draft-bellis-geopriv-flow-identity-00

Ray Bellis
Nominet UK
GeoPriv @ IETF83
Intro

• HELD Identity Extensions (RFC 6155) has `<udpport>` and `<tcppport>` elements
  – DCCP and SCTP variants too
• My idea, based on UK ES work
• Identify a target based on a flow it produced
• Necessary if the target is behind a NAT
• It turns out to insufficient...
CGNs

• On a CGN the same source IP and port can be part of more than one flow, hiding more than one device

• Reversing the NAT mapping needs all of:
  – <layer 3 protocol>, i.e. IPv4 vs IPv6
  – <layer 4 protocol>, i.e. TCP vs UDP, DCCP, ...
  – <src ip, src_port>
  – <dst ip, dst_port>
New Proposal

• A Flow Identity Extension:

```xml
<flow xmlns="urn:ietf:params:xml:ns:geopriv:held:flow"
      layer4="tcp" layer3="ipv4">
  <src>
    <address>192.168.1.1</address>
    <port>1024</port>
  </src>
  <dst>
    <address>10.0.0.1</address>
    <port>80</port>
  </dst>
</flow>
```
Schema Details

• Uses attributes of the `<flow>` element to specify the Layer 3 and Layer 4 protocols

• Considered re-using the RFC 6155 elements, but couldn’t prevent mixing up a `<udpport>` on one end with a `<tcpport>` on the other
  – Likewise for IPv4 vs IPv6
Issues

• I’m not an XML geek – is it extensible enough?
• Can we adopt, and push through quickly?
  – It’s currently a short doc
  – It needs maybe a page more text
Questions?