OSMIUM
RESILIENT SOLUTIONS

gtd

i2cat

esa

Testbed for Bundle Protocol Security (BPSec)

Final Presentation

26/01/2024

Agenda & Objectives

1. Overview of the Project [5']
2. Recap of Core Concepts [10']
3. BP/BPSec Testbed [5']
4. Demonstration [40']
   a) Overall Setup [10']
   b) Configuration and Generated Files [10']
   c) BPSEC Tested Execution and Results [10']
   d) Q&A [10']
5. Project's Achievements and Next Steps [15']
6. Q&A about the Project [15']

Objectives of the FP

1. Show a summary of the work done during the project and its key outcomes
2. Demonstration of the SW developed during the project
3. Questions and answers about the project
4. Ideas for next steps

Overview of the Project: Partners Involved

OSMIUM RESILIENT SOLUTIONS

- Jorge Manuel Finochietto
- Alessandro Cammarano
- Pablo Madoery
- Renato Cherini
- Juan José Grosso (PM)

- Joan de Fuentes
- Ernest Cañamares (PM)

- Oriol Fuste Lara
- Joan Adrià Ruiz de Azua
- Carles Guillamón (PM)

Overview of the Project: Objectives and Results

OSMIUM

gtd i2cat

01

State-of-the-art

Analysis of existing IETF standards, and other state-of-the art resources, identification of problem areas and solutions

02

ESA BP

Definition of the scope of the BP using ESA's already implemented BPv7 and the relevant BP security specification

03

Requirements

Derivation of associated test cases scenarios and definition of the testbed system requirements

04

Testbed

Design, implementation and validation of the testbed architecture

05

BP + BPSEC

Implementation of the IEFT BP v7 and the relevant BP security specification

06

PoC

Definition and implementation of two proof of concept applications

07

Validation

Validation of the BP and BP security specification and interoperability testing with ION

08

Lessons Learnt

Findings and lessons learnt with recommendations for the standards and future systems implementing them

Overview of the Project: Key Issues Encountered

OSMIUM

gtd i2cat

01

Ambiguity

Ambiguity between RFC9172 and RFC9173 when authentication tag is appended to the ciphertext in the block-type-specific data field

02

Interoperability

ION BPSEC does not implement a default security policy of discarding BIB over extension blocks whose integrity is compromised

03

Interoperability

ION BPSEC implementation of RFC9173 is not available in open-source version (ITAR-free version)

04

End-to-end

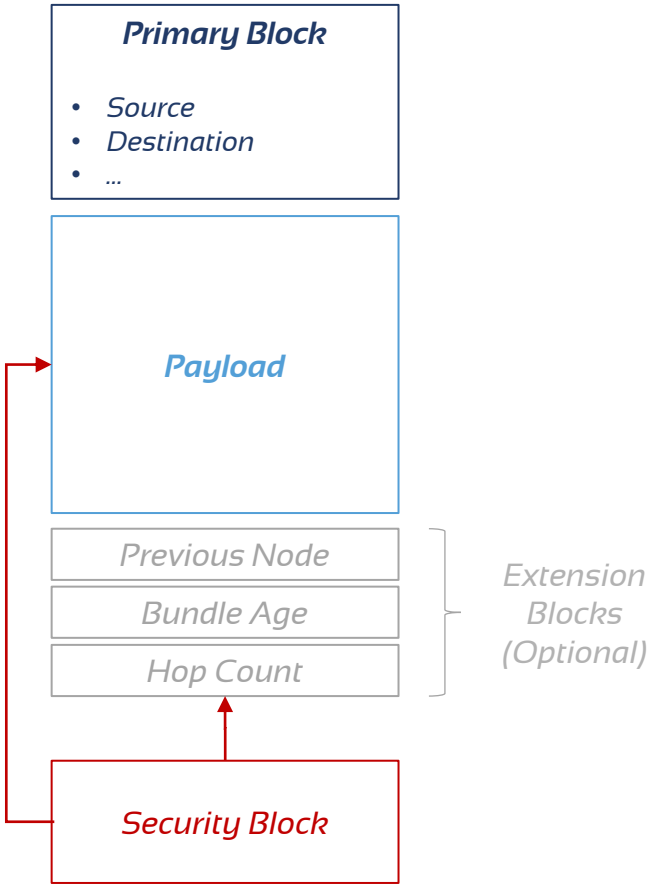
All three extension blocks defined in RFC9171 are designed to work on a hop-by-hop basis so end-to-end policies cannot be proposed

Recap of Core Concepts: Technical Context

- DTN has become a relevant paradigm for future space communication architectures, e.g., EO, Lunar, Mars
- Since 2007, the Bundle Protocol (**BPv6**) has been implemented in several platforms and experiments, e.g., JPL ION
- Security topics have been addressed with the introduction of BP Security Protocol (**BSP**) in 2011
  - A Streamlined Bundle Security Protocol (**SBSP**) has been developed and released in 2015
- Lessons learnt from BPv6 and (S)BSP resulted in IETF proposed standards released in 2022
  - Newer **BPv7** (IETF RFC 9171) which makes it simpler (encoding, structure, ids)
  - A Bundle Protocol Security (**BPSec**) scheme for BPv7 (IETF RFC 9172) based on extension blocks and roles
- CCSDS working on Red Books (draft recommended standards) for both BPv7 and BPSec

Recap of Core Concepts : BP and BPSec in a Nutshell

- BP relies upon the underlying transport protocols for communications, e.g., TCP, UDP
- BPv7 (RFC 9171) defines a "bundle" as a PDU consisting of individual blocks
- Traditionally, security protocols encapsulate the entire packet or its payload; however, BP transports multiple types of information (i.e., blocks), each of which may require different security operations
- Security operations in BPSec are implemented by augmentation instead of encapsulation: by the addition of extension blocks that target existing blocks in the bundle

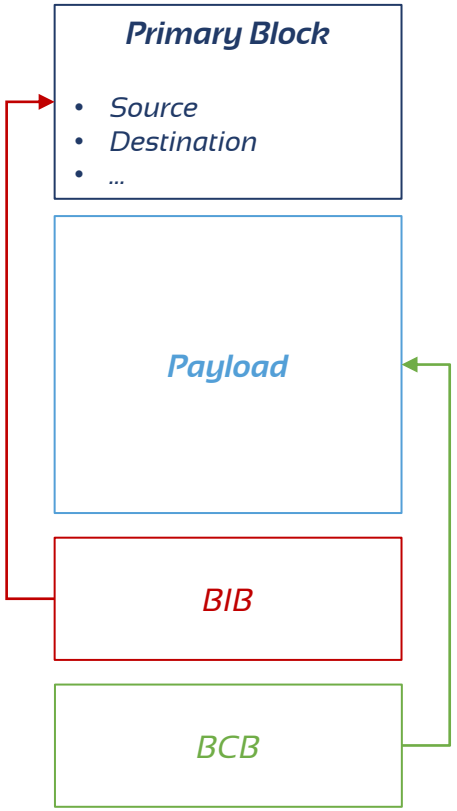


Recap of Core Concepts : Security Blocks & Roles

- BPSec provides 2 mechanisms/blocks for securing individual bundle blocks
  - Block Integrity Block (**BIB**)
  - Block Confidentiality Block (**BCB**), which also includes an integrity service

- BPSec defines 3 different roles for security operations which are assigned to a node when applying its security policy on a bundle
  - **Source**: adds security block (service) to a bundle
  - **Verifier**: checks security block (service) inside a bundle
  - **Acceptor**: terminates a security block (service) from a bundle

- Security policies definition is not part of BPSec; however, they need to be specified in a BPSec implementation as they are responsible of triggering actions that can mitigate security threats, e.g., block/bundle manipulation or injection

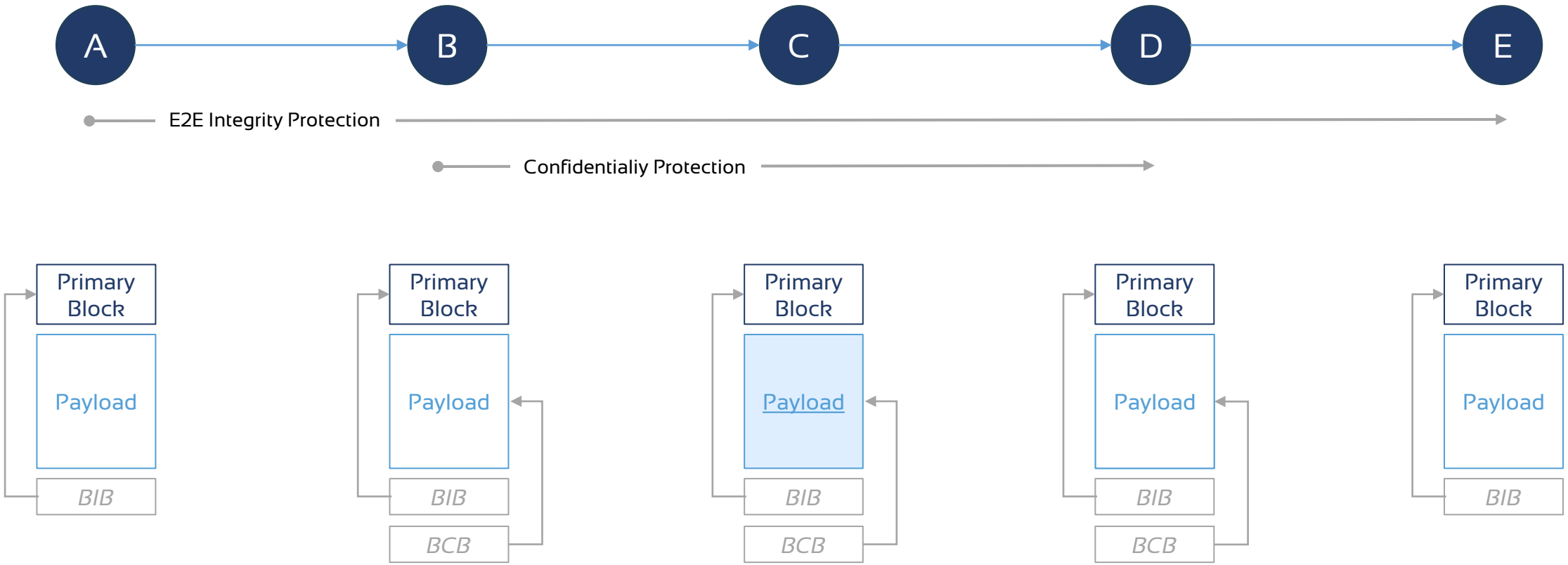


Recap of Core Concepts: Security Policies

- A **security policy** is determined by a sequence of security policy rules
  - Rules are **executed sequentially**
  - A rule may **keep** the bundle as it is, **modify** it or even **discard** it
  - Rules operate on the resulting bundle from the previous one
  - The first rule takes as input the original bundle, as received or transmitted.

- A rule is comprised of three parts
  - **Condition**: is a boolean predicate determining if the rule's specification is going to be executed or not
  - **Specification**: defines the role to play with the bundle, the involved security operation, and, implicitly, possible modifications to the bundle.
  - **Outcome**: maps each possible failure event resulting from the specification execution to actions to be taken

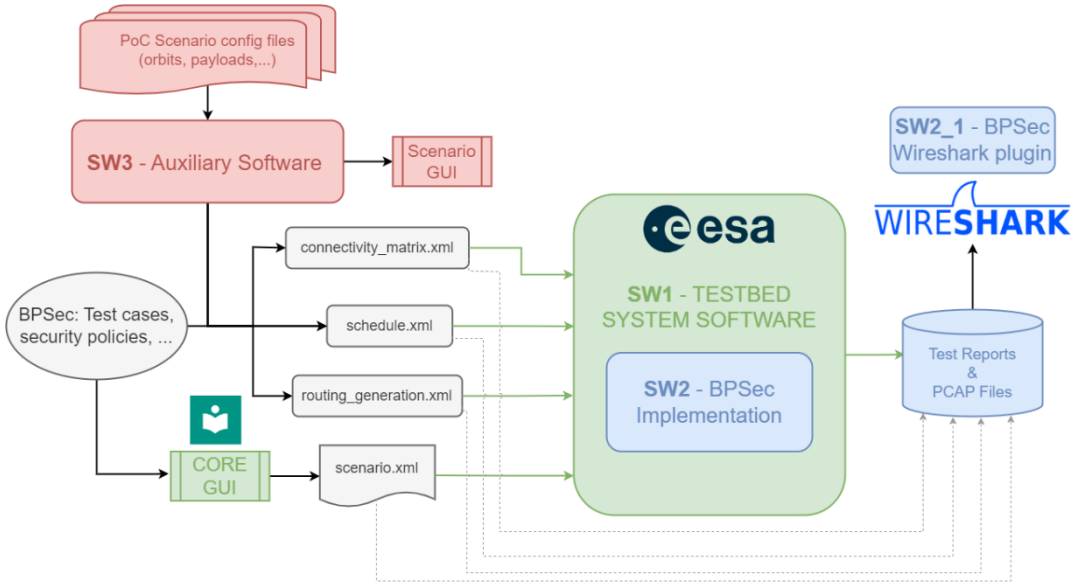
Recap of Core Concepts: A Simple Example



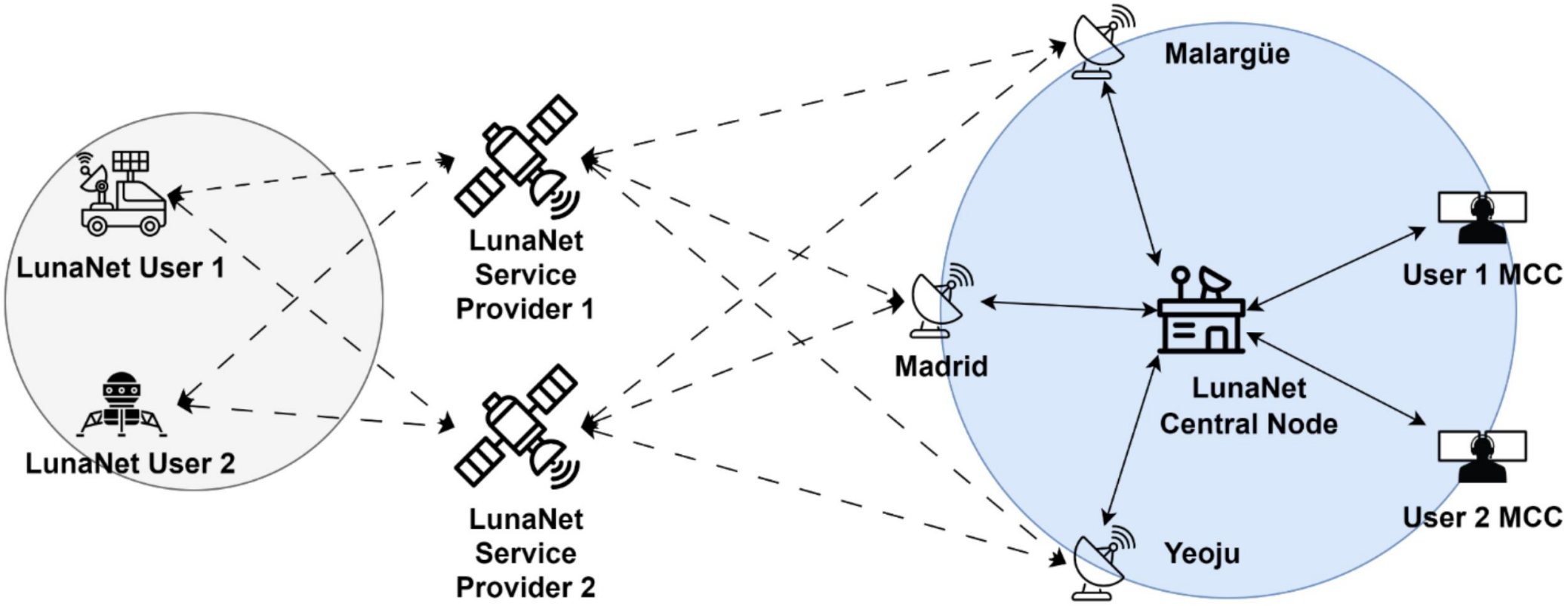
BP/BPSec Testbed: System in a Nutshell

The BPSec testbed allows to:

- Define of permanent or scheduled communication links (using **Linux network namespaces**),
- Characterize transmission delay and data loss (using **Linux Netem** queuing disciplines),
- Define of **BPSec security policies** to mitigate threats,
- Analyse online/offline the traffic, security events and logs,
- Configure in a user-friendly manner the scenarios using CORE (Common Open Research Emulator) architecture (used also in JPL ION).

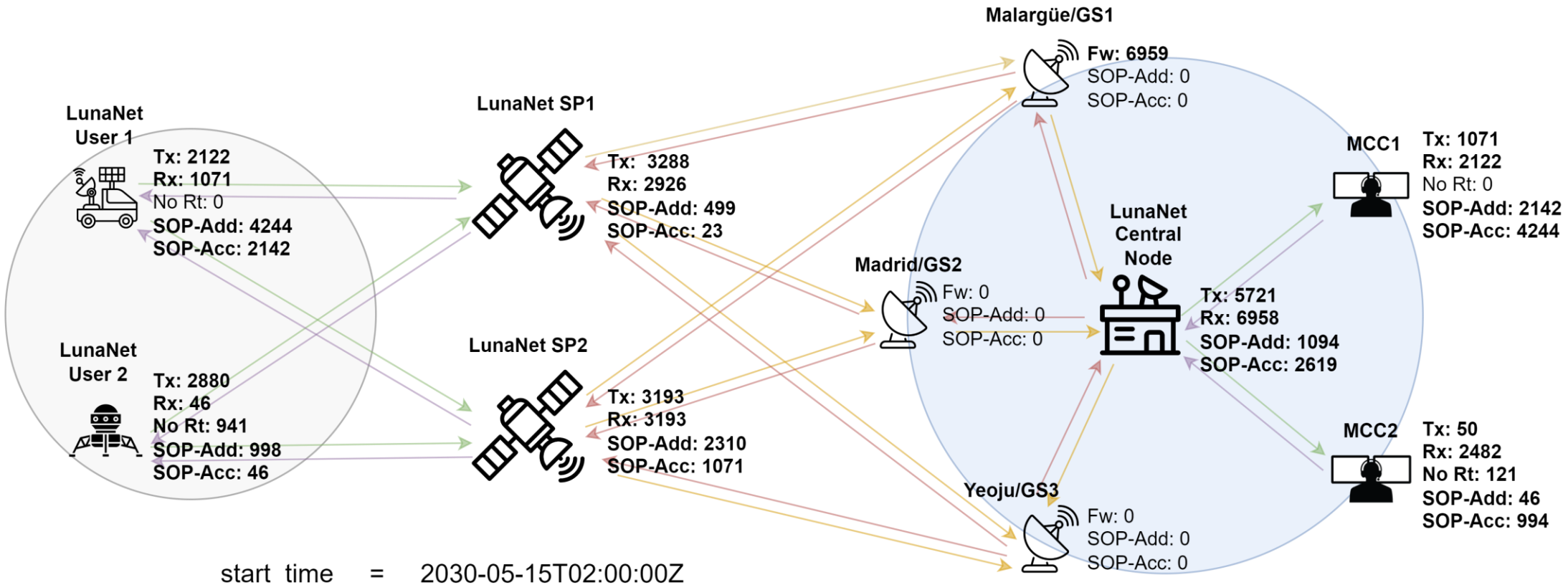


Demonstration: BPSEC Scenario Topology



Live Demo

Demonstration: BPSEC Tested Execution and Results



start_time = 2030-05-15T02:00:00Z
end_time = 2030-05-15T06:00:00Z

Demonstration: Q&A

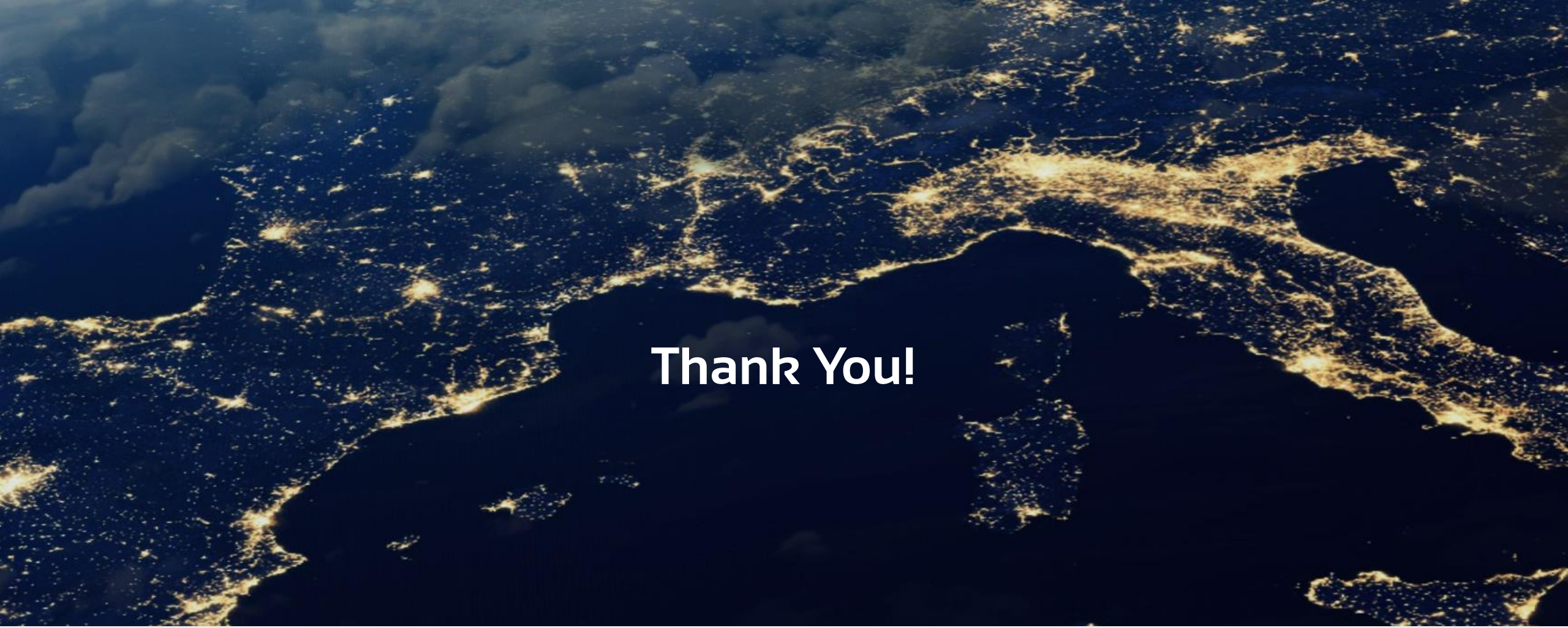
Project's Achievements and Next Steps

Achievements

- **Comprehensive** analysis of BPSec for securing space missions was conducted (analysing IETF, CCSDS, scientific papers and books).
- **Assessment** of **BPSec capabilities** to deal with **common threats**, including data interception, data manipulation, masquerading, and replay attacks.
- **Introduction** a method to address the absence of **formalized security policies** in BPSec specification by means of security rules.
- **Development** of a **flexible testbed** to simulate **BP/BPSec-**enabled delay tolerant networks.
- **Analysis** of testbed behaviour and functioning over two **PoC applications.**
- Paper presented at the **2023 IEEE International Conference on Wireless for Space and Extreme Environments** (WiSEE 2023).

What's next?

- **Extend** the **expressiveness** of **security policy definition**, e.g., including sub-rules, adding break commands, ..
- Further **analyse** the **impact** of **routing dynamics** on the **security policies** and **vice versa**, e.g., security policies might limit the flexibility of the routing by forcing to use a given path or differently key management would have a huge impact to allow communication to happen on any possible route, impact of fragmentation on policies, etc..
- Investigate the application of BPSec in **heterogeneous networks** where multiple service providers are involved, e.g., security policy configuration for multi domain case, key management (what if a key is compromised, how long it take to update it), ..



Thank You!

OSMIUM
RESILIENT SOLUTIONS

https://osmium.solutions

https://tinyurl.com/osmiumsolutions

Osmium Solutions Spain SL
CIF: B67579763

Osmium Italy SRL
P. IVA: 12914450015