FirstMILE security alerts

Automating the alerts into MILE

IETF 95
Buenos Aries, AR
April 5, 2016
Robert Moskowitz
HTT Consulting

draft-moskowitz-firstmile-00.txt
What is the problem?

• No standard input of security alerts/reports into the MILE environment
  – Currently a collection of proprietary management systems and cut and paste into MILE

• Reporting security events may occur at times where the networks is under attack
  – See draft-ietf-dots-requirements-01.txt
What is needed

• A sub/pub reporting system
  – A security monitor subscribes to a security defense system for selected reports
  – The security defense system publishes events to all subscribed monitors

• But first needs a registration of defense system to monitor(s)
  – Support business model of ISP security monitor(s)
  – Establish trust between defense and monitor systems
Why does firstMILE use SSLS

• Same arguments as for DOTS
  – SSE moves the security context within the messaging, reducing the attack surface
  – Though does not need the bi-directionality that DOTS requires
    • But Subscribe process may be viewed as adding bi-directional
Why does firstMILE use SSLS

- If Sub process uses NETCONF
  - Use Chunking to packetize structure XML
  - Use Compression to reduce chunks
  - Same as I2RS

Key Management

Detect Outage + Best Transport

Compression (GPComp)

Chunk Data

Secure Session Envelope (SSE)

Fragment/Re-assembly

API
Compare to mile-xmpp-grid

• Mile-xmpp-grid is more extensive

• But
  – Use of TCP and TLS does not reflect the network conditions during an attack

• FirstMILE can be a communication service for mile-xmpp-grid to use
  – SSLS provides the transport uncoupling and message layer security desired.

• Xmpp can be the sub/pub function used
Next steps

• Either
  – Develop registration and sub/pub in firstMILE
  Or
  – Work with mile-xmpp-grid to merge documents
DISCUSSION