Secure Delay Tolerant Networking Using SBSP and IPMEIR

Enabling Security, Resiliency, and Cost Savings for Space Mission Communications

Presented by: Assi Friedman

Authored by:

Assi Friedman – Innoflight, Inc.

Dr. Edward J. Birrane - UMB County Cyber Defense Laboratory

Innoflight, Inc
9985 Pacific Heights Blvd
Suite 250
San Diego, CA 92121
www.innoflight.com
TeL: (858)638-1580
Fax: (858)638-1581

Introduction

- Innoflight is working with NASA to develop and demonstrate *Secure Delay Tolerant Networking* using NASA's SCaN Testbed
- SCaN Testbed is an advanced communications platform installed on the International Space Station (ISS)
  - Managed out of the NASA Glen Research Center
  - http://spaceflightsystems.grc.nasa.gov/SOPO/SCO/SCaNTestbed/
- Innoflight develops packet/network-based cryptographic solutions for space communications
- Innoflight is teamed with long time DTN subject matter expert Dr. Edward Birrane on the effort

Streamlined Bundle Security Protocol

IETF

Internet Protocol Security (IPsec) Minimum Essential Interoperability Requirements

IPMEIR

Suite-B

Motivation

- Why consider Secure DTN?
  - [$↓] Budget uncertainties ongoing across the board
  - [$↑] Ground stations and dedicated telecom services are expensive to maintain
    - [% ↑] More importantly: the ratio of spacecraft to ground resources is increasing
  - [bps↑] Missions generate ever increasing amount of data
  - [!] Proprietary information must be protected
- *CONCLUSION: We must devise new approaches to reliably and securely move data from the spacecraft to the mission owners.*

The Solution – Global Collaboration

- Share resources, but how?
  - Ground Stations: If a dish isn’t actively tracking, it’s a wasted resource. Why not support other missions?
  - Space Based Systems: Store and forward, SATCOM, etc.
  - Ground Networks: Public connectivity plentiful and cheap, but Quality of Service is limited (throughput, uptime).
- *Cyber Security* is paramount to enabling DoD, govt, commercial and international partners to collaborate
- **Overall goal is to provide data confidentiality and integrity to both the link and data packages:**
  - **S-BSP: Secures the Data Bundle**
  - **IPMEIR: Secures the Communications Medium**

DTN in a Nutshell

- DTN is a "package delivery service"
- Data is packaged into a "bundle"
- Bundle is sent off to its destination via intermediate couriers
- Only that in the case of DTN it's not a single carrier: Spacecraft -> Store & Forward Spacecraft -> Partner Ground Station -> Mission Operations Center
- *Cyber Security:*
  - *How am I securing my package? -> S-BSP*
  - *How am I securing my carriers? -> IPMEIR*

Advantages to DTN

- **Delay** or **Disruption** tolerance is the key strength of DTN
- No need for a real time link between the source to destination
  - Bundle can transit from node to node until arriving at its final destination
- Path can be negotiated based on cost and resource availability
  - Facility and manpower cost savings
- Eventually, it gets there…
  - Based on the actual path, it can take seconds to weeks
- Not surprisingly, DTN saw its first use on deep space missions
- Secure DTN very relevant to contested and congested communications environments

Security Model - IPMEIR

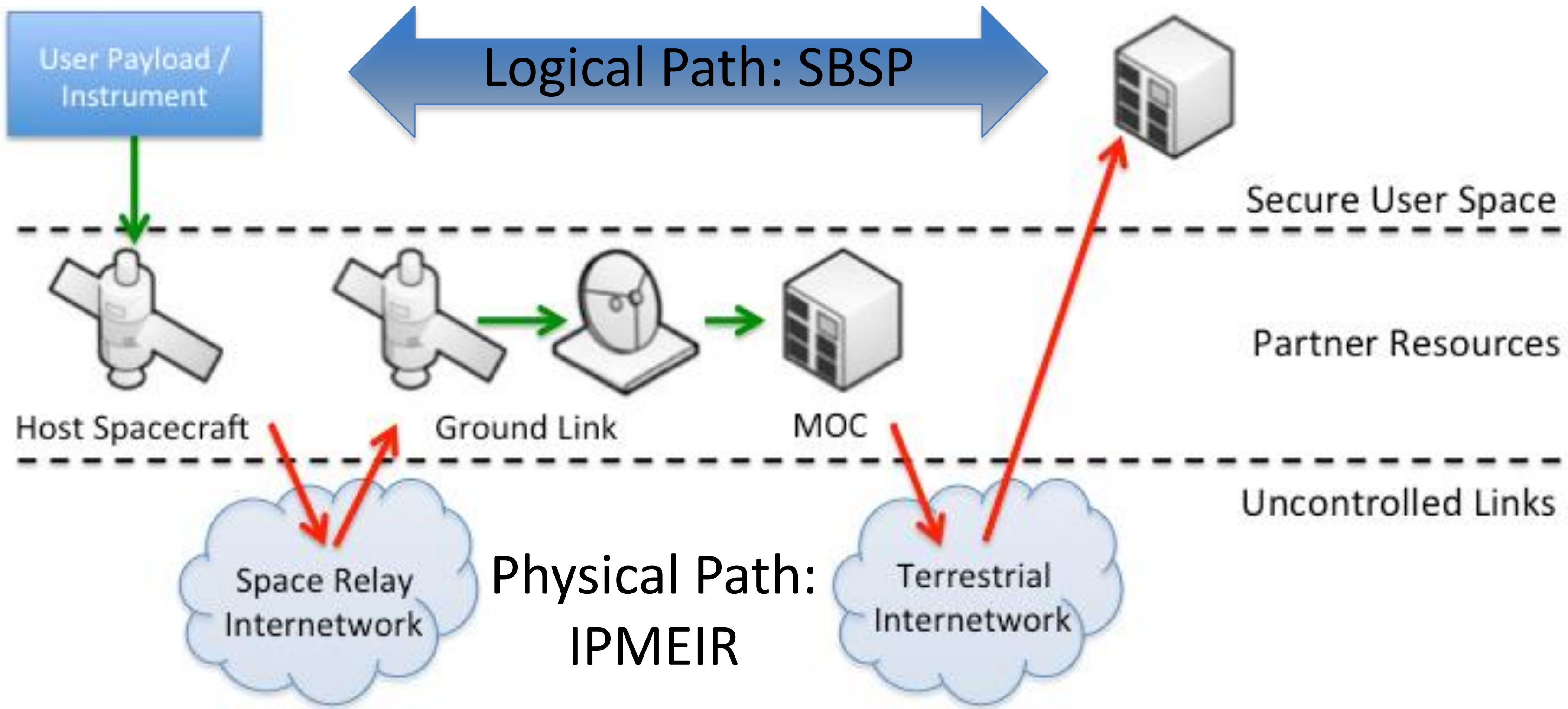
- IPMEIR 1.0.2
  - **I**nternet **P**rotocol security (IPsec) **M**inimum **E**ssential **I**nteroperability **R**equirements
  - NSA created specification in 2010 based on a specific security profile of IPsec and Suite-B ciphersuite
  - Specification publically available at:
    - https://www.nsa.gov/ia/_files/IPMEIR_IS_1.0.1.pdf
- Why IPMEIR?
  - Can be implemented by anyone; proper implementation provides high assurance of confidentiality and integrity
  - Leverage COTS systems and open source implementations
- Benefits:
  - Create secure communications enclaves
  - Know who you're talking to (with key/certificate management in place)
  - Prevent indirect attack vectors
  - Makes sure the bundle arrives to its intended recipient

Security Model – SBSP

- Delay Tolerant Networking
  - Formalized by RFC-5050
  - Establishes the framework for bundle creation and bundle delivery
- Bundle Security Protocol (BSP)
  - Formalized by RFC-6257
  - Establishes a framework for bundle security
- Secure Bundle Security Protocol (SBSP)
  - Improvement and simplification on BSP
  - Adoption of Suite-B ciphersuite

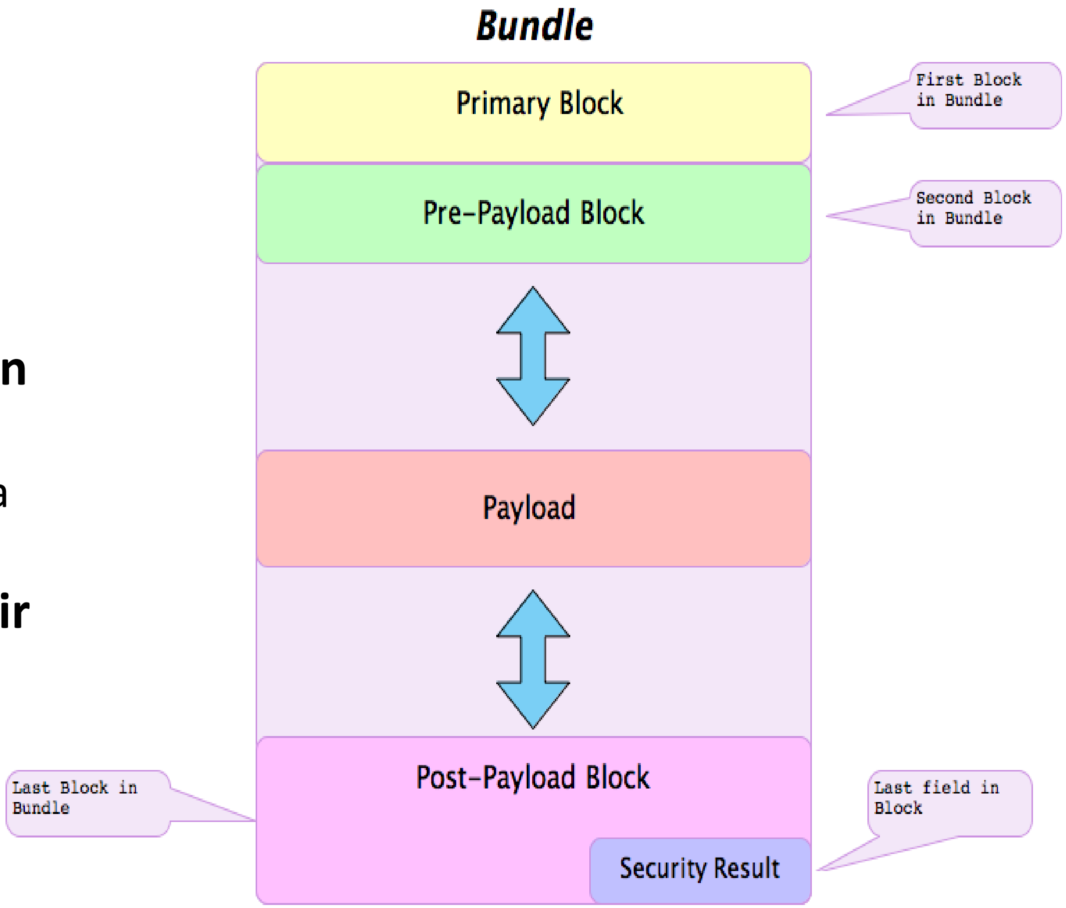
End To End Security – A Layered Model

Securing logical paths through a challenged network is done at the application layer. Data units carry their security with them.



The Bundle Protocol Data Unit

- **Bundle Comprised of Blocks**
  - Order is important
  - First block is the header
  - Single payload block
  - Everything else an "extension block"
- **During Processing, Blocks Kept in Data Structures**
  - For transmit/receipt, bundle is a serialized bitstream.
- **Extension Blocks Each Have Their Own Lifecycle**
  - They are processed independently of each other



The Bundle Protocol (RFC5050) is being standardized within the IETF to address multi-path, multi-hop packetized communication in a variety of challenged environments.

Streamlined Bundle Security Protocol

SBSP being considered by the IETF for a deployable security model for DTNs running the Bundle Protocol. SBSP differs from BSP in 6 fundamental ways:

1. **Decoupled routing/security functions**
   - No security-specific destinations
2. **Minimum number of security blocks**
   - Fewer, more general block types defined than in BSP
   - Block authentication, Block Integrity, Block Confidentiality
3. **Minimum number of security operations**
   - One security operation per bundle
   - An operation is the application of a security service to a security target
     - ENCRYPT(payload), ENCRYPT(header), SIGN(payload), etc…
4. **Deterministic block processing order**
5. **Common block processing**
   - No special rules for payload blocks in a bundle
6. **Simplified rules for fragmentation**

https://tools.ietf.org/html/draft-birrane-dtn-sbsp-00

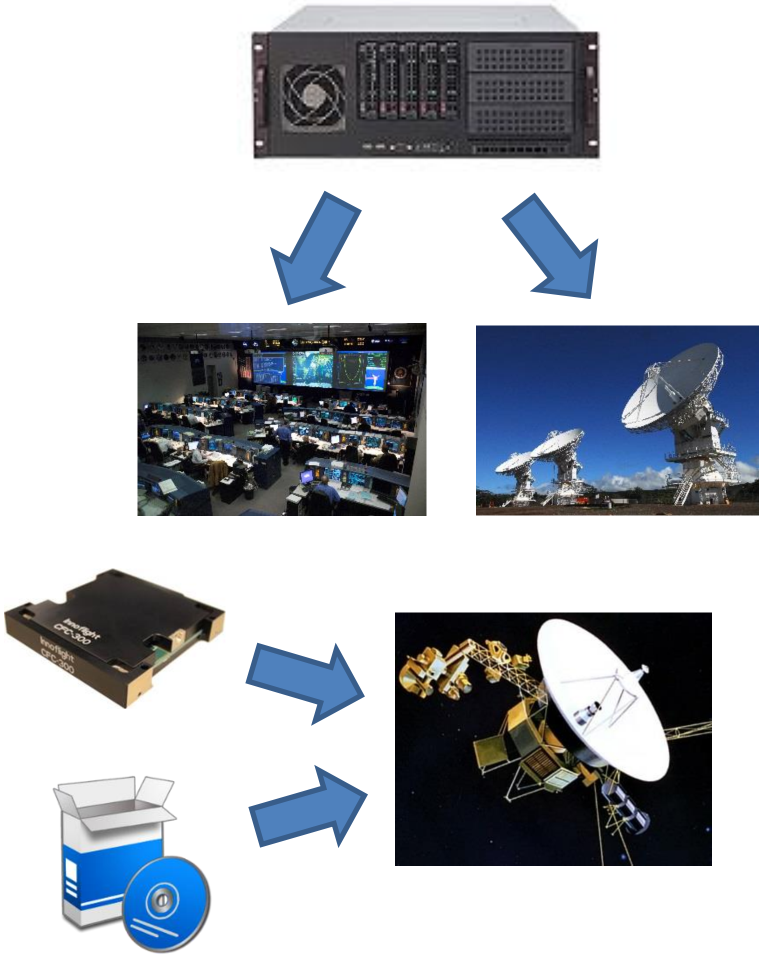
SBSP Key Capabilities

- **Three security block types instead of four**
  - Bundle Authentication Block (BAB), Block Confidentiality Block (BCB), Block Integrity Block (BIB)
- **Concept of "security operation" as (service, target)**
  - (integrity, payload), (confidentiality, payload)
  - Only 1 unique instance of an operation in a bundle
- **Extension blocks treated same as payloads**
  - Extension block no longer replaced by security block
  - Support for integrity of extension blocks
    - (integrity, extension_block_1), (integrity, extension_block_2)
  - Support for primary block integrity
    - (integrity, primary_block)
- **Goal: Backwards compatible with BSP for simple cases**
  - "Simple" cases capture most deployments today.

SBSP provides equivalent security to BSP with significantly less development complexity.

Initial Implementation & Deployment

- Currently working on *Linux* and *VxWorks* code bases
- Ground Appliance
  - IPMeir + SBSP Linux implementation
  - Target: Mission operations, ground stations, etc.
- Spacecraft
  - VxWorks implementation for demonstration on the Scan Testbed
  - Target 1: Security subsystem
  - Target 2: Software for main computer



Summary

- Communications Innovations Enabled by Secure DTN:
  - Provide a high grade Information Assurance (IA) framework for protection of sensitive information
    - DoD/Govt applications include protection of classified information
  - IPMEIR provides link protection with the features of IPsec (security associations, key management)
    - High assurance programs can upgrade from IPMEIR to HAIPE
  - SBSP/DTN provides end to end data protection
  - Allows programs to utilize more affordable means to get data from the space segment to the end user
  - Allows DoD/Civil applications to leverage commercial, public, and partner communications resources

Secure DTN: Multi Layered Security, Communications Resiliency, Operational Cost Savings

Questions?

- Contact information:

  Assi Friedman

  Email: afriedman@Innoflight.com

  Telephone: (858) 638-1580 extension 163

THE BEST THING ABOUT DELAY-TOLERANT NETWORKING - IS THAT EVERYONE GETS IT, EVENTUALLY ☺

network-therapy.com

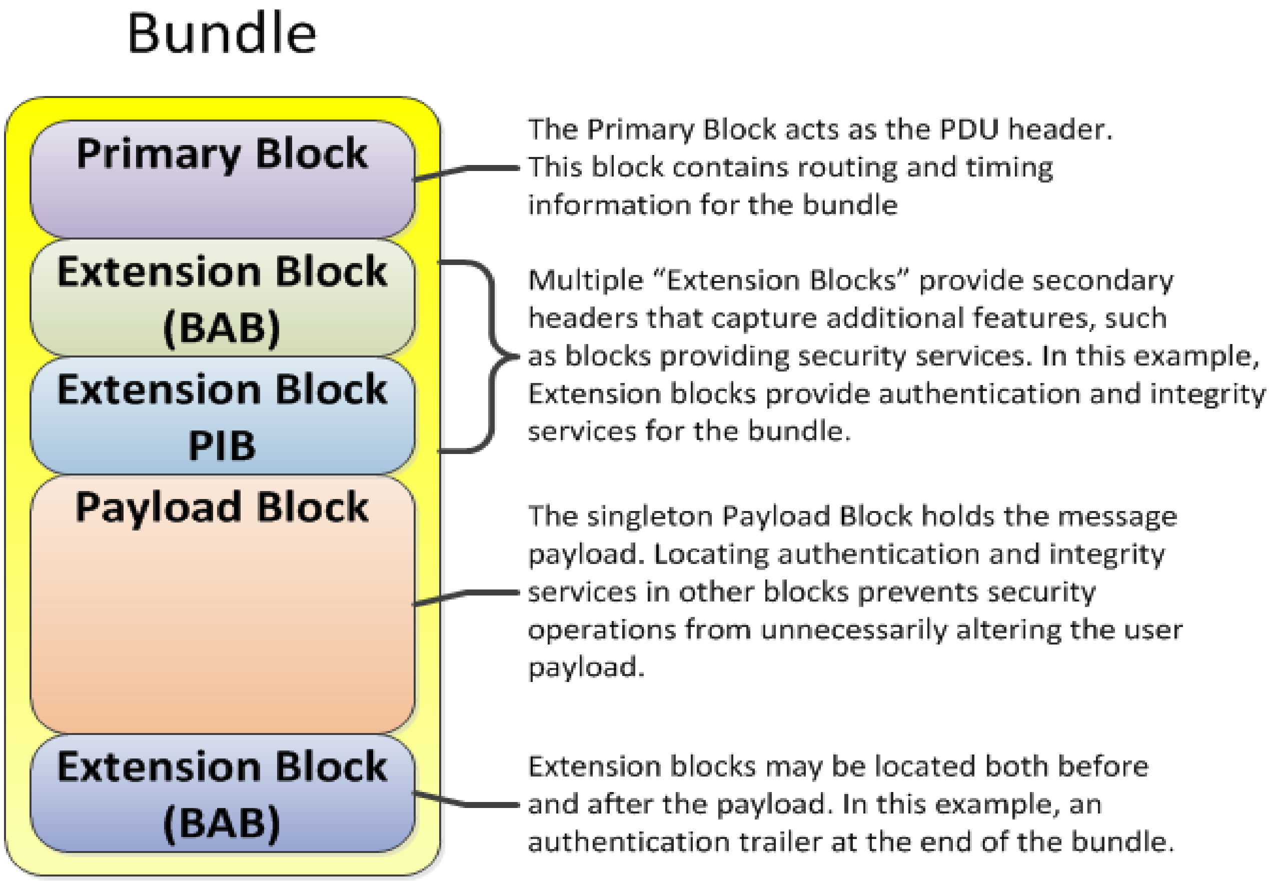
DTN Experimental Security Standard

- **Experimental Specification Provided in May, 2011**
  - MITRE, Trinity College, SPARTA
  - Reference implementations by NASA, Laboratory for Telecommunication Sciences
- **Defines 4 Extension Blocks (BAB, PIB, PCB, ECB)**
  - *Bundle Authentication*: Covers entire bundle
  - *Payload Integrity*: Integrity signature of payload-related blocks
  - *Payload Confidentiality:* Crypto-text of other payload-related blocks.
  - *Extension Security*: Security for non-payload-related blocks.
- **May Have Multiple Blocks For a Single Service**
  - Often a pre-payload block working with a post-payload block.
  - Example: Bundle Authentication of a large bundle
- **Ciphersuites Populate Blocks**
  - BSP blocks contain ciphersuite identifiers and associated information.
  - Bundle agents expected to support multiple ciphersuites.
- **Protocol Does Not Address Management Issues**
  - Key management is an open problem.
  - Security policy enforcement and configuration is an open area.

An experimental security standard, the Bundle Security Protocol (RFC6257) first applies application security concepts to RFC5050 Bundles.

The BSP Security Mechanism

- **One “Block Type” for each security service**
  - Strategically placed in the “Bundle” to implement security
  - Defines “blocks” for authentication, integrity, confidentiality



Bundle

The Primary Block acts as the PDU header. This block contains routing and timing information for the bundle

Multiple “Extension Blocks” provide secondary headers that capture additional features, such as blocks providing security services. In this example, Extension blocks provide authentication and integrity services for the bundle.

The singleton Payload Block holds the message payload. Locating authentication and integrity services in other blocks prevents security operations from unnecessarily altering the user payload.

Extension blocks may be located both before and after the payload. In this example, an authentication trailer at the end of the bundle.

The BSP uses Bundle Protocol extension mechanisms to capture security primitives.