Bundle Protocol Security (BPsec)

Scott Burleigh, IPNSIG

Security

- *Security* in data transmission supports three features as needed:
  - Confidentiality. The sender and receiver of data may need assurance that the data that has been communicated was not divulged to any hostile third party.
  - Integrity. The sender and receiver of data may need assurance that the data that has been communicated was not altered by any hostile third party. (A cyclic redundance check (CRC) can indicate that the data was not altered, but a hostile agent might have altered the data and additionally computed a new CRC to which the altered data conforms.)
  - Authenticity. The receiver of data may need assurance that the asserted sender of the data was the actual sender.
- Security is enabled by the use of secret *keys* that are required in order to compute authenticating signatures and/or to encrypt and decrypt confidential data.

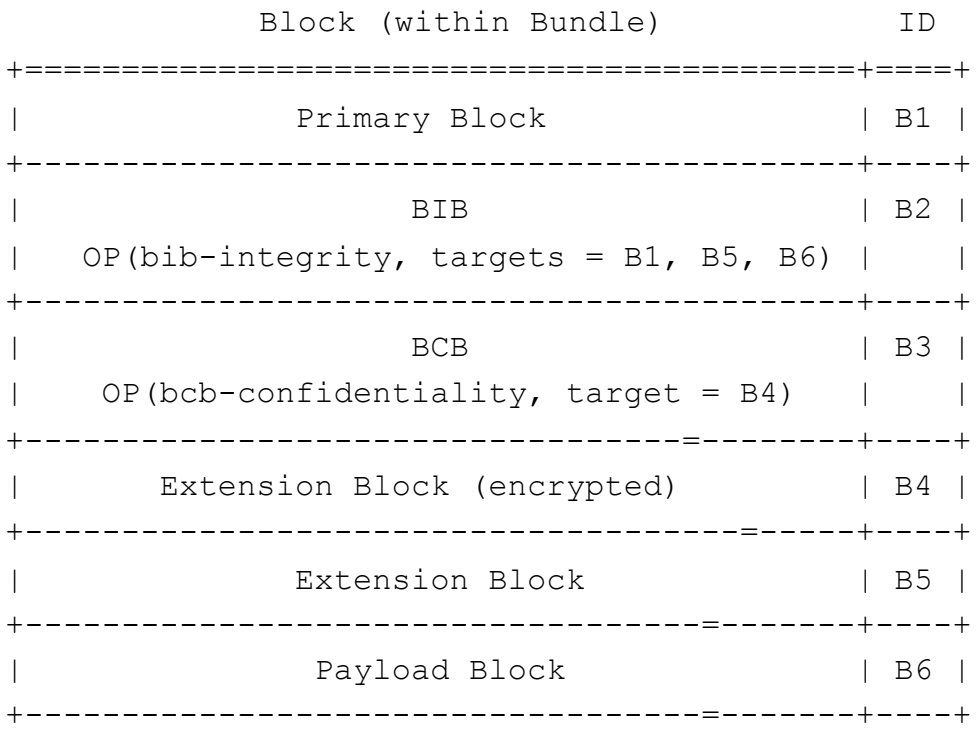
Security in the Internet

- Several protocols are commonly used in the Internet to provide security:
  - IPsec: an additional layer of protocol is applied to Internet Protocol (IP) packets, inserting Authentication Headers (AH) or Encapsulating Security Payload (ESP) headers in front of packet data.
  - TLS: an additional layer of encapsulation, providing integrity, confidentiality, and authentication, is applied to the protocol data units of transport-layer protocols such as TCP.
- These protocols work well in the Internet, but:
  - They introduce additional protocol stack layers, requiring establishment of security associations between senders and receivers, and the same security procedures are applied to all traffic subject to those associations.
  - Security associations must be established and configured by connection handshakes between senders and receivers. Over an end-to-end path spanning high-latency links, these handshakes might take so long that the communication opportunity has ended before secure transmission can begin.

Security in Bundle Protocol

- BPsec is a standardized extension of bundle protocol itself, not an additional layer of protocol. This means that:
  - Security parameters are carried internally in each bundle. No durable security association connections are needed.
  - Each bundle individually may be protected by different security measures.
  - A given bundle's security measures remain in effect even while the bundle resides in storage, waiting for an outbound transmission opportunity.
- BPsec protection is established by the insertion of BPsec extension blocks into the bundles:
  - Block confidentiality blocks (BCBs) contain information needed in order to decrypt other blocks (including the payload block) that have been encrypted.
  - Block integrity blocks (BIBs) contain cryptographic (key-based) signatures enabling verification of that other blocks have not been altered.
  - A BIB signature targeting the primary block guarantees sender authenticity.

An Example



Every BPsec extension block has one or more *targets* – the other blocks in the same bundle that it is protecting.

Here the BIB in block 2 of the bundle contains a signature computed over blocks 1, 5, and 6 (primary block, one other extension block, and the payload block). The BCB in block 3 of the bundle contains information needed to decrypt block 4, an extension block that required confidentiality.

Keys (1 of 2)

- All of these security procedures rely on the availability of secret keys, numeric values that are used to encrypt and decrypt blocks and to compute cryptographic signatures.
- Many familiar network security methods are based on symmetric cryptography, where the same key value is known to both the sender and receiver of data.
  - Simple and rapid computation.
  - But the key can be compromised by an adversary who may discover the sender's copy, the receiver's copy, or an interim copy created when the key was replicated between the two.
  - Protection of all copies of the key requires management of each shared secret, which can itself be compromised unless done very carefully.
  - That careful management incurs costs, limiting the scalability of security based on symmetric cryptography.

Keys (2 of 2)

- An alternative is asymmetric cryptography, where a pair of different but computationally related – private and public – keys are used.
  - A signature computed using the sender's secret private key can be verified by any receiver that knows the sender's corresponding public key.
  - A data item encrypted in the receiver's public key can only be decrypted by the intended receiver using its secret private key.
  - Computation is more complex and much slower.
  - But disclosure of public keys to adversaries is harmless, and the corresponding private keys can only be compromised by compromising their sole owners.
  - So no shared secret management is necessary. Security based on asymmetric cryptography scales without limit.
- Methods of supporting and utilizing asymmetric cryptography in DTN have been proposed but are not yet standardized.