Progress Report

Yin-Hong Hsu

03 30, 2018

Outline

Attack model

Assumption

Other benefits

References

Attack model

- Eavesdropping:
  - the adversary can eavesdrop get unsafe channels to get messages. In the region-based MCS, the sensed information and the corresponding ring signatures are sent through the Internet without encryption so the adversary can get all of them
- Replay attack:
  - after eavesdropping, the adversary can send a copy without modification to AS. In the RCRS, we have added a timestamp in the message structure to prevent this kind of attack so that the overdue messages would be abandoned

Attack model

- Brute force:
  - the adversary is able to try every possible keys and try to make the same signature as the one that matches the eavesdropped message. In the 256-bit RCRS scheme, the key space of MUs private key contains 2 256 possible keys. It is impossible to discover the MUs private key of the message without extremely powerful computing power
- Intersection attack:
  - If a specific signer changes the ring to use every time, the adversary can easily to find out what public key the signer is actually used

Attack model

- Location forgery:
  - In RCRS, if the MU was compromised by adversary, the adversary can tell KA that MU is leaving to another location. So that can remove MU from current ring.
- Fake Base Station:
  - The adversary can use a fake base station to make MU to connect to, and log all traffic includes MU's privacy info. In proposed framework, the SU in Fog Node can provide privacy preserve service.

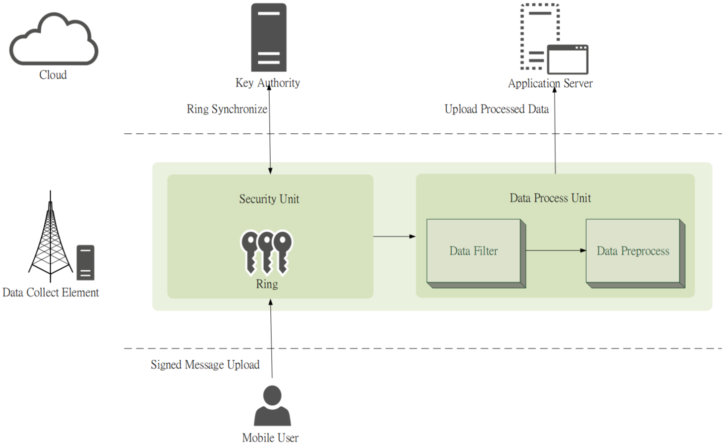

Figure: Architecture

Assumption

- Fog Nodes are fully trusted
- Key Authority is maintained by a trusted third party
- Each Fog Node is a part of an eNB, and the Fog Node can access all parameter in Telecom network
- The connect between Fog Node to KA and Fog Node to Fog Node is trusted

Other benefits

- When MU move to another region, MU do not have had to notify KA where it goes, Fog nodes will deal it
- MU only need to communicate with KA once (register)
- KA will distribute ring to each region periodic. In RCRS, KA have to broadcast to each MU, AS; In proposed framework, KA only have to send new rings to Fog Nodes, then each Fog Node will distribute the ring to MUs in this region

References

Thanks for Your Attentions