Security Challenges on V2X Communications

Mesut ORMANLI
Institute of Pure and Applied Sciences
Marmara University

Vehicular Networks Overview

- Vehicular networks are a special class of mobile networks, which are deployed to the domain of vehicles.
- This type of networks generally operate in ad-hoc basis, because of the characteristics of overland transportation.

Vehicular Networks Overview

- Communications within vehicular networks include
  - vehicle-to-vehicle [V2V],
  - vehicle-to-infrastructure [V2I],
  - vehicle-to-pedestrian [V2P],
  - vehicle-to-device [V2D] and
  - vehicle-to-grid [V2G] communications

  all of those are referred as vehicle-to-everything [V2X] communications.

Vehicular Networks Overview

- In this presentation, common security and privacy challenges intended to the V2X communications, and some of related solutions will be explained.
- First paper focuses on vehicular ad-hoc networks [VANET] security, second paper mainly focuses on security of vehicles itself.

Covered Papers

- [1]: Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANet security challenges and solutions: A survey. Vehicular Communications, 7, 7-20.
- [2]: Bernardini, C., Asghar, M. R., & Crispo, B. (2017). Security and privacy in vehicular communications: Challenges and opportunities. Vehicular Communications, 10, 13-28.

VANet Security Challenges and Solutions: A Survey

- VANET Characteristics
- VANET Security Challenges and Constraints
- Security Requirements [Services]
- Attack Types
- Attacker Types
- Standardization Efforts
- Proposed Solutions from the Literature
- Emerging and Open Issues

VANET Characteristics

- Related to network topology and communication mode:
  - Unbounded and scalable network
  - Wireless communication
  - High mobility and rapidly changing network topology
  - Support to real-time and multimedia applications

VANET Characteristics

- Related to vehicles and drivers:
  - Processing power and energy consumption
  - Time and position knowledge
  - Honesty of participants
  - Existing law enforcement infrastructure
  - Central registration with periodic maintenance and inspection

VANET Security Challenges and Constraints

- Challenges:
  - Network size and geographical relevancy
  - High mobility and dynamic topology
  - Short connection duration
  - Frequent disconnections
  - Trust and information verification
  - Key distribution

VANET Security Challenges and Constraints

- Constraints:
  - Congestion and collision control
  - Low tolerance for error occurrence
  - Environmental impact
  - Risk analysis and management
  - Anonymity, privacy and liability

Security Requirements [Related Services]

- Authentication
- Availability
- Confidentiality
- Integrity
- Privacy and anonymity

Security Requirements [Related Services]

- Data verification
- Access control
- Traceability and revocability
- Error detection
- Liability identification
- Flexibility and efficiency

Attack Types

- Threats to wireless interface:
  - Identity and geographical position revealing [location tracking]
  - DoS [Denial of Service] and DDoS [Distributed Denial of Service]
  - Sybil attack
  - Malware
  - Spam
  - Man in the Middle Attack [MitM]
  - Brute force attack
  - Black hole attack

Attack Types

- Threats to hardware and software:
  - Injection of erroneous messages [bogus info]
  - Message suppression or alteration
  - Usurpation of the identity of a node [spoofing, impersonation]
  - Tampering hardware
  - Routing attacks
  - Cheating with position info [GPS spoofing]

Attack Types

- Threats to sensors input in vehicle:
  - Illusion attack
  - Jamming attack
- Threats to infrastructure:
  - Unauthorized access
  - Session hijacking
  - Repudiation [loss of event traceability]

Attacker Types

- Selfish/greedy drivers
- Malicious attackers
- Pranksters
- Snoops/eavesdroppers
- Industrial insiders

Attacker Classification

- The attackers are classified into:
  - Insider vs. outsider
  - Malicious vs. rational
  - Active vs. passive
  - Local vs. extended

Standardization Efforts

- Public key infrastructure [PKI]
  - A trusted party
  - A registration authority
  - A certificate database
  - A certificate store

Standardization Efforts

- Security architectures:
  - ETSI in Europe
  - NHTSA in United States
- Security standarts:
  - IEEE 1609.2 Standardization of IEEE
  - ETSI Standardizations

Proposed Solutions

- For attacks on wireless interface:
  - Tracking, Eavesdropping and Traffic analysis attacks
  - Information disclosure
  - DOS attack
  - Sybil attack
  - Malware and Spamming
  - Man in the middle attack
  - Brute force attack

Proposed Solutions

- For attacks on hardware and software:
  - Message tampering
  - Spoofing and forgery attacks
  - Message saturation
  - Node impersonation

Proposed Solutions

- For attacks on sensors input in vehicle:
  - Jamming attack
  - GPS spoofing or faking position or illusion attack
- For attacks on infrastructure:
  - Key and/or certificate replication that cause unauthorized access
  - Loss of event traceability [repudiation]

Emerging and Open Issues

- The trustworthiness evaluation of nodes participating in VANET and their misbehavior detection
- The revocation process and the certificate revocation list management and distribution
- The ability of the network to self-organize via a high mobile network environment

Emerging and Open Issues

- Data context trust and verification
- Cryptographic approaches for security, privacy and non-traceability assurance
- Anti-malware and Intrusion Detection System

Security and Privacy in Vehicular Communications: Challenges and Opportunities

- Requirements for Modern Cars
- Intra-vehicle Communications
- In-vehicle Network Gateways
- Inter-vehicle Communications
- Future Directions

Requirements for Modern Cars

- Security requirements:
  - Authentication
  - Intellectual property protection
  - Confidentiality
  - Integrity
  - Access control
  - Message freshness
  - Privacy
  - Availability

Requirements for Modern Cars

- Safety requirements:
  - Safe development
  - Safety risks
  - Real-time constraints
  - Maintenance
  - Free from interference
    - In time domain
    - In communication domain
    - In data processing domain

Requirements for Modern Cars

- Standardization of the architectural requirements:
  - Automotive Open System Architecture [AUTOSAR]
    - Developed by a strong consortium of key players in the automotive industry including BMW, Bosch, DaimlerChrysler, Volkswagen, Ford, Peugeot and Toyota
    - Aims to assist with the development of vehicular software, user interfaces and their management.

Requirements for Modern Cars

- AUTOSAR core modules:
  - Hardware dependent modules
  - Operating system [OS]
  - Basic software [BSW]
  - Runtime environment [RTE]
  - Software components [SWC]

Requirements for Modern Cars

- AUTOSAR safety features:
  - Memory protection
  - Timing monitoring
  - Logic monitoring
  - End-to-end communication
  - Execution modes

Requirements for Modern Cars

- AUTOSAR security modules and services:
  - Crypto service manager [CSM]
  - Crypto abstraction layer [CAL]
  - Secure on-board communication [SecOC]

Intra-Vehicle Communications

- Components:
  - Electronic control unit [ECU]
    - The unit of computation in the intra-vehicular network
  - Communication media
    - The intra-vehicle network is composed of physical wires that interconnect ECUs

Intra-Vehicle Communications

- Bus-based networks:
  - Controller area network [CAN]
  - Local interconnect network [LIN]
  - FlexRay
  - Media oriented systems transport [MOST]
  - Ethernet and BroadR-Reach

Intra-Vehicle Communications

- Security and privacy issues:
  - Authentication of ECUs.
  - Time-propagation errors
  - Network monitoring
  - Self-healing
  - Self-adaptive network
  - Secure communication
  - Counterfeiting and intellectual property theft

In-Vehicle Network Gateways

- In-vehicle gateways:
  - On-board diagnostics [OBD]
  - Tire pressure monitoring system [TPMS]
  - Electrical vehicles [EVs]
  - Remote keyless system [RKS]
  - Infotainment and telematics

In-Vehicle Network Gateways

- Security and privacy issues:
  - For on-board diagnostics
    - Authentication
    - Integrity
    - Secure communication
    - Attacks on third party interfaces
  - For tire pressure monitoring system
    - Authentication and confidentiality
    - Tracking vehicles

In-Vehicle Network Gateways

- Security and privacy issues:
  - For EV charging plug infrastructure
    - Key management
    - Integrity
    - Connection to the smart grid
    - EV privacy

In-Vehicle Network Gateways

- Security and privacy issues:
  - For remote keyless system
    - Security of RKS
    - Security of immobilizer
  - For infotainment and telematics
    - Secure interaction with smartphones
    - Privacy in “pay-as-you-drive” insurance

Inter-Vehicle Communications

- Physical and data link layers: 802.11p.
- IEEE 1609 / WAVE
  - Security features of WAVE
- Security and privacy issues
  - Authentication in V2V and V2I
  - VPKI
  - Pseudonyms [location privacy protection]

Future Directions

- Effective network monitoring
- Secure and efficient data processing
- Scalable and privacy-preserving Services
- Practical and reliable data fusion

Thank You!

- Any questions?