ATOCA Protocol Drafts
draft-barnes-atoca-*

Richard Barnes
Matt Lepinski
Karen Seo
-cap-mime

• It’s a MIME type for CAP
-escape (ESCAPE)

• S/MIME wrapper around CAP
• Two security mechanisms
  – Hash pre-images
  – Digital signatures
• Provisioning of public keys and hash values handled via AMP
-meta (AMP)

- Discovery via DHCP (RFC 5986) + NAPTR
- JSON over HTTP / WebSockets
- Set of message types:
  - C->S: contact info, location
  - S->C: alert sources, certs/pubkeys, hash values
-delivery (LEAP)

<table>
<thead>
<tr>
<th>alert-id</th>
<th>frag-count</th>
<th>frag-no</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Fragment Body</th>
</tr>
</thead>
</table>

- Simple fragmentation for ESCAPE over UDP
- Receiver does buffered reassembly
  - Time-outs to mitigate DOS
- Retransmit to get reliability
Questions

• Is this generally the right set of mechanisms?
• Do the individual protocols have roughly the right shape?
• Adopt as WG item: -meta —> “Discovering alert servers”?
Possibly Adopt in the Future

- cap-mime —> *new milestone* “A MIME media type for CAP”
- escape —> *new milestone* “Secure alert format for alert distribution”
- delivery —> *collapsed milestone* “Lightweight conveyance of authority to citizen alerts”