2016/11/16 @ IPWAVE, IETF 97

Security and Privacy Issues in IPWAVE

Jong-Hyouk Lee (jonghyouk@smu.ac.kr)

Protocol Engineering Lab., Sangmyung University

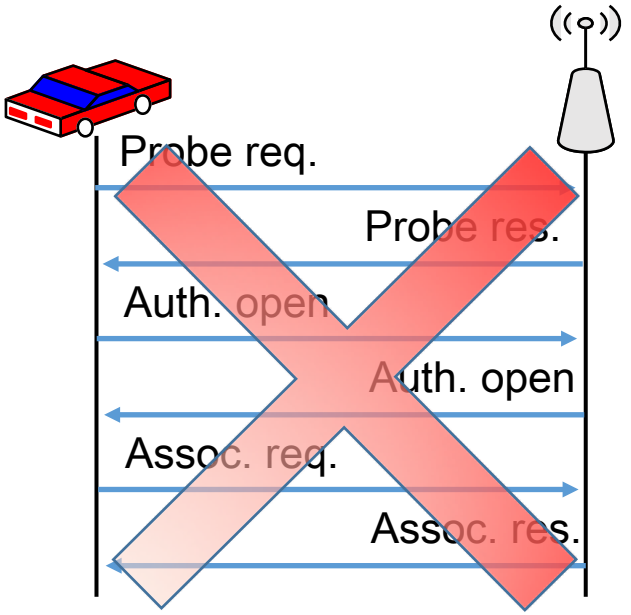
Background (1/3)

- Safety messages are not transmitted in IPv6 packets
  - Non-IP communication is used for safety messages
    - Basic Safety Messages (BSM) in the US
    - Cooperative Awareness Messages (CAM) in the EU

- IPWAVE mainly considers
  - IPv6 packet transmissions over IEEE 802.11 OCB
    - 802.15.4, 802.11ad, LTE-D, LP-WAN, etc. also possible
  - IPv6 Vehicle-to-Infrastructure (V2I) communication
  - IPv6 Vehicle-to-Vehicle (V2V) communication

Background (2/3)

- IEEE 802.11 OCB
  - No authentication procedure
  - No encryption provided
  - No privacy protection



- IEEE 1609 and ETSI TC ITS defined security and privacy mechanisms only for non-IP communication
  - Security/Privacy for BSM over 802.11 OCB
  - Security/Privacy for CAM over 802.11 OCB

Background (3/3)

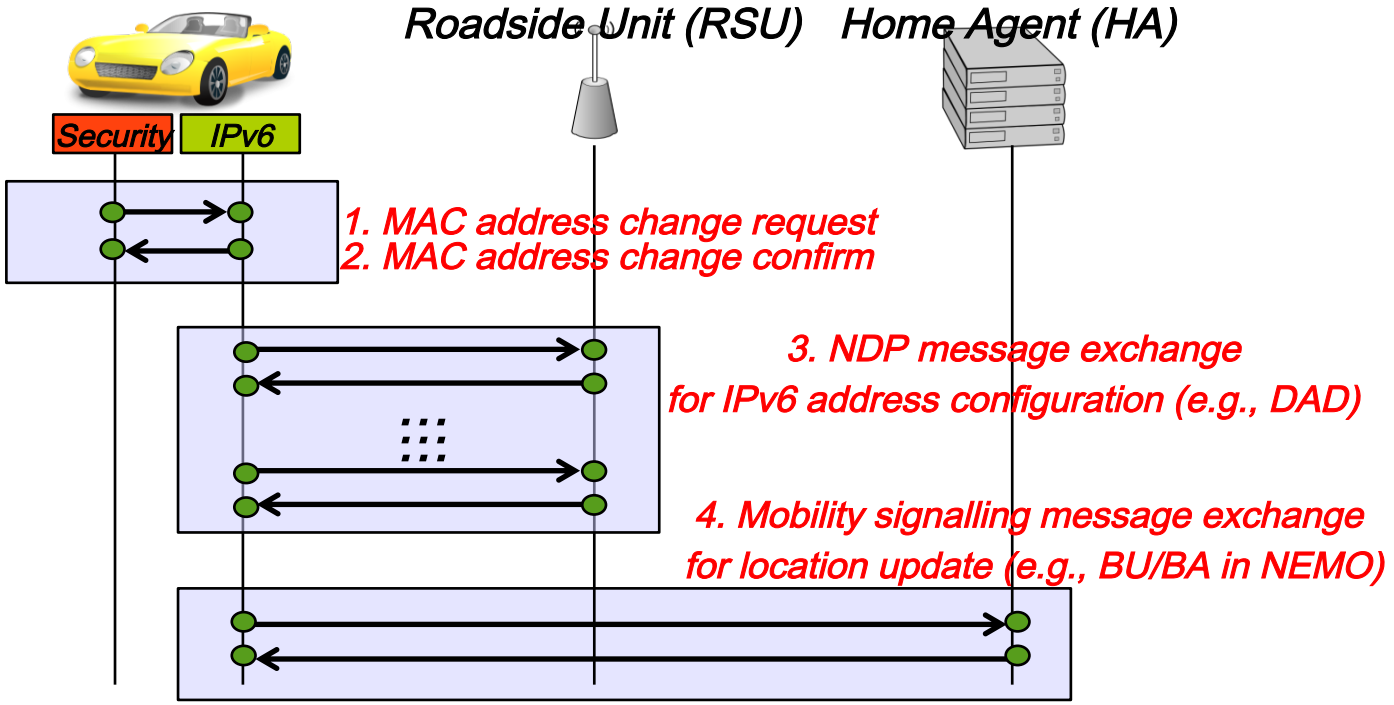
- Security/Privacy by IEEE 1609 and ETSI TC ITS
  - Use of asymmetric cryptography and certificate
    - Elliptic Curve Digital Signature Algorithm (ECDSA)
  - Use of pseudonyms
    - A set of temporary certificates not containing identifiers
    - One pseudonym is used for a short period
  - Use of the MAC (link-layer) address randomization
    - One MAC address is used for a short period
  - Use of pseudonym and MAC address changes
    - For location privacy (privacy vs. performance)

Security/Privacy in IPWAVE (1/5)

- Assumption
  - IPv6 runs over IEEE 802.11 OCB
    - Security/Privacy mechanisms developed for non-IP communication (by IEEE and ETSI) will have impacts
    - For instance, the MAC address change is not controlled by the IPv6 layer, but by the security entity
      - ETSI TC ITS and ISO TC204 define the security entity that manages all security operations, e.g., key and certificate management, pseudonym and MAC address changes, etc.

Security/Privacy in IPWAVE (2/5)

- MAC (link-layer) address change
  - It causes the IPv6 address change
  - It causes IPv6 session disconnections
  - It may impact other IPv6 operations
    - e.g., NDP, DAD, CGA/SEND, BU/BA in NEMO



Security/Privacy in IPWAVE (3/5)

- Pseudonym change
  - It causes the session key change if a pseudonym is used for a key establishment
  - It causes the re-key establishment
    - e.g., SEND/IPSec/TLS

Security/Privacy in IPWAVE (4/5)

- MAC (link-layer) address randomization
  - There are several proposals
    - RFC 7721: Security and Privacy Considerations for IPv6 Address Generation Mechanisms

  - Which one is good for IPWAVE?

Security/Privacy in IPWAVE (5/5)

- Something more needed for IPWAVE privacy
  - MAC address randomization, MAC address change, and pseudonym change are not enough
  - Still IPv6 protocols contain identifier information that can be used for tracking
    - IPSec, IKE, TLS

Next Step

- Documentation needed for security and privacy issues in IPWAVE
  - IEEE 802.11 OCB (with the Security/Privacy mechanisms defined by IEEE and ETSI) impacts on IPv6 protocol operations
  - Specific considerations for V2I and V2V

Thanks!

Jong-Hyouk Lee (jonghyouk@smu.ac.kr)