DOI 10.5162/ETTC2024/B3.3

ENCRYPTION OF PACKET TELEMETRY: A RISK ANALYSIS

Cédric Tavernier
Encryption Expert
Hensoldt France,
115 avenue de Dreux – 78370 Plaisir, FRANCE
cedric.tavernier@hensoldt.net

Jean-Guy Pierozak
Test Range Business Line Manager,
Hensoldt Nexeya France
Route d'Elne, 66200 Montescot, FRANCE
jean-guy.pierozak@hensoldt.fr

ABSTRACT

Telemetry systems are evolving from Continuous Streaming (IRIG106-CH4) to Packet Streaming (IRIG106-CH10, iNET, TmNS…), resulting in the latest version of IRIG106-CH7 mixing both. In Telemetry, packet streaming relies on UDP protocol which is unidirectional and allows some loss of packets. Besides, the need to secure the confidentiality of TM data is growing, leading to cipher part or all of it. We propose in this paper to start build a solution from a rigorous risk analysis. A description of state of the art solution compliant with the risk analysis results will be performed.

INTRODUCTION

Our telemetry system addresses the classical problem of protection the information transmission field: the main objective is to transmit securely some telemetry data through a radio channel.
We will deploy the Risk Analysis Scheme described in Figure 1, with the main following steps: Context Analysis, Fear Events Analysis, Scenarios of attacks, Risk Analysis and resulting Security Countermeasures.

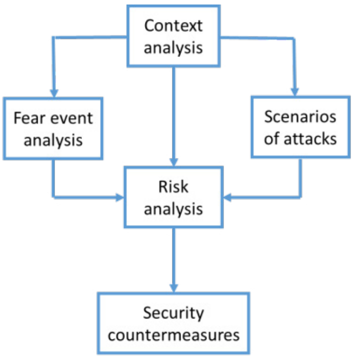


Figure 1: Risk Analysis Scheme

There exist a huge number of risk analysis model in practice. In order to be understood from the largest community, we recommend choosing a model compliant with the popular ISO 27005 [1].

1. CONTEXT ANALYSIS

As shown in Figure 1, the context of the operation is crucial. We consider an aircraft which is equipped of some sensors. During a mission the sensors data are gathered by a Data Acquisition System which transmits the telemetry data to some ground bases (Figure 2). The receiver is in charge of receiving the radio transmission, demodulating it, and encapsulate the data in UDP frames. Besides, the channel is unidirectional and noisy.

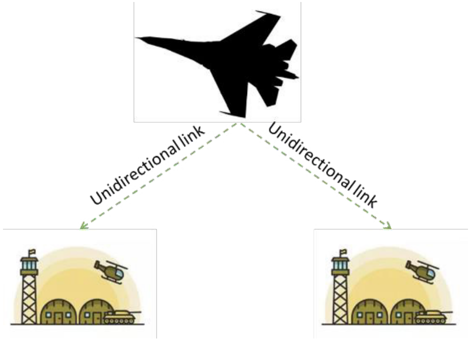


Figure 2: Operational Context

To collect the data, the decommutator is in charge of capturing a certain number of frames which could be stored in well denominated files.

At this stage, we can consider that the essential good is the telemetry data and the support goods are the transmitter, the receivers, the sensors/Data Acquisition System and the storage capacity of the different bases.

2. FEAR EVENT ANALYSIS

Confidentiality: The telemetry data are considered sensitive, thus breaking the confidentiality is a fear event.

Integrity: transmission of wrong, altered or transformed information compromises the interest of the mission, then, it is also a fear event.

Authenticity: the receiver must be sure to get the telemetry data from the right source, otherwise the mission is compromised: this a feared event.

Availability: A very noisy channel may cause a loss of information and may alter the interest of the mission, thus this is also a feared event.

3. SCENARIOS OF ATTACKS

Interception: an attacker may intercept the transmission and break the confidentiality.

Reordering packets: an attacker may intercept some packets and replay it. He can also reorder the packets before sending it to the receiver, and break consequently the integrity.

Attacks from the bases: if the data are not correctly protected, a cyber attack may compromise the telemetry data. If the storage is not protected, some passive or active attacks could compromise the data.

4. RISK ANALYSIS

It is clear that attacking the system inside the aircraft when flying in unlikely. The most likely attack can be over the air with jamming or simply interception. A cyber attack mean must be able to compromise the data in the bases itself, either in the aircraft, or in the data bases servers. On our opinion, the fear events are likely equally probable.

5. SECURITY COUNTERMEASURES

This brief risk analysis shows the need in term of security. We identify where the potential threats can act. Protecting the transport information is necessary but not enough because an attacker may intercept the telemetry data inside the data bases servers, or he could install a spy inside the aircraft when this one is parked at the airport of a base. We deduce that an applicative ciphering would be much more appropriate than a classical solution as VPN (virtual private network) encryption solution. However, we propose to analyse the potential solution by measuring the advantages and drawbacks.

- **VPN ANALYSIS**

Generally, VPN are bidirectional, especially IPsec VPN that works over TCP/IP. It is possible to implement the RFC 3948 and to encapsulate IPSec in UDP. Unfortunately, even in this case, the mandatory initial step consists in the handshake establishment that requires a bidirectional channel. This step allows a mutual authentication and the symmetric key secret sharing. To be compliant with our context, the handshake step (IKEV2) must be bypassed.

- **UDP FORWARDER**

The idea is to forward TCP/IP or UDP packets coming from a port toward another port and cipher the UDP frames in the middle. This method has the advantage not to require any bidirectional channel. Regarding the drawbacks, the UDP forwarder as the VPN only protect the transportation by building a ciphered tunnel, but outside the tunnel, data are not ciphered (clear text).

We deduce at this point that UDP forwarder is much more convenient because it aims to build a ciphered tunnel compliant the unidirectional link issue without requiring strong modification of any standard.

However, to protect the data form the source, to the destination and storage, these tunnel solutions must be associate with a ciphered storage:

- **FULL DISK ENCRYPTION**

For this technology, the disk is fully ciphered and the operating system manages to cipher the data coming from the interfaces and decipher data that come from disk and are directed toward the physical interfaces (hdmi, ethernet, serial,…). It is important to note that this technology do not warrant the integrity of the data. When the server is running, data are available in clear text.

- **FILE SYSTEM ENCRYPTION**

Only files containing the telemetry data are ciphered. It means that between the ciphered tunnel and the ciphered file, the data are in clear text. When the file is created, then only user with the correct key can read the file.
We deduce from these features, that the association between file system encryption and UDP forwarder is more appropriate. We must examine now the impact due to the noisy channel.

All frames must be ciphered using an IV (initial vector of 128 bits in general) which is transmitted in clear. If integrity is requested, then a tag (of 128 bits in general) must be also transmitted in clear. If any error appears on the IV, then the full frame could not be deciphered and shall be discarded. If an error appears on the tag, only the integrity guarantee shall be affected. We note that we cannot avoid this issue. Bypassing the IV means that a fixed word is ciphered in a unique manner: it makes the ciphered text not resilient against statistical attacks.

- **BLOCK CIPHER VS STREAM CYPHER**

We consider here a bloc cipher used with counter operation mode, then the only difference concerns the quantity of data lost. A bit error affects only one bit of a stream cipher whereas it affects a complete bloc (128 bits in general) for a bloc cipher. Regarding the IV and tag, there is no difference.

- **SYNCHRONOUS VS ASYNCHRONOUS**

Encryption can be synchronous or asynchronous. Synchronous cryptography is mostly used for data at rest, and also for digital signature. Asynchronous cryptography is usually used for data in transit and in cases where encryption and decryption keys need to be shared or exchanged.

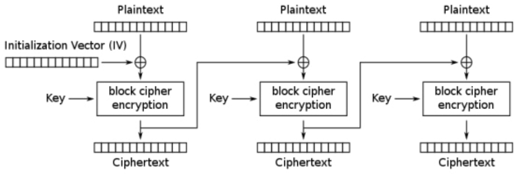
Synchronous ciphers have the advantage that key stream can be pre-computed before plaintext or ciphertext is provided, often with parallelism. They have the disadvantage of ciphertext malleability (a known change in ciphertext produces a known change in plaintext) and so will need to be combined with some form of message authentication. If a transmission is only received in part, in can be difficult to recover the fragment as the exact position in the key stream needs to be identified (synchronisation).

Asynchronous ciphers are largely serial in the encryption process (though not necessarily the decryption process) and the key stream can only be computed once the plaintext/ciphertext is provided. However, changing the ciphertext changes subsequent key stream and so there is considerably less malleability and a degree of message authentication. They also allow easy synchronisation at any point in transmission as the receiver can infer key stream after an initial run up of cipher bits (self-synchronisation).

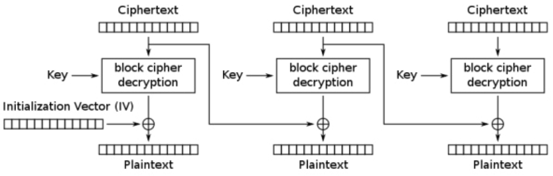
Hence, we deduce that according the context, an asynchronous cipher is recommended since it brings more resilience regarding the resynchronization. A lost of packet is dramatic for counter operation mode for example whereas it implies only a lost of two blocs for a chaining mode like CBC. We present as example an asynchronous operation mode that is suitable with our scenario.

We remind that a block cipher mode of operation is an algorithm that uses a block cipher to provide information security such as confidentiality or authenticity. A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block. A mode of operation describes how to repeatedly apply a cipher's single-block operation to securely transform amounts of data larger than a block.

In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector **IV** must be used in the first block.



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

The encryption corresponds in term of computation to:

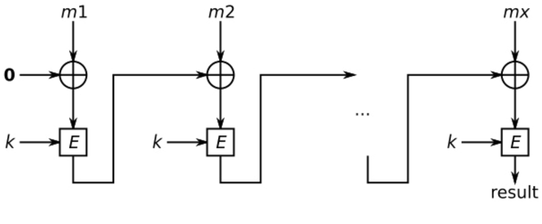
$$C_i = E_K(P_i \oplus C_{i-1}),$$
$$C_0 = IV,$$

The decryption corresponds to the following formulas:

$$P_i = D_K(C_i) \oplus C_{i-1},$$
$$C_0 = IV.$$

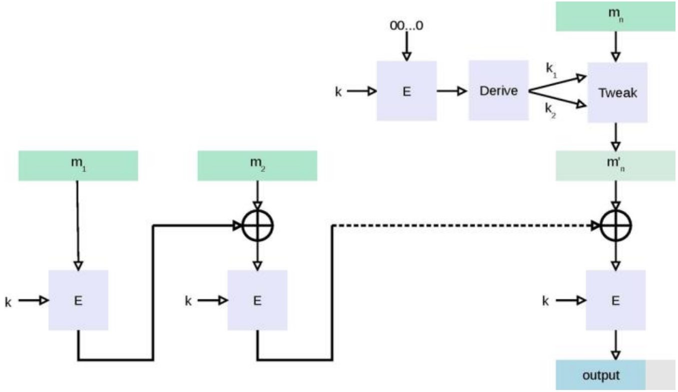
We not that the decryption formulas imply that in case of erroneous bloc, only two consecutive blocs are affected. This mode does not require any counter: even if a bloc disappears, the resynchronization is done after loosing one bloc maximum.

Regarding the integrity, the CBC-MAC provide this feature without involving much more calculation. To calculate the CBC-MAC of message m, one encrypts m in CBC mode with zero initialization vector and keeps the last block. The following figure sketches the computation of the CBC-MAC of a message comprising blocks m1||m2||…||mx using a secret key k and a block cipher E:



DOI 10.5162/ETTC2024/B3.3

CBC-MAC on its own is not secure for variable-length messages, but it can be slightly modified by using the standard One-key MAC (OMAC) which is a message authentication code constructed from a block cipher much like the CBC-MAC algorithm:



CONCLUSIONS

After deploying a Risk Analysis Scheme on the topic of cyphering the Packet Telemetry, we deduce at that UDP forwarder is much more convenient because it aims to build a ciphered tunnel compliant the unidirectional link issue without requiring strong modification of any standard.

Besides, the association between UDP forwarder and file system encryption is more appropriate.

About the impact due to the noisy channel: stream cyphering seems be more convenient, as a single bit error will affect a single bit of the ciphered stream but the use of IV may compromise the integrity of the complete frames and the synchronization may be an issue.

Finally, by studying the synchronous and asynchronous mode of ciphering we recommend using asynchronous chaining mode that brings a certain resilience in term of resynchronization, number of impacted packets in case of errors et integrity checking.

Our future work is to combine the need of segregating the Telemetry data depending on their security level, and the implementation of a ciphering solution compliant with this risk analysis.

REFERENCES

[1] ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management.” https://www.iso.org/standard/75281.html, 2018