How to Secure Your Network

Hendrik Beukes,

Senior Professional Services Engineer

What is TRANSEC

- Transmission Security (TRANSEC) prevents an adversary from exploiting information available in a TDMA satellite network even without defeating encryption.
- With only link encryption, an adversary can still answer questions like:
  - What types of applications are active on the network?
  - Who is talking to whom?
  - Is the network or a particular remote site active now?
  - Based on traffic analysis, what is the correlation between network activity and real world activity?
  - Is a particular remote site moving?
  - Is there significant acquisition activity?

All Defense-Grade Products Support TRANSEC

Hub & Line Cards

DLC-T, DLC-R

- DLC-T supports DVB-S2/DVB-S2X
- DLC-R demodulates up to 16 channels
- FIPS 140-2 Level 3, TRANSEC
- Evolution, Velocity

Tactical Hub

- Cost-effective, compact, durable
- Compatible with any Defence remote
- FIPS 140-2 Level 3
- MIL-STD 810G
- **R**uggedized **a**nd **V**irtualized **E**nviron.

Remote Solutions

9-Series

- Rackmount and board (manpack)
- DVB-S2/ACM w/ ATDMA returns
- 8-port GigE switch (9350)
- 30% reduced SWaP (950mp)
- FIPS 140-2 Level 3, TRANSEC, MIL-STD 810G, WGS
- Evolution, Velocity

9-Series Aero

- Board, rackmount, and ARINC
- Ultra high-speed COTM (over 1,600 km/hr)
- 2nd demodulator for multicast overlay or beam switching
- FIPS 140-2 Level 3, TRANSEC, MIL-STD 810G/DO-160G, WGS
- Evolution, Velocity

ST Engineering

TRANSEC Goals

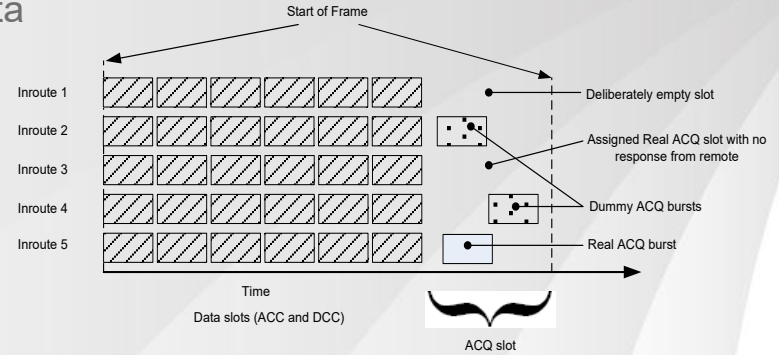
	TRANSEC Requirement	Benefits
1	Mask Channel Activity	Prevents transmission activity from being used as an intelligence gathering
2	Control Channel Information	Detection of repetitive data streams unsuccessful
3	Hub and Remote Authentication and Validation	Ensures only authorized use of network resources

TRANSEC Goal #1 – Mask Channel Activity

- Transmission activity can be used as an intelligence gathering mechanism
  - TDMA carriers are based on dynamic traffic bursts so changing traffic volumes and number of active senders can be detected.
  - DVB-S2 carriers send easily identifiable “fill frames” when there’s no user data to send.
- These vulnerabilities allow adversaries to extrapolate information on timing, location or scale of strategic activities.

TRANSEC Goal #1 – Mask Channel Activity

- TRANSEC negate these risks by:
  - Using Free Slot Allocation for TDMA bandwidth distribution
    - Creates a constant “wall of data” regardless of traffic profiles
    - Empty bursts are indistinguishable from user data
  - Creating fill-frames with random data for underutilized DVB-S2 carriers
    - Empty frames are indistinguishable from user data
  - Obfuscating acquisition activity
    - Creates traffic in the acquisition slot when no remotes are actually joining the network
    - Suppresses acquisition slot bursts even when remotes are acquiring



ST Engineering

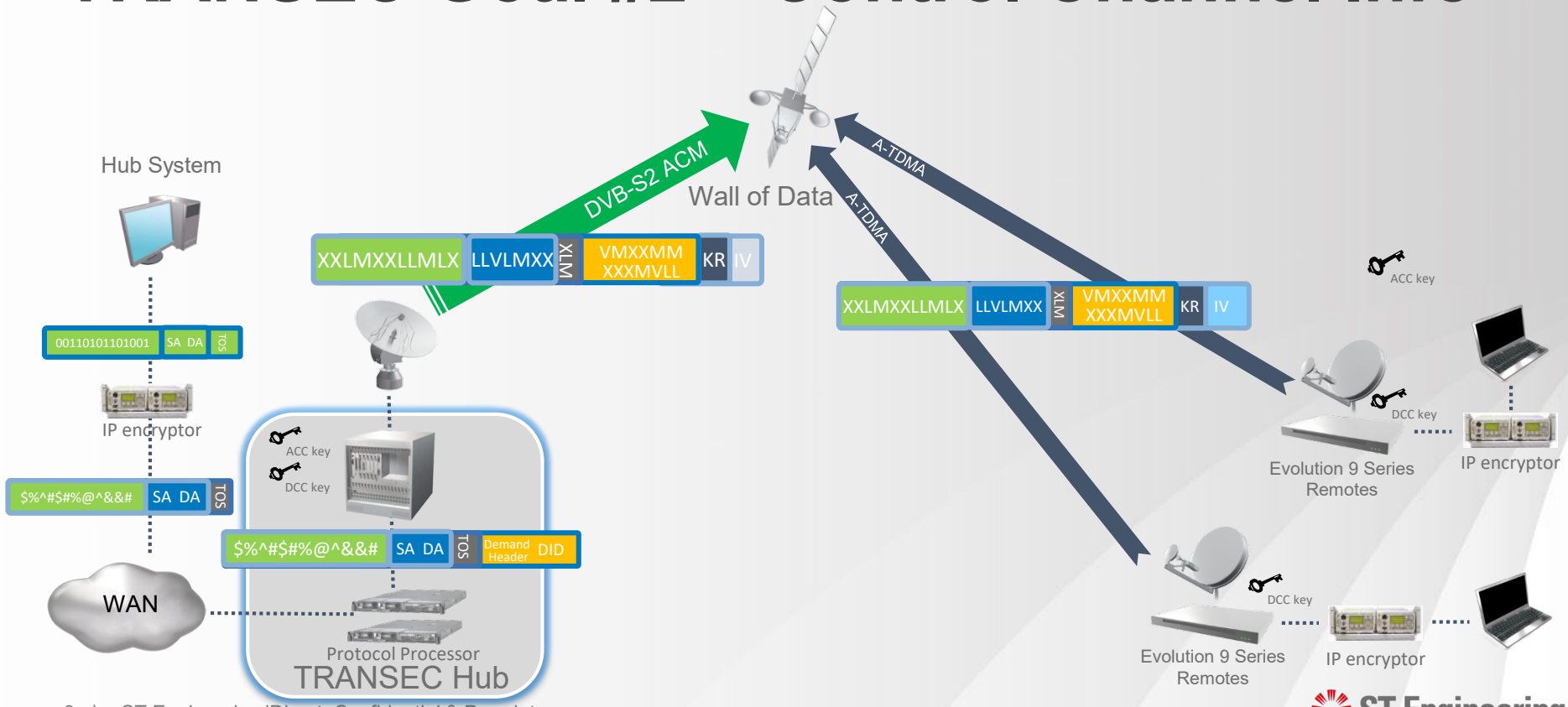
TRANSEC Goal #2 – Control Channel Info

- When only user data payloads are encrypted, a great deal of data is still available
  - Both Layer 2 and Layer 3 packets have traffic engineering information (source, destination, priority, size) embedded in their headers
    - Size and priority information can betray the type of application in use.
    - Source and destination tell an adversary who is talking and when.
  - Layer 2 Control & Signaling information sent in the clear can reveal network activity levels.

TRANSEC Goal #2 – Control Channel Info

- TRANSEC solves this by:
  - Encrypting both Layer 3 payload, header, as well as Layer 2 traffic and signaling.
  - Changing encryption keys frequently.
- Acquisition Ciphertext Channel (ACC)
  - Only used during Acquisition and Authentication.
  - AES 256-bit CBC symmetric encryption.
  - Key is initially injected into the remote manually (RSP) then updated over the air in operation.
  - Key is rolled every 28 days by default. Key is stored if the power is turned off. Remote must manually rekey if it is out of network for two keyrolls.
- Data Ciphertext Channel (DCC)
  - Encrypts all user data traffic with the DCC key using AES 256-bit CBC symmetric encryption.
  - Masks activity with random blocks of data when remotes have no data to send (“Wall of Data”).
  - Key is updated over the air every 8 hours by default. Not stored if power is cycled.

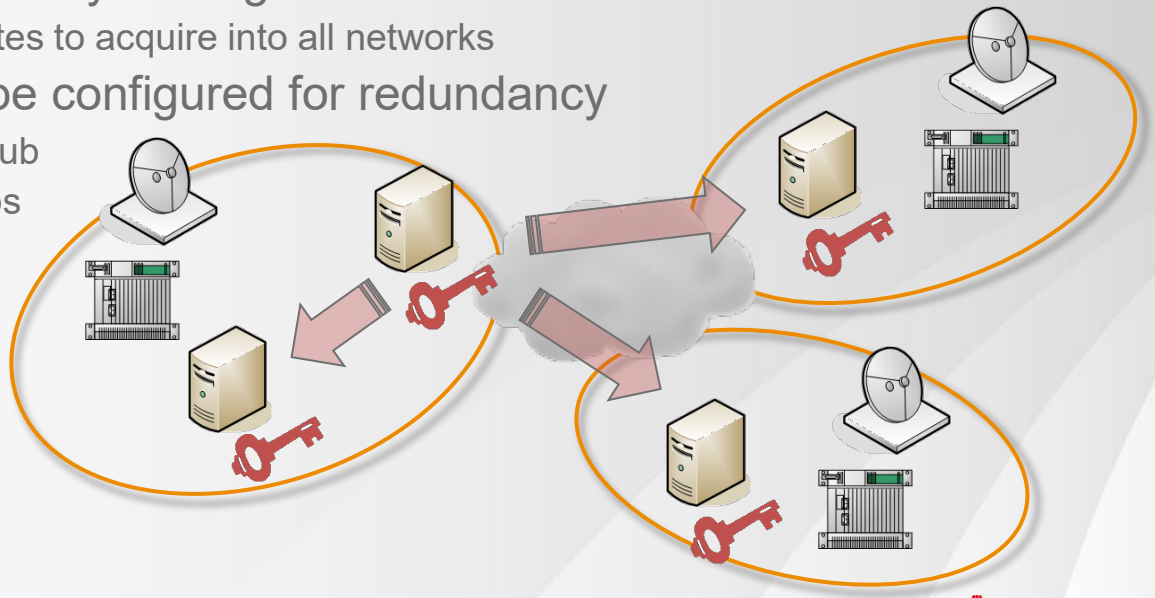
TRANSEC Goal #2 – Control Channel Info



ST Engineering

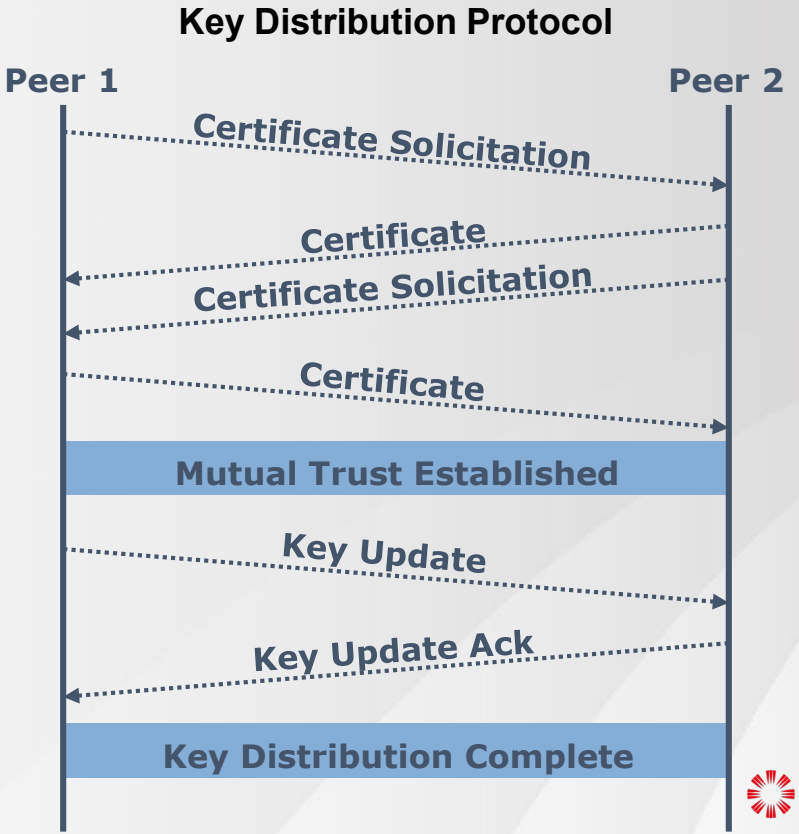
TRANSEC Goal #2 – Control Channel Info

- Global Key Distributor (GKD)
  - GKD distributes ACC key among one or more networks
    - Allows roaming remotes to acquire into all networks
  - Multiple GKDs can be configured for redundancy
    - Within an individual hub
    - Between multiple hubs



TRANSEC Goal #2 – Control Channel Info

- Key Rolls
  - Changing encryption keys periodically helps prevent attackers from deriving keys from captured data (cryptanalysis).
  - iDirect TRANSEC makes rolling period configurable.



ST Engineering

TRANSEC Goal #3 – Hub/Remote Validation

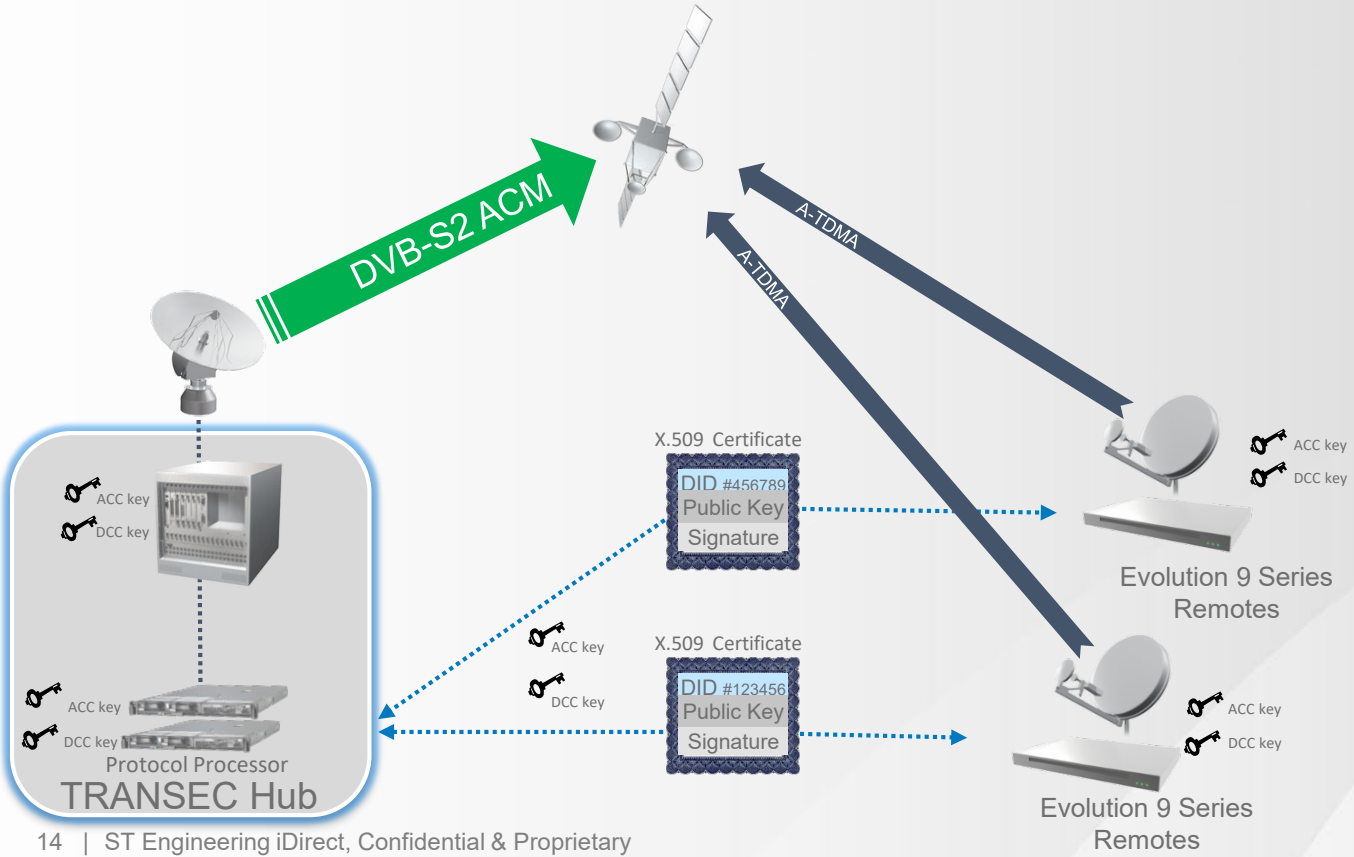
- Unauthorized use of network resources can lead to a “man-in-the-middle” attack
  - A remote might be “spoofed” and inserted into a secure network.
  - A secure remote might be coerced into joining an insecure network.

- While these kinds of attacks are extremely difficult even in non-TRANSEC environments, the risk of eavesdropping cannot be ignored.

TRANSEC Goal #3 – Hub/Remote Validation

- TRANSEC eliminates these threats by:
  - Using Public Key Infrastructure (PKI)
    - Key distribution
    - Message authentication
  - Employing X.509 standards for:
    - Verifying identities
    - Establishing trust between network elements
    - Providing methods for dealing with security compromises
- Each network element (PP, HLC, remote) has a X.509 certificate
  - A certificate is a document that connects a public key to an identity.
  - Used to authenticate remotes, PPs, HLCs, and build a chain of trust.
  - Certificates are issued by iDirect CA (embedded in iVantage NMS).

TRANSEC Goal #3 – Hub/Remote Validation



Acquisition and Authentication

ST Engineering

TRANSEC Goal #3 – Hub/Remote Validation

- Handling Security Compromises
  - “Zeroize” is a process for removing all Critical Security Parameters (CSPs) from a network element (ACC and DCC keys, Public/Private keys, options file).
  - Certificate revocation adds a certificate to the CRL, breaking trust between an entity and the rest of the network.
    - Network acquisition fails
    - Key distribution ceases to work
  - Operator-triggered key rolls, in combination with certificate revocation prevents network elements from decoding data.

FIPS 140-2 Compliance

- FIPS 140-2 Background
  - Federal Information Processing Standard (FIPS) Publication 140-2
  - Published by the National Institute of Standards and Technology (NIST).
  - Documents US Standard for Security Requirements for Cryptographic Modules
  - Four Increasing Levels of Security for Crypto Modules
  - Lab Testing and Agency Submittal to achieve Certification
- We have expanded our existing FIPS 140-2 certification from Level 2 to Level 3
  - Cloak module 1.0.2.0
  - Embedded in the 9 series remotes and DLC line cards
  - Features a strong physical measure for tamper prevention

A Best in Class Cybersecurity Solution

At Satellite 2019, iDirect Government was recognized as having the Top Cybersecurity Solution in 2019 by the Mobile Satellite Users Association (MSUA) for TRANSEC solution.

ST Engineering

Thank You