational information, many organizations are insisting upon COMSATCOM networks that meet more robust Operational Security (OPSEC) and Information Assurance (IA) requirements.

This document discusses how the satellite industry is progressively improving its understanding of these security requirements, beyond the pure IA domain, and is addressing these concerns. The document provides examples of how commercial providers leverage secure infrastructure for the development of high-grade, assured communications solutions. The concept of Secure, Ensure and Assure is explained in the context of mobile satellite services (MSS). The paper outlines the difference and relationship between the three terms and concludes that U.S. Government users are focused on solutions that can provide "Assured" communications.

Building on the U.S. Government's certification and accreditation process, this document outlines the different threats within a typical MSS network infrastructure. The outcome reveals that implementing a 100 percent IA-compliant infrastructure is not sufficient to address all vulnerabilities without the proper OPSEC support. The outcome outlines what the industry is doing to identify and mitigate these vulnerabilities.

GLOBAL DEMAND AND THE CHANGING LANDSCAPE

In the late 1990s through 2000, the telecommunications industry predicted the enormous increases in demand for ground-communications bandwidth due to increased use of the Internet. The industry expanded access to bandwidth-intensive services, such as video and games, launching the era of the wideband. Internet protocol data traffic grew exponentially, despite the dot-com bubble burst in the mid-2000s. After consolidation in the industry, demand forecasts became more realistic, driven by the development of new applications and technologies in the consumer market -- such as smart phones and high-definition video streaming.

Similarly, in a very short period starting in the late 1990s, the satellite industry has grown exponentially. Based on a report from the Satellite Industry Association, during the last decade the satellite industry grew threefold, from $64.4B in 2001 to $189.5B in 2012[*].

The market for fixed satellite services (FSS) evolved from being used in very specialized applications -- mainly video and Internet distribution, point-of-sale and voice backhaul -- to enterprise applications (commercial and military) with large amounts of remotes sharing broadband networks. Commercial and military satellites followed a similar trend.

The MSS market has not been indifferent to this trend. Companies such as Inmarsat and Iridium have been strong in the market for decades, offering basic voice and bandwidth data services to highly mobile users. Other regional operators have been providing more specialized services to focused markets. All of these operators have combined to build an MSS market that boasted revenues of approximately $1.4B in 2012.

The MSS segment has populated the marketplace with specialized terminals and handsets, and dominates very specific segments of the overall global market. Recently, global missions, the push for mobility with bigger pipes and more capabilities have forced the MSS segment to adapt and evolve. The introduction of next-generation satellites provides more power to the user terminal and allows operators better on-board capabilities. This allows reuse of spectrum while using more aggressive modulation schemes for higher data rates. Machine-to-Machine (M2M) and tracking applications are leading the growth in volume of narrowband communications.

Traditionally, fixed satellites were used for high-bandwidth applications and MSS satellites were de-facto for mobility for thousands of users requiring little or no access to broadband. However, technological enhancements and changing user requirements have blurred the traditional gap between mobile and fixed satellite markets. Every day, more fixed users are looking for deeper penetration in networks with higher density of remotes. Likewise, mobile users require access to more bandwidth, with smaller and more portable devices.

While all of the above are specific trends in the commercial industry as they relate to the user requirements, government-funded satellite systems are following the same trends. The projections for the U.S. Government and military satellite market forecast a growth of about 100 percent for the next seven years. This projection includes an increase from a half million in-service units in 2011 to more than one million by the end of 2021[†]. By nature, commercial and government missions are different, and this document will not focus on commercial systems supporting commercial users. However, additional non-tangible differences are observed between services provided by commercial satellite systems compared to government assets supporting defense or intelligence missions. The U.S. Government's preferred option is to use government assets. However, depending on their mission priority, area of operation, capacity and capabilities requirements, and availability of ground resources, government users are sometimes restricted or denied access, or find their resources in areas of operation limited. These situations force governments to fulfill these requirements beyond government assets, using commercial systems.

This document focuses on commercial systems supporting government users. Although commercial enterprises are also concerned about security of their information and its users, the assessment of the posture in a

[*] Online Source: SIA; *State of the Satellite Industry Report*; June 2013; http://www.sia.org/wp-content/uploads/2013/06/2013_SSIR_Final.pdf.

[†] Source: NSR; *Government and Military Satellite Communications, 9th Edition*.

government network toward security in satellite systems is often a subjective matter. This is because users are often forced to reduce the classification or waive security requirements in order to allow access to systems, simply because there are no alternatives.

As with any information system, vulnerabilities, risks and controls change from system to system. In the context of this document, an MSS user is referred to a single person or a very compact (small) group, transporting hand-carried (briefcase-style) or smaller equipment kits (handsets or terminals) and using them in short- to mid-term deployments for data and/or voice communication derived from either L, Ku, Ka or X-Band commercial satellites. This paper focuses on some of the initiatives that the MSS industry segment is undertaking to provide assured communications that mitigate IA and OPSEC threats when operating over commercial satellite assets.

SECURE, ENSURE AND ASSURE

Security terms are often misinterpreted, creating vulnerabilities especially at the operational level. The paradigm described below forces users to take security measures that in some cases mitigate these vulnerabilities, but in other cases simply mask the real issues. The challenge for OPSEC strategists is to find the right balance and mitigating measures between Securing, Ensuring and Assuring the information. It is important to clarify that the approach depends 100 percent on the context of the mission.

Securing is directly related to protecting the information from direct attacks. Controls are implemented to create boundaries around the sensitive information. Its ultimate goal is to protect the confidentiality, integrity and accessibility of the information system. The role of the certifier is to understand the context of the mission and, based on that, define the appropriate posture that will address all necessary IA controls. However, none of the controls can be implemented or enforced on shared platforms such as traditional MSS networks. This is because either an enclave can't be shared with other users or foreigners perform the administration. This factor creates the need to assume that the entire network is "untrusted", pushing the boundary outside to the edge instead of closer to the satellite link. The data user will need to encrypt end-to-end data streams (thus reducing the bandwidth available to users), and voice users are expected to ride an unsecure network that is full of mousetraps and sources of information ready for collection and analysis.

Therefore, a certifier needs to rely on a second factor, ***Ensuring*** that the users are capable of executing their missions securely. Certifiers need to warrant that their understanding of the vulnerabilities identified in the system is sufficient to certify that the controls in place are sufficient to deal with a variable and dynamic environment, such as a commercial MSS network.

The role of trust in ensuring security is important from the user perspective, assuming that none of the vulnerabilities have morphed into something not mitigated since Certification and Accreditation (C&A) (C&A is discussed in more detail later). It also relates to trust in the other direction, from certifiers assuming that users will use the system and guidelines specified. This is achieved with proper training programs and regular audits and vulnerability assessments. That is the main reason why it is necessary to renew C&A annually. However, an inherent threat that rarely is addressed properly is adjusting C&A to changes in the environment. C&A is achieved by the certifier taking a snapshot in time on the landscape of the MSS network, then implementing the proper controls. However, the nature of the business prompts services providers to make changes frequently. It is very difficult for certifiers to anticipate changes that will impact the risk profile and adjust the C&A in a timely manner.

Finally, ***Assuring*** this is only achieved through the combination of ***Securing*** and ***Ensuring*** capability. ***Assuring*** is the key term that wraps up the concept of creating an OPSEC "bubble" around an MSS network. A proper definition for assure, in this context, is making certain that something actually happens. In other words, making sure that the objectives for an effective IA implementation incorporate a proper OPSEC strategy. As this is a relationship between the government and a commercial contractor providing MSS services, the relationship needs to have a holistic framework for a proper OPSEC environment.

CLOSING THE GAP IN SECURITY

Historically, U.S. Government systems have been isolated in two distinct user groups, the Department of Defense (DoD) and the Department of Homeland Security (DHS) -- following different standards, approach and procedures. To establish infrastructure in support of mission-critical information systems in the DoD, users must seek and complete DoD Information Assurance Certification and Accreditation Process (DIACAP) approval before operating the system. DIACAP was introduced in 2006 by the National Security Agency (NSA) in an attempt to implement risk management for information systems. A similar process called Risk Management Framework (RMF), based on the National Institute of Standards and Technology (NIST) is followed when users are seeking approval to operate sensitive DHS information systems.

Authority to Operate (ATO) is the result of a successful DIACAP or RMF approval, granted by the Designated Approval Authority (DAA), the DoD- or DHS-designated IA official. The objective of the C&A process is to identify risks, implement mitigation strategies, and create and manage IA capabilities and services in the information system. IA controls are system and managerial requirements to meet the confidentiality, integrity and availability standards set forth by the information owner to meet the mission-assurance objectives. Combining the appropriate lists of Mission Assurance Category (MAC) and Confidentiality Levels forms the specific set of baseline IA controls. DoD users will follow the set of controls and guidelines specified in DoD Instruction 8500.2, while DHS users must follow DHS Directive 4300A.

As a general rule, a certifier (C&A) is a different entity from an auditor. The certifier is the individual (or team) that defines the IA posture and confirms that the information system meets the stated requirements. The auditor is more practical and will verify that the design and implementation plan introduced by the certifier meets the requirements. Five phases are clearly identified in the guidelines for DIACAP: 1- Concept; 2- Acquisitions and Development; 3- Testing; 4- Operations and Maintenance; and 5- Disposal. Similarly, DHS' RMF follows six phases for a complete development of the life-cycle management of the system: 1- Categorize; 2- Select; 3- Implement; 4- Assess; 5- Authorize; and 6- Monitor. While the C&A is a one-time procedure until ATO is achieved, DIACAP and RMF require recertification annually to verify that 1- changes have not been implemented from the original baseline, and 2- changes to baseline (if any) do not affect the IA posture of the information system. This approach is the methodology implemented to bridge the gap between development and implementation, and lifecycle management (maintenance and obsolescence).

Understanding that DoD and DHS systems have similar weight in the approach to control the national security interests, DoD is migrating to DoD Information Assurance Risk Management Framework (DIARMF) in a collaborative effort with the NIST. DIARMF is an effort to create a more consistent approach toward the process to obtain ATO that meet NIST framework objectives tailored to the DoD mission. By merging the security controls from the traditional DoD mission with the RMF process recommended by NIST, new nomenclature has been developed. The former C&A process is now Assessment and Authorization (A&A), and integrates the same six steps of the traditional RMF, in the context of DoD information systems. Although waivers for recertification are being granted under DIACAP, DIARMF is the new standard for new systems, and pressure is on to force some old systems certified under DIACAP become DIARMF certified.

Security in the Space Systems

Countries with highest activity in defense (United States, Russia, China, European Union, Israel, Japan and India) have very high dependency on satellites for communications, weather reporting, navigation and intelligence gathering. Despite several checks and balances currently implemented in the United States, regulation to ensure that access to special satellite technology is limited to those and other countries in an attempt to protect national security interests. Some threats considered unintentional, such as space debris, must be monitored to protect orbiting assets. Other threats, considered intentional, make satellite systems a primary target for adversaries carrying out attacks on military operations.

Space systems generally comprise three elements: a space sub-system consisting of satellites; a ground or terrestrial sub-system that includes supporting ground facilities; and the air-interface that connects the two previous elements. There is a general consensus by users and industry about native vulnerabilities in services operating over satellite. Users have a general acceptance of the fact that the air interface in the satellite services operate as any commercial wireless link, and is a prime candidate for collection of data and denial of service. However, all elements should be protected to minimize threats on mission success. This document focuses on threats related to satellite commercial fleet and commercial infrastructure supporting commercial and government missions.

In-Orbit Security

In-orbit threats are commonly caused by debris, either outer-space particles or mission-related fragments generated after collisions or explosions. A recent study from the Congressional Research Service[‡] reveals that the Space Surveillance Network, a system of telescopes, radars and sensors that operates under the supervision of USSTRATCOM, has in its tracking inventory more than 23,000 objects 10 cm in diameter or larger orbiting the earth. To be considered threats, the objects must be 10 cm or larger for low-earth-orbit (LEO) satellites, and larger than 1 meter for geosynchronous orbit (GEO) satellites. However, only 1,100 objects (about 5 percent) of that inventory are active satellites, the other 95 percent is uncontrolled debris. Commercial and military satellites are constantly tracking debris and anticipating possible collisions.

In-orbit intentional direct attacks are also used by governments to damage in-orbit assets. Low-power lasers deployed in-orbit on small satellites, high-power, ground-based lasers, or high-altitude lasers operating on airborne platforms can be aimed to damage thermal control, electro-optical, structural and power-generation components. Due to distance (related to power) and mission specifications, LEO satellites are most vulnerable to this kind of attack.

Other in-orbit threats are direct attacks to payload, Telemetry Tracking and Control (TT&C) links, or the actual hardware. Jamming is the most common form of attack aimed to interrupt the link on the uplink, downlink, or both, targeting both military and commercial satellites. Uplink and downlink jamming happens when very high-power RF signals are transmitted directly to the satellite to create interference on specific transponders. Downlink

[‡] "Threats to U.S. National Security Interests in Space: Orbital Debris Mitigation and Removal", *Congressional Research Service*, http://www.fas.org/sgp/crs/natsec/R43353.pdf

jamming is also common. It is achieved by creating an RF "bubble" around an emitter that creates ground interference affecting specific users that operate within the emission radius range.

In-orbit attacks can also be aimed to affect TT&C. Adversaries can attempt implementation of man-in-the-middle attacks to modify or send commands to impact payload. This type of attack is usually implemented in the ground segment and can be prevented by increasing the security on the link. Major satellite operators have been implementing ground controls and type-1 encryption to protect the link. Jamming is another way to impact the TT&C link. Jamming occurs by sending either pulses or a constant interfering signal on the link to interrupt communication between the ground segment and the satellite. Operators have implemented techniques that prevent long-term effects of jamming with frequency-hopping links, together with redundant TT&C ground sites to facilitate triangulation and avoid direct ground attacks.

Security on the Ground

Protecting the infrastructure (ground and space sub-systems) is the first response by many service providers to ensure service availability. Typically, commercial operators stop there, leaving protection of the air interface to the users. Protecting user and control data over the air interface will ensure confidentiality and integrity of the information. The goal is to minimize information that can be snooped if signals are intercepted and collected, and to establish robust protocols to minimize man-in-the-middle attacks.

The role of the industry is to satisfy as much as possible the requirements of the users. The role of the users (including the government) is to define what these requirements are. A constant challenge is that these requirements cannot be implemented using government assets and they are forced to operate in commercial infrastructure. Common reasons for not achieving such requirements are either lack of resources (spectrum availability) or, on a lesser scale, lack of ground segment (landing facilities or terrestrial connectivity, etc.). When implementing services in commercial infrastructure, the majority of cases have to deal with security (resources available for the mission do not meet minimum criteria for the mission.)

The Security Posture of the Users

Unfortunately, IA C&A is not a one-size-fits-all approach. Regardless of how robust, planned, and controlled the network infrastructure is, it is still administered and operated by humans. A basic IA principle is to incorporate a three-layer protection system: Protect, Detect and React. However, these layers are only effective with a proper human, technological and operational infrastructure working together. The security posture is the holistic approach implemented in the organization to operate and maintain an information system. It includes the human factor, the technological infrastructure and the operational support -- for a robust three-layered protection.

A traditional MSS satellite system implemented for commercial use brings complexities that are usually not present in the traditional FSS world. Understanding and recognizing the existing vulnerabilities in the MSS network is definitely the first step to define the proper security posture. Information comes from many sources and, depending on the context, the organization must define the strategy to protect the information.

Operational Security

Operational Security (OPSEC) is the process that implements safeguards in the system to protect critical information and observable actions that might not necessarily be considered sensitive or classified, but that could give adversaries an advantage if that information is pieced together with other information to create a bigger picture. It is estimated that about 90 percent of the information collected and used to perform large-scale attacks is exploited OPSEC vulnerabilities from open sources. This is called OSINT (Open Source Intelligence), referred to intelligence collected from publicly available places (social media, trade shows and events, web sites and newspapers, etc.).

Unfortunately for MSS users, the human factor and OSINT is not the only source of OPSEC-related information that can be exploited. MSS systems operate mainly as a shared infrastructure allocating resources to users. Systems operating overseas share critical systems that also process and store information overseas, which require following local regulation. The paradigm that users face is how to meet their mission requirements when they know that their mission can only be achieved using systems that create vulnerabilities. Perhaps the users don't even know the extent of these vulnerabilities, and the value that information can provide to adversaries. In the following sections this claim will take better context.

Building the Proper OPSEC Environment

The industry clearly understands the need to change and is adjusting to meet new requirements. Service providers understand that threats and vulnerabilities in their systems will affect missions and lives, and have demonstrated their interest in allocating funds to meet contractual OPSEC requirements, and build-up infrastructure that facilitates IA C&A procedures.

The industry also understands now that the impact of exposing critical information is beyond economic or commercial competition. Exposure of critical information can be exploited if it reveals mission or strategy details affecting national-security interests. Personnel writing specific OPSEC requirements must understand the technology, and must be conversant in the organization's OPSEC program and mission. OPSEC practitioners must provide contracting representatives with training to ensure appropriately specific OPSEC requirements are included in contracts.

The overlooking of details is common error that government contract procedures frequently make when releasing solicitations. These details often create gaps in security that are not easily fixed. Contracts are usually specific on IA metrics and targets. However, they should also be specific in requirements related to OPSEC, by listing the specific information that shall be protected. That is an efficient way to have industry and technical evaluators thinking about impact in their selection process and anticipating mitigation plans. In other words, OPSEC must be incorporated in the contracting process to ensure it gets implemented in the program from the beginning.

Lastly, OPSEC is usually treated as an overall concept. Rarely is it addressed as a stand-alone plan to achieve specific objectives, based on the specific context of the implementation. Similar to the way a complete Organizational Conflict of Interest (OCI) plan became a standard requirement for procurement of services under DISA, implementing a requirement to develop a specific OPSEC plan based on specific information criteria, metrics and risk analysis will help the industry better understand the priorities for the different missions.

WHAT THE INDUSTRY IS DOING PROACTIVELY

Three fronts are being addressed by the industry. The first is enhancements in the system to mitigate certain vulnerabilities. Enhancements in the system are not only on the service-provider side. By having more accurate understanding of the mission vulnerabilities, the industry has been able to implement enhancements in the system. These include: more robust air interface; full key management and hardened encryption algorithms in the SIM cards; better protection on the ground infrastructure; partitioning and compartmentalization of traffic and information stores; and improvement of processing and user control.

The second front is the implementation of additional internal controls to protect and safeguard sensitive information (minimizing OPSEC exposure). The industry has implemented tactics such as: full control of the lifecycle support (firmware and hardware) of the user terminals; compartmentalization of call detail, transactions and other sensitive records; protection of real-time geo-location details; and keeping subscriber control in U.S. hands, thus reducing details that can be used by foreigners (friendly or unfriendly) for collection and analysis or denial of service.

The third front is the cooperation between the industry and government agencies to better understand user requirements -- to effectively shape the roadmap for the industry. This understanding also changed the way users implement solutions. Issues such as hiding in plain sight allow the industry to lower the visibility of users in their system, and users to lower the visibility in the field. A critical factor that the industry has enhanced is back-office, having implemented better tools and strategies for network operations and helpdesk support.

CONCLUSION

It is clear that as the baseline user requirements for MSS changed, the technology was enhanced and the industry made progress in assimilating the requirements to use technology wisely. The challenge comes with the time that government regulators adapt to change, to allow progress to become implemented in certified networks. This is where users are getting creative, having a better understanding of technology and service-provider options, and crafting effective solutions to meet the requirements -- securely.

At the same time, the MSS industry segment is helping government understand what works best for the mission. Different from the old MSS model, in this new industry the mentality of “one size does NOT fit all” is becoming the norm. Customization is becoming the standard, regardless of the market segment it is targeting. Whether it is service used by first responders, intelligence or big Army, OPSEC and IA is the priority.

###