GRE for DOTS Transport

Evaluating the alternatives to UDP

IETF 95
Buenos Aries, AR
April 8, 2016

Robert Moskowitz
HTT Consulting

draft-moskowitz-dots-gre-01.txt

Topics

- Networking issues
- P2P vs RESTful
- Security Context and Fate sharing
- Transport alternatives
- Discuss

The Network issues faced by DOTS

- Messaging during the worst time
- UDP filtering at upstream ISPs may interfere with DOTS over UDP
  - Double-edged effect, in lessening the impact of an attack, but interfere with UDP-based signaling.

DOTS needs P2P, Not RESTful

- DOTS servers independently message DOTS clients
  - “The Attack Seems Over”
- How to provide peer communications within REST
  - Two messaging channels?
  - Unsolicited Responses?
- How to recover/restore state if either agent reboots?

Security Context and Fate Sharing

- DOTS cannot afford computational costs of secure data objects
  - e.g. PEM and DSRC (IEEE 1609.2)
- Secure communications trades this cost with that of maintaining security state.
  - Security state fate-shares with communications state
    - ESP, TLS/DTLS
- Greater fate-sharing = more rigid security context > larger attack surface.

Designing for DOTS

- Select a communication that is
  - Bi-directional (either agent can start)
  - Not commonly blocked during DDoS attack
  - Minimal data over-the-wire to fit into a single MTU
  - Support peer communications
  - Secure with minimal fate-sharing

Designing for DOTS

- Consider
  - ESP in Transport mode
  - GRE Tunneling
  - GRE compressed
  - UDP with message level security

DISCUSSION