Cybersecurity in SATCOM – Examining the Layers

INTRODUCTION

As the world becomes more connected, it has become increasingly easy for people to communicate and share information. We are in an age where people can access and remotely control devices from anywhere in the world. However, these pathways of communications open up potential attack vectors for malicious actors to remotely eavesdrop, intercept or modify sensitive data.

In order to stay ahead of these malicious actors, organizations must change from the mindset of wondering "if we've been hacked" to preparing for when we are hacked. Whether it is a "script kiddie" hacker or nation-state actor, your organization will likely face ongoing and persistent attempts to breach your network. With this in mind, it's easy to see the traditional model of a single network firewall gating access to your data is no longer sufficient.

In spite of the growing number of cyber-attacks and data breaches, you don't often hear the specifics of how the incident was actualized. Malicious actors have a variety of methods at their disposal to conduct an attack and gain entry into a network or device. When an attack is underway, it may not always be apparent. There are many types of attacks to be considered. For example, an attack may involve an actor passively

monitoring traffic to identify possible times to carry out an attack based on network patterns. Another type of attack may involve the changing or corrupting of data. In the end, the results range from denial of service or the intent to deceive people with misinformation to outright fraud or worse.

It is without a doubt that the protection of sensitive data is critical to any organization. Information assurance can be achieved with the proper protection mechanisms to ensure the confidentiality, integrity, availability and non-repudiation of data.

When it comes to securing a network, all possible points of entry need to be considered, up to and including wireless communications. A Wi-Fi network presents several security challenges for any network administrator, in part because a bad actor doesn't even have to be inside the physical walls. Satellite communications (SATCOM) networks offer an even more significant problem. SATCOM has a footprint that covers large areas of land and oceans. A SATCOM network is potentially vulnerable to attack from actors located anywhere in the satellite's footprint. With government agencies being the biggest user of SATCOM, their networks present a highly desirable target for bad actors.

Applying cybersecurity in a SATCOM environment requires a layered security approach, or Defense-in-Depth as it is sometimes called. As recognized by the National Security Agency (NSA), Defense-in-Depth is an effective means to protect networks by presenting multiple obstacles for would-be hackers. This approach brings together multiple strategies to mitigate threats, protecting your data and SATCOM network.

In this paper, we will examine the following layers of defense in an iDirect Government (iDirectGov) SATCOM network: Interference Mitigation, WGS certification, TRANSEC, FIPS 140-2 certification, and Security Content Automation Protocol (SCAP).

Interference Mitigation

The growth of wireless products and services has dramatically increased in the last 25 years. The marketplace has been inundated with wireless products like phones, networking devices, and satellite radios. The advent of the Internet of things (IoT) added non-traditional communication devices like refrigerators, electric meters, and garage doors to the mix. Plus we are now looking at the next generation of wireless services: 5G and multi-orbit satellite constellations. The ability to roam freely without being tethered by a cord has made life better for some. However, the increased number of wireless products also increases the potential for radio frequency (RF) noise and interference.

One of the key elements of wireless communication is the availability and use of the RF spectrum. This is particularly true for SATCOM networks where the introduction of noise or interference, intentional or unintentional, can degrade a SATCOM network, sometimes rendering it completely unusable. Given SATCOM is a critical communications asset for the military, the stakes can be very high.

Due to the finite amount of RF, some organizations and agencies restrict the spectrum for use with specific applications or services. Despite their efforts, the ever-growing demand for wireless capability still results in congestion and interference within the RF spectrum. The industry has recognized this surge in devices and usage, and has responded with innovations to address the situation, but to date, successes have been constrained due to cost or the nature of how devices are deployed.

iDirectGov addresses the concern of interference through the use of signal excision, part of our Glowlink product line. iDirectGov's

Communications Signal Interference Removal or CSIR, our signal excision capability, eliminates an interfering signal from the authorized signal of interest (SOI). With only the SOI's center frequency, bandwidth, and symbol rate information, iDirectGov's CSIR will monitor and remove an interfering signal in real-time. iDirectGov's CSIR is capable of removing a variety of unwanted signals, whether they are modulated carriers, unmodulated tones, or interference that changes characteristics (such as burst or frequency hopping).

iDirectGov CSIR is a mature digital signal processing solution designed to excise an interfering signal before it reaches the receiver's demodulator and decoder. Based on the SOI's information noted above, iDirectGov CSIR can monitor and remove an interfering signal with as little as 1dB of power separation from the SOI. Additionally, iDirect CSIR has little to no effect on the signal quality of the SOI.

iDirectGov CSIR brings an ingenious and proven capability that protects vital communication but yet is simple to use and implement.

WGS Certification

In the 1980s the Defense Satellite Communications System (DSCS) was launched. After nearly two decades of service, the military chose to leverage the latest technological advancements to create a more powerful, longer-lasting satellite constellation. Thus was born the Wideband Global SATCOM System, or WGS. This system is so powerful that a single WGS satellite has more capacity than all of the DSCS satellites in space.

WGS enhances and augments the legacy DSCS satellite constellation, and it's continuously being updated with newer technology.

Having the WGS certification means the military has tested iDirectGov's equipment and software, and is confident our ground equipment will perform as needed. Ensuring the ability to be certified requires a ground-up design approach, and shows iDirectGov's commitment to the U.S. Department of Defense (DoD). WGS is their primary satellite constellation for communications, ranging from voice and data to video and C4ISR missions. It's also used for the GBS network, which is the government's global broadcast system used to disseminate classified and unclassified information.

Being WGS certified gives our customers the assurance that they are working with a platform that's been thoroughly tested, vetted, and has the authority to operate (ATO) on the WGS constellation. The WGS certification process is multi-faceted and broken into four phases.

Negotiations with the U.S. Army Strategic Command (ARSTRAT) begin with what is known as Phase Zero. During that phase, ARSTRAT reviews iDirectGov's proposed test matrix showing how we will be testing our products to ensure they are compliant with access requirement for the WGS constellation.

Once the proposed test is approved by ARSTRAT, Phase One begins. Phase One involves internal testing at iDirectGov. Some of these tests are quick, while some take several days to complete. Along the way, we may find areas of improvement that give us the opportunity to refine the product and make it better for the warfighter. This phase alone can take a few months to potentially a year.

Once all the internal testing is complete, a test report is created and submitted to ARSTRAT. If approved, Phase Two begins and the report is released to another organization called Joint Satellite Enterprise Center (JSEC). They conduct their own check to ensure our test results match what was presented in the report. This phase can last anywhere from three to six months.

Once JSEC has completed their work, they produce their own test report and deliver it to ARSTRAT, beginning Phase Three. ARSTRAT reviews and grants a certification number authorizing the products and software to operate on the WGS constellation.

TRANSEC

TRANSEC (Transmission Security) protects against adversaries who try to obtain information through monitoring the satellite waveforms traveling between remotes and hubs by

addressing vulnerabilities in an IP-based VSAT architecture's transmission path. Factors such as increased traffic, terminal spoofing, and data interception can all be used to infer classified data.

The waveforms and protocols of TRANSEC-enabled networks are specially designed always to appear the same, regardless of the amount of traffic or the number of active users.

TRANSEC enables the following protections:

- Masks Channel Activity – conceals traffic volumes and obfuscates acquisition activity.
- Controls Channel Information – disguises traffic volumes to secure traffic source and destination.
- Authenticates and Validates Hub and Remotes – ensures remote terminals connected to the network are authorized users.

With the release of the 9-Series Satellite Routers and Defense Line Cards (DLCs), iDirect Government has developed a TRANSEC module designed to meet the stringent FIPS 140-2 Level 3 requirements as defined by the National Institute of Standards and Technology (NIST). Through hardware and software development, the embedded yet independent TRANSEC module operates through a separate and trusted path from all other interfaces on the product. The module also features a robust physical security measure for tamper prevention and the capability to zeroize the security keys or critical security parameters (CSPs) stored on the module itself. If required, the revocation or zeroization of the keys can be accomplished either over-the-air (OTA) by the hub operator or locally on the remote by authorized personnel.

ONE-WAY NETWORKS

iDirectGov has further enhanced its TRANSEC capabilities by securing one-way broadcast transmissions. Based on their encapsulation method, LEGS, the iDirectGov platform can provide the same level of security for one-way networks as it provides to two-way networks mentioned above. The 900 and 9350 (remotes with dual-modulator support) are capable of dual-domain TRANSEC – the ability to establish two independent chains of trust (sets of X.509s) between two different Certificate Authorities (CAs).

An example use case of this feature would be one demodulator on a two-way TRANSEC network while the second demodulator receives a separate one-way TRANSEC secured broadcast. With one-way TRANSEC, Elliptical Curve Cryptography (ECC) is used for key generation along with X.509 certificates for authentication in each security domain.

iDirectGov's 9-Series Satellite Routers and DLCs have been designed to provide higher performance and data rates plus increased functionality and security compared to their predecessors

X.509 CERTIFICATES

SATCOM networks are vulnerable when looking at hub and remote unit validation. In traditional single channel per carrier (SCPC) architectures, established links remain active for very long periods of time. Because these connections are point-to-point fixed and there is a significant level of coordination between personnel commissioning the SCPC, users have a high degree of confidence an adversary is not trying to assume the identity of a trusted entity. In time division multiple access (TDMA) networks, remotes are routinely coming into and dropping out of the network. This is especially true of networks with mobile or itinerate terminals where terminals are located in moving vehicles, aircraft or maritime vessels. This type of dynamic environment gives an adversary a greater opportunity to obtain a VSAT remote through lawful or illicit channels, spoof the device ID, and insert a rogue remote into a secure network. Equally feasible is an adversary acquiring a VSAT hub and coaxing a blue force remote into the adversary's network.

To mitigate this risk, iDirectGov has implemented X.509 digital certificates on TRANSEC remotes. An X.509 certificate uses RSA public-key encryption. With public-key

encryption, two related keys are generated: one private key and one public key. The functionality of these keys is so that anything encrypted with the public key can only be decrypted with the private key, and anything encrypted with the private key can only be decrypted with the public key. In the iDirectGov system, X.509 certificates can be generated via the NMS server. Certificates are placed on all TRANSEC line cards and Protocol Processors as well as on the remotes. The hub system keeps the public keys of each remote configured to operate on the hub, and the remotes have the public keys of each hub. During network acquisition, the remote encrypts its X.509 certificate with its private key, and the hub verifies by decrypting the certificate with the remote's public key and vice versa. This process ensures a remote is not only authorized to operate in the network, but that the hub is a trusted entity.

Through these security measures, the use of TRANSEC adds an authentication mechanism that prevents adversaries from joining a protected network or launching "man-in-the-middle" attacks. Conversely, adversaries would not be able to re-direct a TRANSEC-enabled remote to joining another network without the proper identification and authentication.

FIPS 140-2 Certification

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government security standard for accrediting cryptographic modules. The standard is published by the National Institute of Standards and Technology (NIST).

FIPS 140-2 provides stringent third-party assurance of security claims on any product containing cryptography that may be used by a government agency. FIPS 140-2 establishes the Cryptographic Module Validation Program (CMVP) as a joint effort between NIST and Canada's Communications Security Establishment (CSE).

As defined by NIST, FIPS 140-2 has four levels of security for hardware:

- Level 1 provides the lowest, basic level of security. Only one approved security function or algorithm is required, and no specific physical security mechanisms are required other than production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.
- Level 2 requires features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access.
- Level 3, in addition to the tamper-evident requirements of Level 2, dictates a mechanism to prevent an intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms are required to have a high probability of detecting and responding to attempts at physical access and/or use or modification of the cryptographic module. Examples include the use of strong enclosures and tamper detection/response circuitry that zeroes all plain text CSPs when the removable covers/doors of the cryptographic module are opened.
- Level 4 requires that the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

In addition to the hardware requirements described above, FIPS validation applies to the cryptographic solution as a whole, including the operating system and software.

iDirect Gov's TRANSEC module in the 9-Series Satellite Routers and Defense Line Cards is certified FIPS 140-2 Level 3. With the introduction of this TRANSEC module, a daughter card is integrated at the board level. The TRANSEC module will contain all of the cryptographic information and functionality, and most importantly, can be zeroized when compromised.

In addition to enabling FIPS 140-2 Level 3 certification, the TRANSEC module architecture brings a major improvement to the FIPS certification process. As mentioned previously, our Network Management Software (NMS) is a key component of our FIPS-certified solution. By moving the encryption function to the TRANSEC module, re-certification is only required when there's a change to code on the TRANSEC module.

AES 256 BIT ENCRYPTION

A great deal of traffic volume and priority information can be gleaned by examining the in-band or out-of-band control information within an encrypted TDMA network. The IP header of a packet contains source, destination, and priority information. For a TDMA network to provide the quality of service (QoS) needed to support real-time traffic, data quantities and prioritization information must be gathered. This information could be more useful to an adversary than channel activity data because it is specific enough to delineate between general communications (like email and web traffic) and tactical communications (like voice and video).

The only solution for this vulnerability is to completely encrypt all Layer 2 information as well as any control information disseminated to the remotes. The encryption methodology must be secure enough to thwart an adversary long enough that the data becomes old and useless. We have implemented Federal Information Processing Standard 140-2 certified 256-bit keyed Advanced Encryption Standard (AES) for all Layer 2 and control information on our products. The encryption of the Layer 2 frames has a side benefit of re-encrypting the data payload. Therefore, the transmitted IP header itself is AES-encrypted. Additionally, the iDirectGov TRANSEC TDMA slot is a fixed size to obfuscate any traffic characteristics. This Layer 2 encryption solution solves all existing control channel vulnerabilities. The iDirectGov Layer 2 encryption method goes a step beyond to feature over-the-air (OTA) key updates and a unique Layer 2 frame format, including an Initialization Vector (IV) that ensures randomization of repetitive data streams. The net result is that adversaries are precluded from detecting any repetitive pattern, which could aid them in deciphering encryption algorithms.

Security Content Automation Protocol (SCAP)

SCAP is the configuration standard for the United States Department of Defense (DoD) Information Assurance (IA) program and IA-enabled devices and systems.

Since 1998, the Defense Information Systems Agency (DISA) Field Security Operations (FSO) has played a critical role in enhancing the DoD's security systems by providing SCAPs. These provide technical guidance to "lock down" information systems and software that might otherwise be vulnerable to a malicious computer attack. iDirectGov's implementation of SCAP standards ensures the highest level of compliance has been met. In addition, we support a number of manual configuration changes to meet additional SCAP guidelines, including Red Hat Linux-specific recommendations.

Security Readiness Review (SRR) scripts test products for SCAP compliance and are available for operating systems and databases that have SCAPs.

Information Assurance is becoming a very critical component of any organization's information systems management strategy to ensure data and systems' integrity, confidentiality, and availability are protected and available to support the missions at hand. Threats to systems and data come in many

forms ranging from malware infecting a system to a sophisticated cyber-attack on critical systems by state-sponsored actors. Cyber-attacks have become so sophisticated and serious that governments have devoted entire organizations specializing in counter cyber intelligence to combat this problem around the clock.

Conclusion

Individuals and organizations are able to connect and communicate with each other more easily now than ever. Unfortunately, this ability to connect has also made it easier for malicious actors to reach out and disrupt the flow of information and collaboration between others.

The capabilities and features embedded in the iDirectGov platform enhance and protect critical communications. The inherent security we offer protects and minimizes the attack surface from actors that may, intentionally or unintentionally, interfere with your line of communications. Our customers can trust our security measures are not only battle-tested but also certified to meet today's strictest security standards.

About

iDirect Government, LLC a wholly owned subsidiary of ST Engineering iDirect, delivers secure satellite-based voice, video and data applications with anytime and anywhere connectivity in the air, at sea and on land. iDirect Government's advanced satellite IP solutions are used for critical ISR, airborne, maritime and COTM communications to support force protection, logistics, situational awareness, disaster recovery and emergency response. Building on more than 15 years of global satellite communications experience, iDirect Government provides the most bandwidth-efficient, scalable and highly secure platform to meet specialized applications of multiple federal, state and local government agencies, including the Department of Defense, both domestically and abroad.

iDirect Government's specialized technology includes transmission security (TRANSEC), Communication Signal Interference Removal (CSIR™) anti-jam technology and Open Antenna Modem Interface Protocol (OpenAMIP).

iDirect Government is headquartered in Herndon, Va. For more information, please visit http://www.idirectgov.com.