DTN Security Key Management

IETF93 - July 22, 2015

Fred L. Templin

Fred.l.Templin@boeing.com

DTN Security Key Management

DTN nodes observe the Streamlined Bundle Security Protocol (SBSP)

SBSP requires a public key distribution system

All DTN nodes must subscribe to the public key distribution service

https://datatracker.ietf.org/doc/draft-templin-dtnskmreq/

Public Key Distribution Alternatives

- Request-Response
  - Online Certificate Status Protocol (OCSP)
  - Not delay tolerant
- Publish-Subscribe
  - Receiver informs Trusted Authority of interest in specific keys
  - Trusted Authority informs receiver if keys are revoked
  - Receiver has no way of knowing whether new keys are valid on first use
- Blacklist Broadcast
  - Trusted authority broadcasts list of all revoked certificates
- Whitelist Broadcast
  - Trusted authority broadcasts list of all valid certificates

Whitelist Broadcast

- Requires reliable DTN multicast
- Requires that receivers trust a secured trust authority
- Receivers need assurance that the trust authority has not been compromised
- Answer – multiple trust authorities each multicast portions of the whitelist bulletin

DTN Security Key Management Requirements

REQ1: Must Provide Keys When Needed

REQ2: Must Be Trustworthy

REQ3: No Single Point of Failure

REQ4: Multiple Points of Authority

REQ5: No Veto

REQ6: Must Bind Public Key with DTN Node Identity

REQ7: Must Support Secure Bootstrapping of a Node's Identity and its Public Key

REQ8: Must Support Revocation

REQ9: Revocations Must Be Delay Tolerant

DTN Security Key Management Design

- DC1: Must Perform Timely Key Provisioning
- DC2: Pub/Sub Model
- DC3: Publication Must Be Spread Over Multiple KAs
- DC4: Availability and Security

Limitations and Challenges

- Requires scalable, reliable multicast
  - DTN multicast reliable (hop-by-hop rather than end-to-end retransmission)
  - Scalability not an issue for many DTNs
- Key Authorities must be protected against physical attacks (must be kept in secured facilities)
- Scaling can be accommodated by organizing Key Authorities in confederations, where each confederation services a portion of the DTN
- Scaling of public key whitelist itself must be considered. May not work well with millions of keys