

**Transmission Security
(TRANSEC) in an IP-based
VSAT Architecture**

February 2011

As the ability to monitor satellite transmissions grows more sophisticated, the need to implement increased levels of security becomes more critical. In combatant situations, where even a small spike in traffic can be a critical piece of intelligence, the need to mask any communications activity becomes apparent. The National Security Agency (NSA) in the United States has outlined the following vulnerabilities inherent in an IP-based TDMA transmission that must be addressed in order to provide true Transmission Security, or TRANSEC:

- ◆ *Channel Activity* – The ability to secure transmission energy to conceal traffic volumes.
- ◆ *Control Channel Information* – Disguise traffic volumes to secure traffic source and destination.
- ◆ *Hub and Remote Unit Validation* – Ensure remote terminals connected to the network are authorized users.
- ◆ *Anti-Jam and Low Probability of Intercept* – While a consideration, this is not a mandate by the NSA or any other organization.

This paper will discuss elements and considerations of providing a TRANSEC-compliant IP-based VSAT network and the approach iDirect has taken to implement TRANSEC.

Background

TRANSEC requires all network control channels and Management & Control (M&C) data to be encrypted and that any and all traffic engineering information be obfuscated from an adversary. For example, TRANSEC requires a communications channel to appear completely full to an adversary even if little or no actual data is flowing. This is contrasted with communications security, where the actual communication (e.g. voice, video or data stream) is encrypted but certain header information is sent in the clear. While the encryption is virtually impenetrable, the information in the IP header including the source address, destination address and, most importantly, the ToS field are in the clear. With the IP header of an encrypted packet in the clear an adversary can determine how much of the traffic stream is voice, video or data. More significantly, an adversary could determine when high-priority flash-override traffic has been initiated and from which location.

In an SCPC (single channel per carrier) satellite network topology, achieving TRANSEC compliance is relatively straight forward. For SCPC connections, a bulk encryptor is employed to encrypt any data and control information traversing the network. The IP header of the packet would be encrypted by the bulk encryptor prior to being transmitted to the satellite. In addition, since an SCPC link is static and always on and no control information needs to be exchanged between the SCPC modems, all of the TRANSEC requirements are met.

In a TDMA network, TRANSEC compliance is more difficult. A TDMA network dynamically allocates bandwidth to remotes; therefore, there must be some type of control information transmitted to each device in the network. This control data, containing traffic engineering information, as well as information available from an encrypted IP packet header, can be exploited by an adversary. For example, anomalous traffic volume to a specific remote can indicate new activity in that area while varying ratios of voice-to-data traffic can denote the distribution of intelligence (data) compared to lower priority voice traffic.

iDirect has implemented the following solutions in response to the security vulnerabilities of a TDMA VSAT network.

Channel Activity

Challenge

The first vulnerability that exists in a TDMA network is the availability of traffic engineering information. In an SCPC network, the link is static with no variation in transmission characteristics based on end user communications. An adversary looking at a satellite transponder with a spectrum analyzer will see a constant RF signal. This is contrasted with a TDMA network. A TDMA in-route carrier energizes and de-energizes as traffic flows and stops. The on and off nature of a TDMA in-route is the natural extension of the ability to allocate satellite transponder space to remotes that have transient demands. While this characteristic makes TDMA networks much more bandwidth efficient, it allows an adversary to determine peak periods of activity, identify unusual or unexpected activity spikes, and identify locations of remotes that have remained quiet for a period of time and suddenly experience increased traffic volumes. The obvious risk in having this information in the hands of an adversary is the potential to extrapolate timing and location of scale of strategic activity.

Solution

iDirect has implemented free slot allocation in its TDMA bandwidth distribution algorithm. With free slot allocation, an adversary snooping satellite transponder energies will see a constant “wall of data” regardless of traffic profiles. As the name implies, free slot allocation keeps the in-routes active regardless of actual traffic flows. Free slot allocation preserves the efficiencies of a TDMA system while obfuscating actual traffic volumes, negating the risk of using transmission activity as an intelligence gathering mechanism.

Acquisition Activity

Challenge

The rate at which remotes acquire into a network can provide critical information to an adversary about troop activities. All TDMA networks provide a dedicated channel for remote acquisition activity. If adversaries monitor the activity in this channel they will be alerted to troop movements by a flurry of acquisition activity.

Solution

iDirect has exceeded the TRANSEC requirements by addressing the acquisition activity vulnerability. The iDirect acquisition algorithm inserts dummy bursts from remotes already in the network and intentionally skips acquisition bursts at times of high activity. The algorithm ensures an adversary sees only a random distribution of acquisition activity. The iDirect acquisition algorithm goes a step further by randomly varying the dummy burst’s frequency, timing and power. This randomization ensures an adversary cannot distinguish between a dummy burst and actual acquisition activity.

Control Channel Information

Challenge

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. As previously discussed, the IP header of a packet contains source, destination and priority information. In order for a TDMA network to provide the quality of service 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, versus tactical communications like voice and video.

Solution

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 unusable. iDirect has implemented FIPS 140-2 certified 256 bit keyed AES encryption for all Layer 2 and control information. 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 iDirect TRANSEC TDMA slot is a fixed size, again to obfuscate any traffic characteristics. This Layer 2 encryption solution solves all existing control channel vulnerabilities. The iDirect Layer 2 encryption method goes a step beyond to feature over-the-air key updates and a unique Layer 2 frame format including an Initialization Vector that ensures randomization of repetitive data streams. The net result is that adversaries are precluded from detecting any repetitive pattern, which can aid in deciphering encryption algorithms.

TDMA TRANSEC SLOT					
Encryption Header			Segment		FEC Coding
IV Seed	Key ID	Enc	Demand	LL Headers & Payload	

Figure 1

Hub and Remote Unit Validation

Challenge

Another vulnerability of a TDMA VSAT system is the concept of Hub and Remote Unit validation. In traditional SCPC architectures, when a link is established, it remains active for very long periods of time. Because these connections are fixed, and there is a significant level of coordination between personnel commissioning the SCPC, a high degree of confidence exists that an adversary is not trying to assume the identity of a trusted entity. In TDMA networks, remotes are routinely coming into and dropping out of the network. This is especially true of networks with COTM (Communications on The Move) terminals where vehicles are traveling under bridges and behind buildings. This type of dynamic environment gives an adversary a greater opportunity to obtain a VSAT remote through licit 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 terminal and coaxing a blue force remote into the adversary's network.

Solution

To mitigate this risk, iDirect has implemented X.509 digital certificates on TRANSEC remotes. An X.509 certificate utilizes 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 such 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 iDirect system, X.509 certificates can be generated via the NMS server or provided by a third party. 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 device. 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.

Operational Implementation

Challenge

Implementing security and ensuring all security policies are followed can be a burden to the soldier in the field. Implementing TRANSEC and performing key management is no exception. A robust TRANSEC network requires the use of at least two network-wide keys. One key, commonly known as the passphrase, is typically long lived and is used to encrypt acquisition activity and one key which is used to encrypt frame header information. The use of front panel displays to enter a passphrase and external key fill mechanisms places an undue burden on the warfighter and introduces security vulnerabilities.

Solution

iDirect has implemented a FIPS-approved software method of key generation and automatic, over-the-air key distribution protocol. Not only does the software-based key generation and key distribution mechanism make TRANSEC operation simpler and more convenient for the warfighter, it makes the system much more secure by removing a human from key distribution.

Another advantage of automatic key generation and distribution is that it seamlessly enables a global COTM TRANSEC network. By automatically generating and distributing new acquisition passphrases a single, dynamic passphrase can be utilized across global networks.

DVB-S2 Considerations

For increased bandwidth efficiencies, DVB-S2 offers faster data throughput and better coding capability. DVB-S2 uses the industry's leading forward error coding technology, Low-Density Parity-check Codes (LDPC) coupled with BCH coding. This concatenated LDPC-BCH coding scheme provides performance very close to the theoretical Shannon limit resulting in a 30-40 percent bandwidth efficiency increase over existing DVB-S systems. iDirect's latest release iDX 2.3 enables TRANSEC over DVB-S2/ACM thus allowing not only additional bandwidth efficiencies stemming from Adaptive Coding and Modulation (ACM) but also providing an extra level of security by creating a continuous wall of strongly encrypted traffic that remains constant. With iDX 2.3 iDirect also introduces FIPS 140-2 Level 1 certified software as well as FIPS 140-2 Level 2 compliant* TRANSEC-capable IP modems.

Conclusion

There are inherent benefits to the IP-based DVB-S2/TDMA platform that iDirect utilizes, with respect to bandwidth efficiency, scalability and the scope of applications that it enables. There are also inherent security risks with a TDMA platform. The iDirect TRANSEC over DVB-S2 architecture is able to provide the highest levels of network security while maintaining the efficiencies and benefits of the TDMA architecture. iDirect has implemented the most efficient TRANSEC -compliant network architecture in the VSAT industry today, which ensures the QoS characteristics of the network are preserved.

* Certification pending.