Key Distribution for Delay Tolerant Networks

Cherita Corbett, Angela Dalton
Johns Hopkins University Applied Physics Laboratory
Laurel, MD
cherita.corbett@jhuapl.edu, angela.dalton@jhuapl.edu

The Bundle Security Protocol (BSP) [1] provides data integrity and confidentiality services for the Delay Tolerant Networking (DTN) Bundle Protocol (BP) [2]. BSP requires keys for encrypting and signature verification of bundles. However, the BSP specification does not address and explicitly excludes the key management process from the security protocol specification. Without key management, keys must be manually pre-placed on all DTN nodes needing to secure bundles. This work seeks to provide a mechanism for distributing X.509 public key certificates to alleviate the need for pre-placement.

This poster presents an experimental key distribution mechanism we have developed for DTN2. DTN2 [3] is an open-source reference implementation of the DTN bundle protocol. We assume that each node has its own private key and corresponding public key certificate. When a DTN node is missing the public key certificate needed to encrypt or verify a bundle, the bundle is queued while the node sends a "Key Query Bundle" requesting the missing certificate from the owner. The node with the certificate responds with a "Key Response Bundle." Intermediate nodes along the path traversed by the response bundle can cache the certificate locally. This will allow intermediate nodes to respond to future queries for the same certificate, thereby reducing delay at the requesting node. Our implementation is integrated into the bundle protocol agent (BPA) and uses the bundle protocol itself to transport the queries and responses. The key query and response process is transparent to the user. The BPA will detect when a certificate is missing and initiate a query. The BPA of the node that receives the query will automatically send a response containing the certificate if it has it. A live demonstration of this feature will be presented using Android Nexus S smartphones.

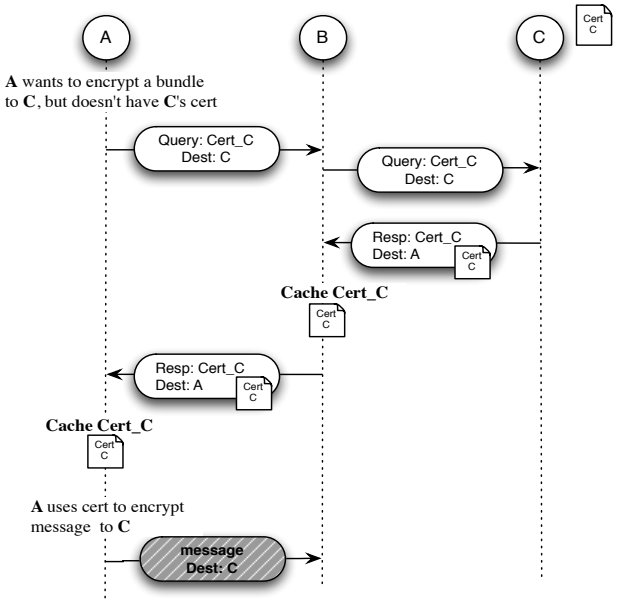

Figure 1. Message exchange for key distribution

Future work will investigate an out-of-band channel that does not use the bundle protocol transport to query neighbors for certificates.

[1] S., Farrell, S., Weiss, H., and Lovell, P., "Bundle Security Protocol Specification", RFC 6257, May 2011
[2] Scott, K. and S. Burleigh, "Bundle Protocol Specification", RFC 5050, November 2007
[3] DTN2, http://www.dtnrg.org/wiki/Code