Streamlined Bundle Security Protocol (SBSP) Discussion

History, Recommendations Implementation, Status, and Todo

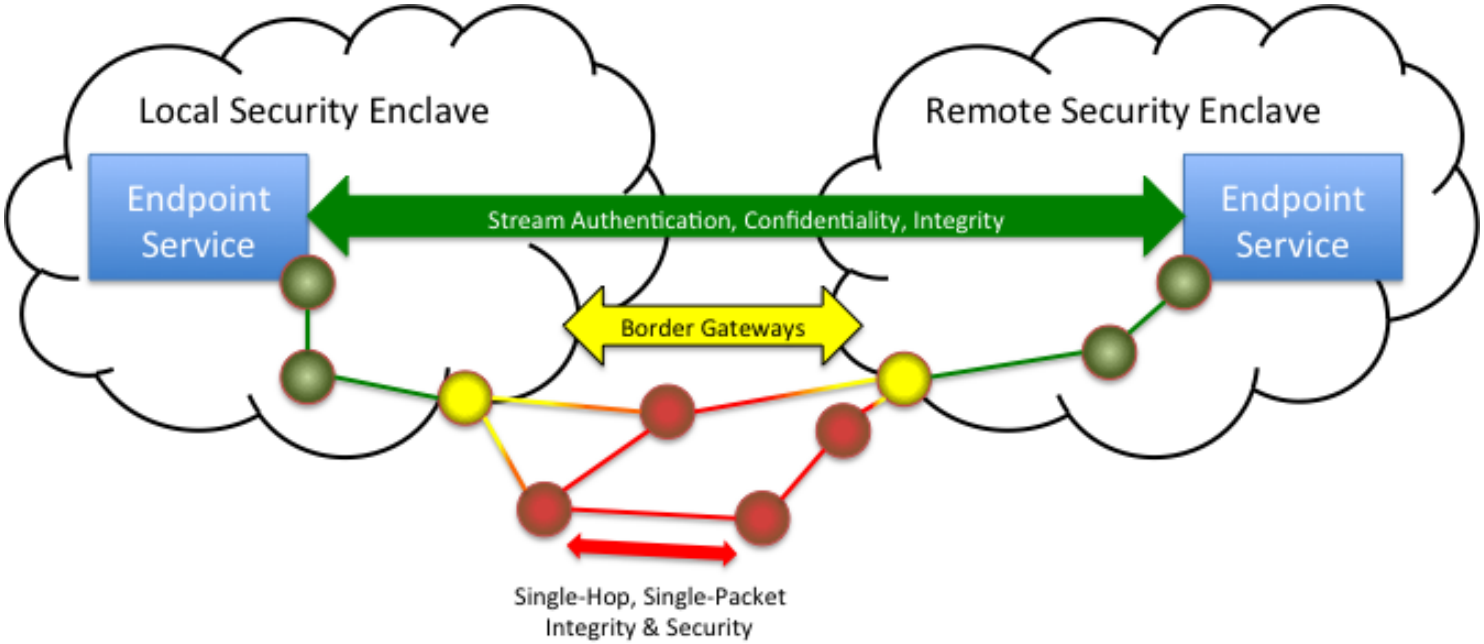
Ed Birrane

March 26, 2015

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Motivation: Security Challenges Differ at Each Layer

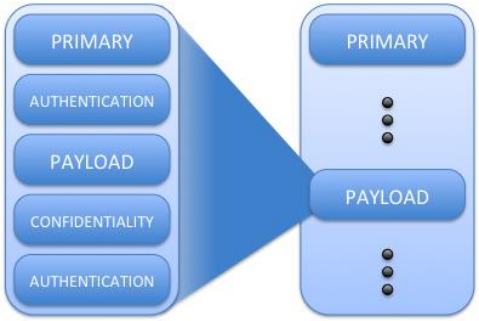
Security in an internetwork must be addresses at every communication layer.



- **Link-layer security is not sufficient for this model**
  - **Impractical to coordinate link layers across administrative domains**
  - **Shared links carry differentiated data from multiple communities**
    - **One security standard or policy for a shared link is not enough**

Motivation: Desirable Properties

- **Atomic Services**
  - Each bundle must support three atomic security services
    - Authentication, Integrity, Confidentiality
- **Cascading Operation Support**
  - Atomic services may need to be applied multiple times
    - Security block “recursion” was an issue in RFC 6257 (BSP)
    - Encapsulation may provide a less risky approach
  - Levies dependencies between bundles and blocks in bundles.
  - Typically only needed for a subset of the network. (super encryption)
- **Encapsulation**
  - Put bundle(s) into another bundle
    - Novel way to support cascades
    - “New” bundle may have own endpoints
    - Takes “recursion” out of the bundle



History: DTN Experimental Security Standard

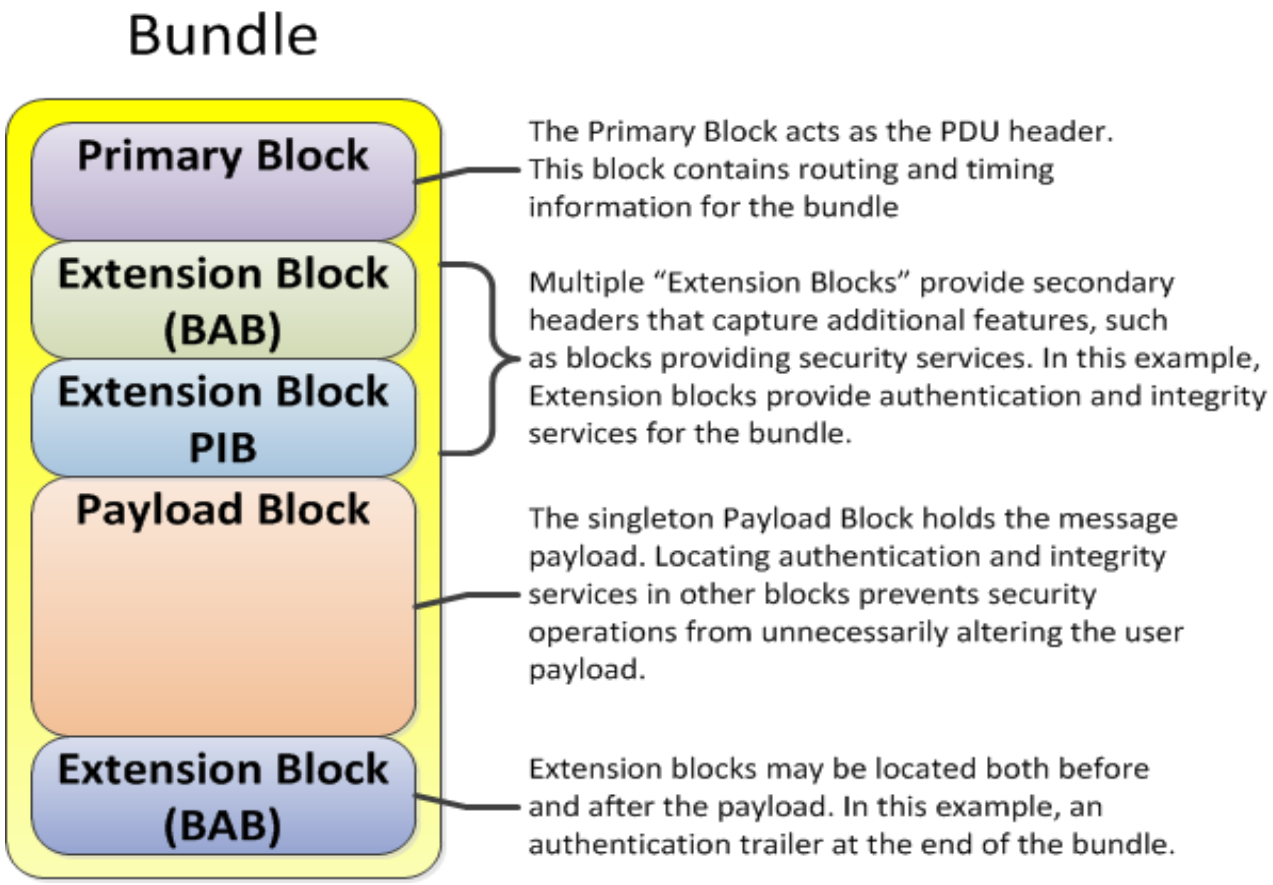
An experimental security standard, the Bundle Security Protocol (RFC6257) first applies application security concepts to RFC5050 Bundles.

- **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.

History: The BSP Security Mechanism

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

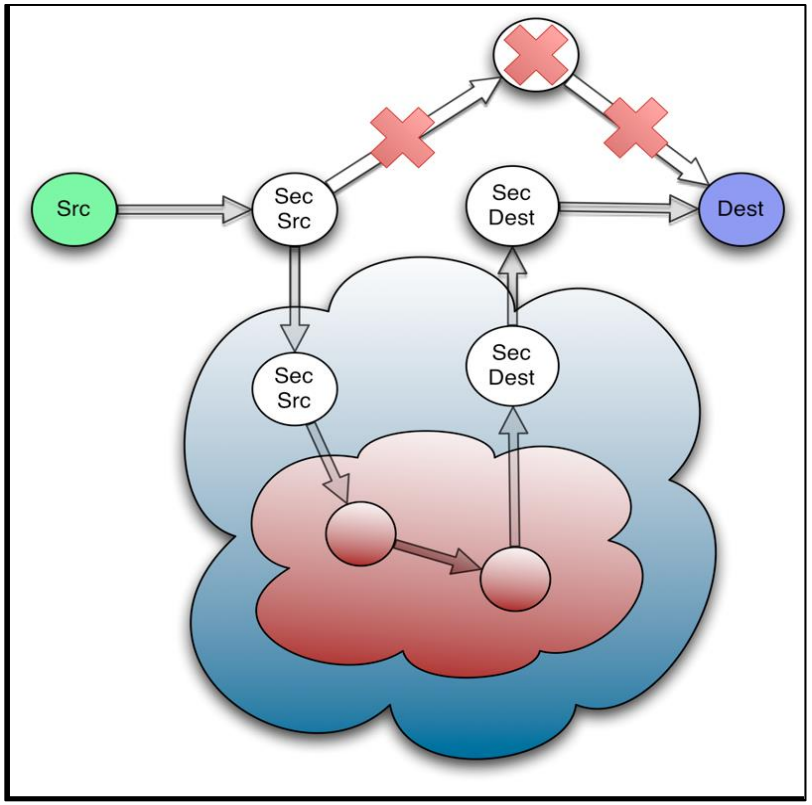
- **One "Block Type" for each security service**
  - **Strategically placed in the "Bundle" to implement security.**
  - **Defines "blocks" for authentication, integrity, confidentiality**



History: BSP Coupled Routing and Security

Each security block has a security source and destination

- **Layered Security**
  - Security-sources may differ from the bundle source.
  - Security-destinations may differ from the bundle destination.
- **Caveats**
  - Up to the security-aware node to ensure there are no conflicts amongst all security-destinations in all security blocks in the bundle.
  - **Cannot reach the bundle destination before reaching all necessary security-destinations.**



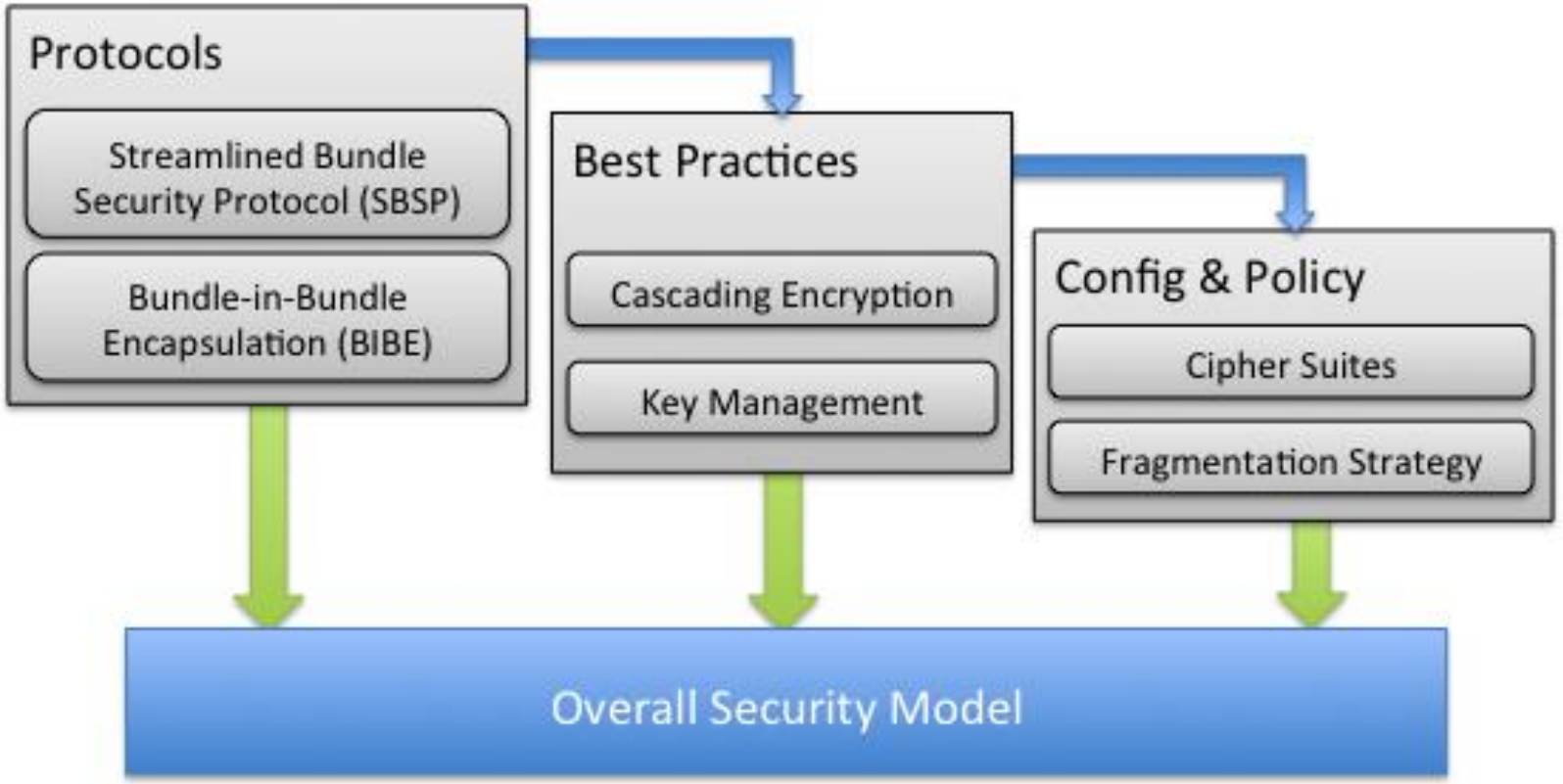
Recommendations: Lessons Learned from the BSP

Experience implementing RFC6257 helps us form a deployable end-to-end security model.

- **Decouple routing and security functions**
  - **BSP defined "security sources" and "security destinations"**
    - **Identifies "gateways" in the network, tricky to implement. Possible to specify unsatisfiable sequence of security destinations, especially in ad-hoc networks**
- **Make common cases simple and efficient**
  - **Restrict recursive nesting of security operations**
- **Secure all block types equally, no special rules for payload**
- **Fragmentation must be addressed more completely**
- **Decouple protocol, policy, and configuration**
  - **BSP specifies all three in one specification, making a change in one area require an update of the spec, or causing implementations to lose conformance**
  - **Policy and configuration likely differ between space and terrestrial networks**

Recommendations: Decompose Security Documents

Our model is a combination of three categories of information working together to secure challenged internetworks.



Implementation: SBSP Key Capabilities

- **Decouple Security/Routing**
  - **Significant refactoring around security-specific destinations**
- **3 security block types, not 4**
  - **Bundle Authentication Block (BAB), Block Confidentiality Block (BCB), Block Integrity Block (BIB)**
  - **Deterministic block processing order.**
- **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)**
- **Simplified rules for fragmentation**
- **Goal: Backwards compatible with BSP for simple cases**

Todo: Likely Updates to SBSP

SBSP proposed to DTNWG from DTNRG. Some changes pending.

- **An extension block identification scheme**
  - RFC5050 does not uniquely identify extension blocks.
  - SBSP has a ~~creative solution~~ hack to identify blocks using dictionary offsets.
  - An RFC5050bis would address this and SBSP must be updated accordingly.
- **Updated authentication flags**
  - What happens when a bundle goes through a waypoint that doesn't understand BSP?
  - Restrictive authentication: drop the bundle
  - Permissive authentication: drop the block
- **Some clarifications on fragmentation from mailing list**
- **Review block nesting restrictions**
  - Unlike BSP, SBSP places restrictions on nested security
  - Need to review order: restrict BIB(BCB) or BCB(BIB)

Todo: Ciphersuite Definitions

- **Symmetric key ciphersuites**
  - Based on HMAC-SHA256, AES
- **Suite-B Ciphersuites**
  - Initial work done by Angela Hennesey – update for SBSP
- **Support for multiple parallel authenticators**
  - Security multi-cast
  - SBSP does not allow multiple blocks for the same function
    - If you want 3 potential integrity signatures, you can't add three BIBs to the bundle.
    - Recommendation is support multiple signatures in one block
- **Define Security Compatibility profiles**
  - Do not require all implementations to support all ciphersuites

Todo: Policy Considerations

Less Security than Required	When the network requires a certain level of security, such as encrypted payloads or authenticated message exchange and a message is received without this information, the network must handle this in a uniform way. Most policies require not forwarding the message, but the level of logging, error messaging, and updates to local configurations should be discussed as a matter of policy.
More Security then Required	Similarly, when messages are received that contain authentication, integrity, or confidentiality when they should not, a decision must be made as to whether these services will be honored by the network.
Security Evaluation in Transit	Some security services may be evaluated at a node, even when the node is not the bundle destination or a security destination. For example, a node may choose to validate an integrity signature of a bundle block. If an integrity check fails to validate, the intermediate node may choose to ignore the error, remove the offending block, or remove the entire bundle.
Fragmentation	Policy must determine how security blocks are distributed amongst the new bundle fragments, so as to allow received fragments to be validated at downstream nodes.
Block and Bundle Severability	Distinct from fragmentation, nodes must decide whether a security error associated with a block implies a larger security error associated with the bundle. If blocks and bundles are considered severable, then an offending block may be omitted from the bundle. Otherwise, a bundle should be discarded whenever any of its constituent blocks are discarded.

Todo: Best Practices

Security Capability	Description
Basic Security Services	Best practices must describe how to implement the basic security services of authentication, integrity, and confidentiality in the context of a given networking architecture.
Primary Block Privacy	The primary header of a message contains significant information relating to sources, destinations, timestamps, and other processing flags that may need to be hidden in parts of a shared internetwork.
Primary Block Integrity	Authenticating a message ensures that it was not altered in transit between two nodes. However, if a node is compromised, hop-by-hop authentication will not capture malicious changes made at the node. End-to-end integrity mechanisms accomplish this, but typically cannot protect the primary header in a message. Best practices discuss how to integrity sign immutable portions of a primary header.
Cascading Operations	The cascade of basic security services must be addressed by best practices. These operations occur when multiple security operations are performed on the same data, such as the case with super-encryption.
Intermediate Destinations	Often used with cascading operations, an intermediate destination levies a requirement that a bundle be routed through a particular node on its way to a destination. The intermediate destination typically represents some waypoint associated with security operations, such as the endpoint of a security tunnel.
Path Verification	A common request in a secured internetwork is to provide a signed listing of each node traversed by a bundle on its way from sender to receiver. In addition to representing an example of a cascading integrity operation, policies and mechanisms for how this information is collected and representing in the bundle should be addressed in any best practices document.
Multicast Parallel Authenticators	Security in the context of multicasting presents challenging operational concepts for how to validate a received bundle that carries multiple integrity signatures. In any network supporting secure multicast, best practices must address mechanisms and policies as they would apply to parallel authenticators.