Attested Proximate Location

draft-mandyam-rats-proxlocclaim

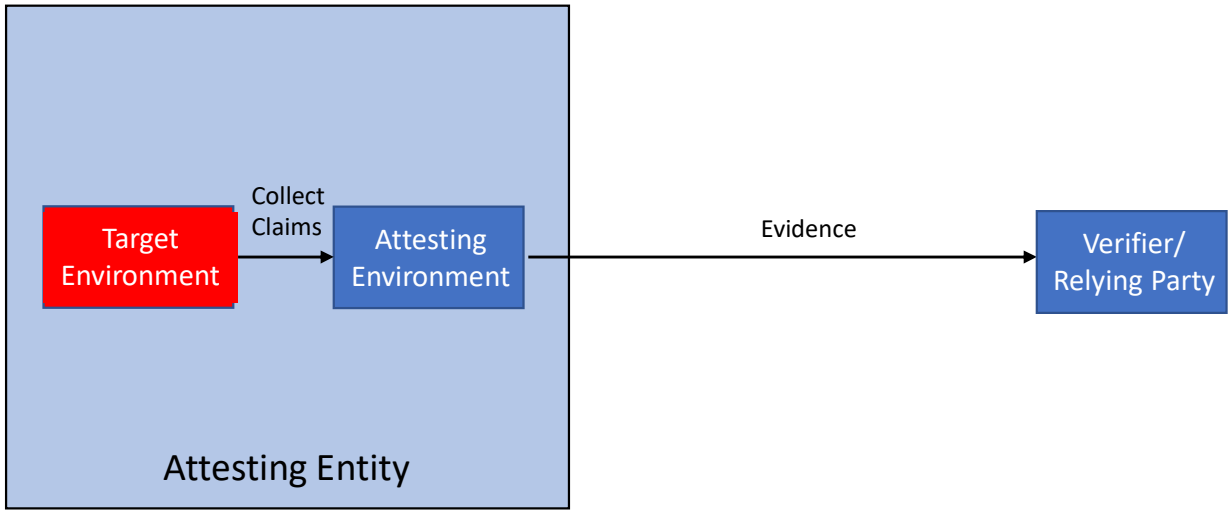
References

1. The Entity Attestation Token. https://datatracker.ietf.org/doc/draft-ietf-rats-eat/. IETF Internet Draft.
2. Remote Attestation Procedures Architecture. https://datatracker.ietf.org/doc/rfc9334/. IETF RFC.
3. G. Mandyam et al. "UWB Secure Ranging in FiRa". https://www.firaconsortium.org/sites/default/files/2022-08/FIRA-Whitepaper-UWB-Secure-Ranging-August-2022.pdf.

Introduction

- Attested geolocation is a means by which an attester can provide “evidence” of its security state
- The attester is composed of an attesting environment and a target of attestation
- Evidence can come in the form of claims [1], which can be sent via cryptogram to a verifier
  - Usually a verification is within the functionality of a Relying Party, but it is not strictly necessary [2]

Introduction (cont.)

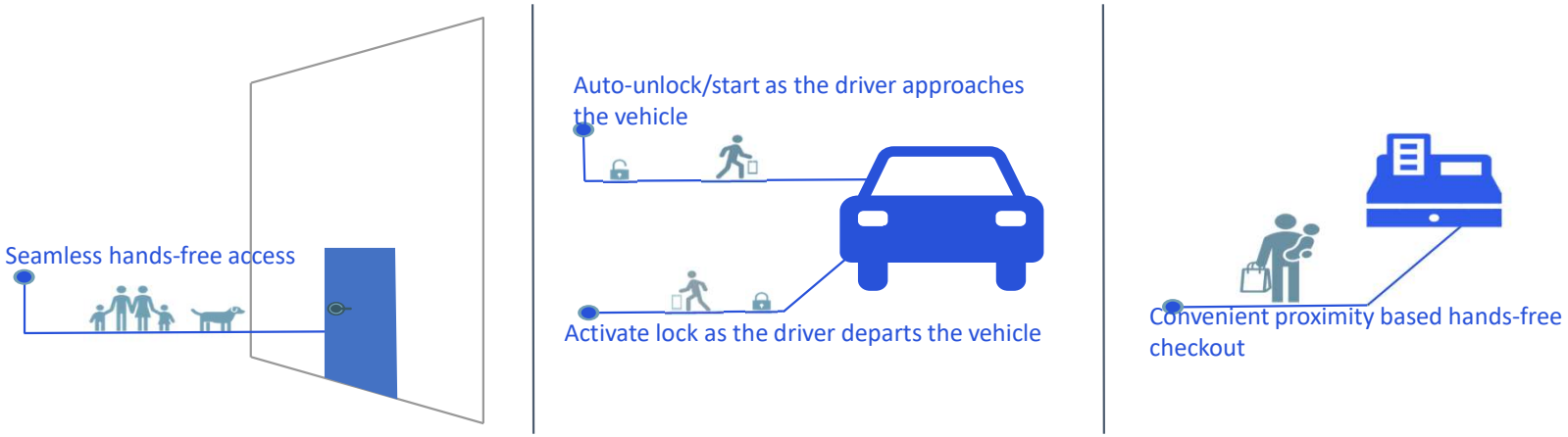


Introduction (cont.)

- Attested geolocation is mature feature [1]
- Attester presumably has access to trusted sensor data from which it can derive a location for the claim
  - Conveyed in the form of a geodetic coordinate system (e.g. WGS-84)

Secure Ranging

- Secure ranging involves the process where a “reader” is able to detect the relative location of a device and use this information in the context of authentication [3]
  - Examples: car door unlock, restricted access facility entrance



Attested Proximate Location

- Secure ranging reader may seek to attest the location of the target device
- Deviation from reference architecture in [2] as attester is not integrated with target of attestation
  - “Delegated attestation”
- A proximate location claim would ideally include the following information
  - Unique identifier of target device (e.g. ueid in [1])
  - Projected location of device to known geodetic coordinate system
- Relying Party can use the proximate location claim as part of any authorization provided to the device (device owner)
  - Would be part of its appraisal policy [2]

Projected Location

- Assumption: reader knows its own geolocation coordinates (e.g. integrated GNSS engine)
- Reader detects relative location of device
  - Distance and angle-of-arrival (azimuthal)
  - Vertical angle-of-arrival also possible
- Use of map-based projection allows for estimation of gpS coordinates

Map-based projected location: UTM transformation

- Universal Transverse Mercator (UTM) system projects lat/lon to x/y coordinates in a planar representation of surface of Earth
- Given relatively small distances between reader and device in practical settings, planar projection should be sufficient
  - Insignificant contribution from Earth curvature
- Geolocation to UTM conversion via well-known formulas
  - As an example, Pacifico Yokohama (35.4586, 139.6370) converts to UTM 376318 Easting, 3924756 Northing in UTM Zone 54N

Map-based Projected Location (cont.)

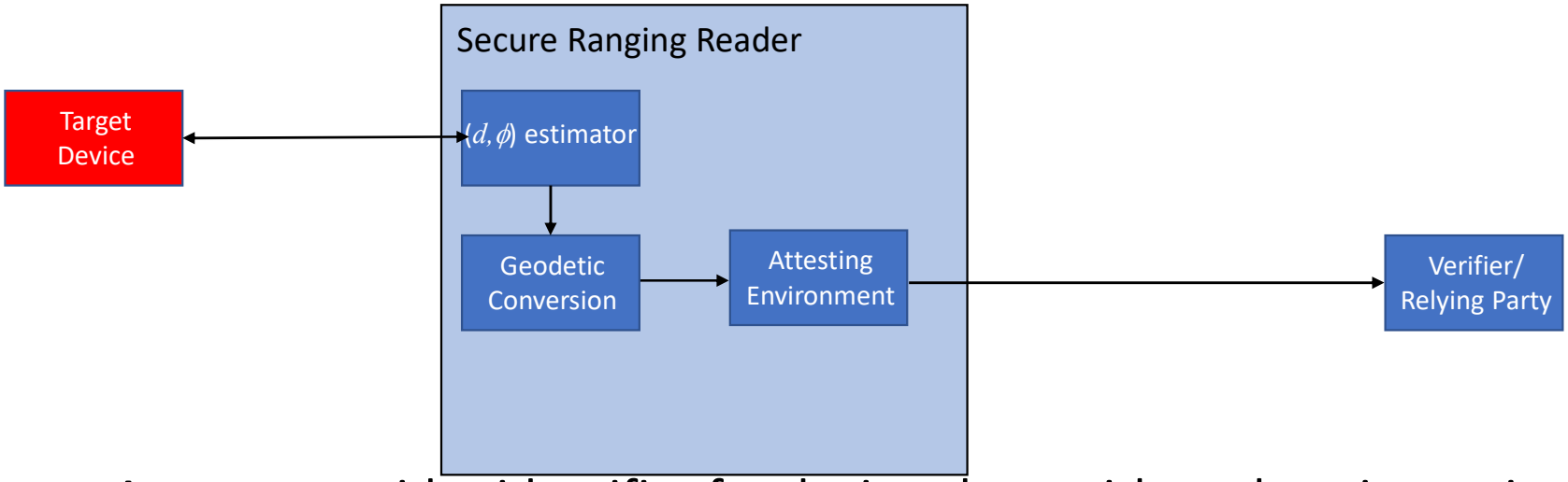
- Assume Easting/Northing pair for reader is given as (e,n), and target device is at relative distance d and AoA ϕ, with both endpoints within same UTM zone
- UTM pair for device (e_{dev},n_{dev}) can be found as

$$e_{dev} = e + d\ cos(\phi)$$
$$n_{dev} = n + d\ sin(\phi)$$

- Note that UTM zone transition between secure ranging endpoints is unlikely due to ranging distance (typically less than 10 m) versus zone dimensions
- UTM -> WGS-84 conversion also well-known

System Architecture Example

- Secure ranging reader: delegated attestation



- Attester provides identifier for device along with geolocation estimate in attestation token

Obtaining Target Device Identifier

- Target device can communicate unique ID independent of ranging operation
  - Example: transmission of attestation token from target device to reader
    - Will include identifier that can be relayed in delegated attestation
  - Can be via sideband communications channel
- Reader can also assign unique ID to the device
  - Example: reader is integrated in device manager, that is capable of assigning and provisioning unique ID on target device
- Reader can leverage a ranging session-specific identifier

Proposed Claim

```
proxloc-type = { target-ueid => ueid, ; derived from EAT claim ueid
                 ? target-location => location ; derived from EAT claim location if WGS-84 coordinate projection possible
                 ? aoa => float ; angle-of-arrival optionally sent
                 ? distance => float ; ranging distance optionally sent
                 ? aoe = float ; angle-of-elevation optionally sent   }
```

- All location attributed optionally sent; what if nothing is sent?
  - Verifier/RP can still use this claim as an indication of the reader attesting to its inability to reliably determine location of target device