iDirect **GOVERNMENT**

WHITE PAPER

Cybersecurity in SATCOM – Taking a Defense in Depth Approach

INTRODUCTION

Connectivity. In March of 2020, what had been a nice-to-have for streaming video and shopping online became essential as millions of people converted to a work-from-home model almost overnight. The COVID-19 pandemic highlighted so many benefits of the global network – access to information, collaboration, connections to family and friends. The already high demand for bandwidth soared. However, these increased pathways of communications expanded potential attack vectors for malicious actors to remotely eavesdrop, intercept or modify sensitive data.

To stay ahead of these malicious actors, individuals and organizations must change from the reactive mindset of wondering "if we've been hacked" to a preventive mindset, building in layers of protection to combat these harmful attacks. Whether it is a "script kiddie" hacker or nation-state actor, all networks will likely face ongoing and persistent attempts to breach. Looking at the new highly-distributed and decentralized networking paradigm, it's easy to see the traditional model of a single network firewall gating access to an organization's data is no longer sufficient.

In spite of the growing number of cyber-attacks and data breaches, organizations don't often share 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, intrusions may involve an actor passively monitoring traffic to identify possible times to carry out a future 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.

The protection of sensitive data is, without a doubt, 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.

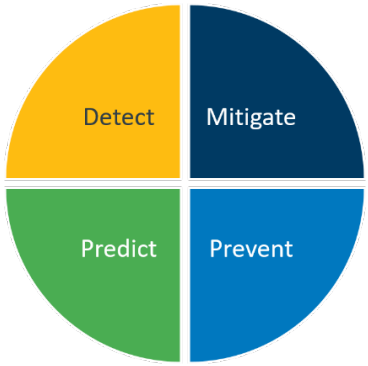
When it comes to securing a network, all possible points of entry should be assessed, up to and including wireless communications. A Wi-Fi network presents several security challenges for any network administrator, in part because a bad actor doesn't even have to be inside the physical walls. Satellite communications (SATCOM) networks offer an even more considerable 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 an organization's data and SATCOM network. The idea behind this approach is if one mechanism fails, another checkpoint is ready and waiting to thwart an attack.

This paper examines the following layers of a Defense-in-Depth approach to an iDirect Government (iDirectGov) SATCOM network: detect, mitigate, prevent and predict.

Detect

Detection allows the user to discover and identify the existence of a security lapse. In an iDirectGov network, detection centers around the iVantage network monitoring tool, spectrum monitors and geolocation product.



iVANTAGE

As part of the Network Management System (NMS), iVantage provides an easy-to-use responsive graphical user interface (GUI) and reports on performance irregularities in an organization's SATCOM network.

Network performance is monitored in iVantage including in-routes, remotes, applications and the IP packet level. With this information a network operator can immediately respond to any threats to the security of the network.

SPECTRUM MONITORING

iDirectGov's spectrum monitoring tools perform automatic and operator-directed monitoring to detect interferences and unauthorized users,

measure carrier and transponder performance, and generate out-of-tolerance alarms.

These tools allow the user to effectively measure and analyze the transponder spectrum. The spectrum monitoring products can be used as stand-alone appliances or as part of a larger spectrum monitoring network to include geolocation capabilities. The flexible architecture allows for plug-and-play operation locally and/or remotely via a standard LAN/WAN.

GEOLOCATION

Geolocation allows operators to view real-time spectra for the detection and characterization of interference. The Model 8000 seamlessly transitions from detecting the interference to geolocating the interference with the click of a button. Model 8000 geolocates transmit terminals quickly and accurately. It locates the interference by taking advantage of the weak replica of the signal that an adjacent satellite will receive. Downlinks for the primary and adjacent satellite are acquired and analyzed to extract precision time difference and/or frequency difference information used for locating the interfering signal. Once the signal has been located, the operator is ready to take the appropriate steps to mitigate.

Mitigate

Mitigation is used to remove or avoid any potential network threats. iDirectGov uses Communication Signal Interference Removal (CSIR™) technology and dual-mode and beam choice features to mitigate threats to a SATCOM network.

The growth of wireless products and services has dramatically increased in the last 25 years. The marketplace has been inundated with wireless products such as phones, networking devices and satellite radios. The advent of the Internet of Things (IoT) adds non-traditional communication devices such as refrigerators, electric meters and garage doors to the mix. Plus, the next generation of wireless services are on the horizon: 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 brings the potential for more 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 and 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 by responding with innovations to address the situation. To date, successes have been constrained due to cost or the nature of how devices are deployed.

CSIR™

iDirectGov addresses the concern of interference through signal excision technology, part of the Glowlink product line. iDirectGov's Communications Signal Interference Removal (CSIR) 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 can remove 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 and is simple to use and implement.

DUAL-MODE

Dual-mode gives users the benefit of targeted connectivity combined with ubiquitous global coverage. iDirectGov's 9-Series modems can operate on both Evolution and Velocity networks, giving the user the ultimate flexibility.

BEAM CHOICE

When designing SATCOM networks in a mobile environment, the beam strength and the footprint are of the utmost importance, especially in theater. By providing users "Beam Choice," they can prevent network reacquisition due to a weakening signal or a change of footprint. Operators can manually select the ideal beam for their missions rather than using the automated process.

Beam Choice is not limited to just beams in an Evolution network. It also allows for selection of beams in a Velocity network for complete global coverage.

Prevent

Preventing security threats moves the battle for security to a more proactive stance. iDirectGov utilizes transmission security (TRANSEC) and Information Assurance (IA) to protect communication signals and network hardware from potential threats.

TRANSEC

TRANSEC 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), iDirectGov has delivered 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 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.

> *"The value of security in a military SATCOM network is life or death"*

ONE-WAY NETWORKS

iDirectGov has further enhanced its TRANSEC capabilities by securing one-way broadcast transmissions. Based on its encapsulation method, the iDirectGov platform can provide the same level of security for one-way networks as it provides for 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.509) between two different Certificate Authorities (CAs).

An example of this feature is having 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 balance higher performance and data rates plus increased functionality and security with the solid reliability the iDirectGov brand represents.

INFORMATION ASSURANCE

Information Assurance (IA) refers to managing the risks of processing, storing and transmitting data and the systems used for those actions. IA uses physical, technical and administrative tasks to control these risks. iDirectGov utilizes a two-pronged approach to IA: one safeguards the servers and a second covers the remotes. By protecting both the servers and the remotes, potential attack surfaces are reduced.

IA is a critical component of any organization's information systems management strategy to ensure data and protecting the 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.

SECURITY CONTENT AUTOMATION PROTOCOL (SCAP)

SCAP is the configuration standard for the United States Department of Defense (DoD) IA program and IA-enabled devices and systems. SCAP services are offered on all servers in an iDirectGov network, including the NMS, Protocol Processor (PP) and the Global Key Distributor (GKD).

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 is met. In addition, iDirectGov supports 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.

SHIELD

SHIELD is a service available to users of Major Defense releases beginning with Evolution 4.2.2.0. iDirectGov identifies potential vulnerabilities in remotes using a DoD-approved scanning tool called Nessus developed by Tenable. The Nessus scanner identifies vulnerabilities that could allow unauthorized control or access to sensitive data, misconfiguration, default passwords and service vulnerabilities.

iDirectGov conducts the SHIELD scans to evaluate the 9-Series remotes for vulnerabilities that hackers could use to access a system or network. The data is then used to design a Remote Security Bulletin (RSB) that is posted to the iDirectGov TAC website for iSupport Premium customers and for SHIELD subscribers to load to their remote hardware. These security update packages for remotes are available

approximately twice per year and cover all 9-Series modems including airborne variants.

Predict

Predictive measures lay the groundwork to avoid security threats before they are launched by bad actors. By using iDirectGov's Satellite Access Management System (SAMS), reporting tools and Network Health Checks, users can predict potential outages and threats before they happen.

SATELLITE ACCESS MANAGEMENT SYSTEM

SAMS™ is a powerful satellite capacity and link resource management tool used for planning and organizing space, ground and network assets that support satellite communications. Using SAMS, satellite traffic planners can manage their network traffic and perform link budget analyses to optimize space assets while meeting data throughput needs. Designed for both fixed and mobile networks, it provides network-wide visibility and performance assessment.

REPORTING

When looking at reports, some of the biggest benefits are an increased understanding of risks and opportunities in an organization's satellite network. Reports can enable the streamlining of processes and improve efficiency.

The robust NMS provides automatic alerts and warnings that can help operators anticipate potential attack vectors. Performance stats per network, in-route, remote, application and IP packet level permit effective network management.

Outside of the NMS, iDirectGov offers a Bandwidth Timeslot Correlator (BTC) that allows network operators to view and analyze bandwidth and timeslot allocations. The BTC expands Network Operations Center (NOC) capabilities in a Time Division Multiple Access (TDMA) network to enable network operators to manage time slot allocations and to optimize networks to avoid network traffic gridlocks. The software module also provides an automated graphical representation of historical time slot usage and bandwidth for a given network, in-route group or remote. By using historical data, users can re-define and enhance upstream links for better throughput performance and achieve savings in satellite bandwidth and costs. These report designations are configurable through a user interface.

NETWORK HEALTH CHECKS

Maintaining a healthy network is one of the most important steps to security and efficiency of a satellite network. Through the iDirectGov Premium iSupport program, a comprehensive network analysis can be conducted in four key phases: customer consultation, data collection, data analysis and report documentation. Through the health check, network conditions are assessed and recommendations are made for improved efficiency and security.

Conclusion

Individuals and organizations can 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 users.

The capabilities and features embedded in the iDirectGov platform enhance and protect critical communications. The inherent security in iDirectGov's solutions protects and minimizes the attack surface from actors that may, intentionally or unintentionally, interfere with lines of communications. Customers can trust iDirectGov security measures to be battle-tested and 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.