Basic Support for Security and Privacy in IP-Based Vehicular Networks

draft-jeong-ipwave-security-privacy-06

Tae (Tom) Oh
Professor
School of Information
Golisano College of Computing and Information Sciences
Rochester Institute of Technology

Agenda

- Security Attacks
- Security Countermeasures

Security Attacks

- Security and privacy are very important V2I, V2V and V2X.
- Only identified and authorized vehicles should be allowed.
- Reliable communication between vehicle, mobile devices in VANET and the Internet.

Different Attacks

- False information attacks
  - Disseminating false driving information. Ex. Sybil attach.
  - Multiple false identities for non-existing vehicles can confuse real vehicles and wrong maneuver decisions.
  - **Mitigation:** Identification scheme needs to check the validity of a user with his/her identification information.
- Impersonation attacks
  - Pretend to be other vehicles with forged IP or MAC addresses
  - **Mitigation:** Authentication scheme needs to check whether MAC or IP address associate with permanent identifier.

Security Attacks-Types

- Denial of service attack
  - Generate bogus services to either vehicles or servers in the cloud. This causes vehicles or servers to become extremely busy.
  - **Mitigation:** Vehicle collaborations to monitor suspicious activities.
- Message suspension attack
  - Drop packets originated by other vehicles in multihop V2V or V2I communications.
  - Hinder reliable data exchange for safe driving in cooperative driving environments.
  - **Mitigation:** Good vehicles and RSU detect suspension attacks.

Security Attacks-Types

- Tampering attack
  - An authorized and legitimate vehicle may be compromised by a hacker so that it can run malicious firmware or software.
  - **Mitigation**: Forgery prevention of firmware (bootloader) performs a secure booting scheme. Remote attestation scheme detects abnormal behavior. Security firmware update protocol performs a safe update.

Security Attacks-Types

- Tracking
  - Use MAC and IPv6 addresses to track moving vehicle.
  - **Mitigation:** Update MAC address and IPv6 addresses periodically.

Security Countermeasure

- Identification and authentication
  - Valid certification for valid vehicles.
  - X.509 certificate (TLS certificates) + vehicle identification number (VIN)
  - A decentralized Identifier (DID) can be used by good vehicles with assistance from a verifiable claim service.
- Integrity and confidentiality
  - A secure channel between two communication entities.
  - Session keys: Internet Key Exchange Protocol v2 (IKEv2)

Security Countermeasure

- Non Repudiation
  - The messages generated by a vehicle can be logged by its neighboring vehicles.
  - Blockchain technology
- Remote Attestation
  - Secure booting can be performed by Root of Trust (RoT), and a remote attestation can be performed through both the secure booting and RoT

Security Countermeasure

- Privacy
  - MAC address pseudonym-update periodically.
  - Affects on-going traffic + update of neighbor caches.