Threats to GEOPRIV Location Objects

draft-barnes-geopriv-lo-sec-00

IETF 69, Chicago, IL, USA
Background

- L7LCP Requirements document had an ad-hoc discussion of threats to the LO communicated over that channel
- This document takes that section as a start for a systematic study of threats to an LO over its entire “life cycle”
  - What bad things can happen to an LO?
  - When can these things happen?
- This document just discusses threat, not countermeasures
What’s in an LO?

• LO encodes bindings between data elements

• Sighting bindings: (ID, Location, Time)  
  “An entity with this identifier was at this location at this time”

• Rule bindings: (Tuple, Rule)  
  “These are the rules for how this sighting should be handled”
Sighting Binding

<?xml version="1.0" encoding="UTF-8"?>
     entity="pres:meaningless-F32AC8D@example.com">
    <tuple id="sg89ae">
        <status>
            <gp:geopriv>
                <gp:location-info>
                    <gml:location>
                        <gml:Point gml:id="point1" srsName="epsg:4326">
                        </gml:Point>
                    </gml:location>
                </gp:location-info>
                <gp:usage-rules>
                    <gp:retransmission-allowed>no</gp:retransmission-allowed>
                </gp:usage-rules>
            </gp:geopriv>
        </status>
        <contact>sip:geotarget@example.com</contact>
        <timestamp>2003-06-22T20:57:29Z</timestamp>
    </tuple>
</pres>
Integrity and authenticity

- High-level Threat: Corruption / falsification of bindings
- Sighting bindings
  - Location and time: Replay
  - Location and identity: Spoofing / swapping
  - Levels of identity: Swapping between layers
- Rule bindings: Removal of rules
Confidentiality

- Unauthorized disclosure of a location object or parts of a location object
  - Rules can express policy, but not enforce
- Eavesdropping
  - Whole LO or parts of it
- Anonymity is selective availability
  - Location, time authorized, but not identity
  - Identity, time, but only rough location
Questions

• Does this capture all the threats people perceive?
• Perhaps a different perspective: What constitutes a secure location service? What guarantees do people want?
• Is this something the WG is interested in pursuing?
Next Steps

• Based on valuation of threats, determine requirements for countermeasures

• Standards and BCPs for countermeasures