SOFTWARE-DEFINED VEHICULAR NETWORKING SECURITY:
Threats and Opportunities for 5G

Marc Lacoste, David Armand, Franck L’Hereec
Frédéric Prévost, Yvan Rafflé, Sébastien Roché

C&ESAR 2019, Virtualization & CyberSecurity Track
Rennes, November 19, 2019
connected & autonomous vehicles raise multiple security concerns


juicy target for hackers, growing # of attacks

safety-security gap, liability issues
connected & autonomous vehicles: a core 5G use case

1 vehicles
VANETS, vehicular clouds
software-defined vehicular networks

2 edge

3 clouds

cellular and wireless connectivity
- 3GPP and ETSI standards
- low-latency protocols for V2V and mobile edge networking

Orange – unrestricted
connected & autonomous vehicles: a core 5G use case

V2X ecosystem

a holistic vision of protection is needed:
- software and hardware
- vehicle, network, and cloud tiers
- covering the full data life-cycle

software
- Security

hardware
- Security

vehicle
- Security

network
- Security

cloud
- Security

1 vehicles

VANETS, vehicular clouds

software-defined vehicular networks

cellular and wireless connectivity
- 3GPP and ETSI standards
- low-latency protocols for V2V and mobile edge networking

Orange – unrestricted
some key automotive use cases

Lane Merging
coordinate vehicle trajectories to enhance safety & efficiency
- wireless communication, positioning system (GNSS)
- authenticity, integrity of shared data: avoid accidents
- privacy: data must not be stored

See Through
extend perception range beyond vehicle line-of-sight
- camera, video server
- integrity: lower if multiple sources of information
some key automotive use cases

HD Local Map Acquisition

use the cooperative sensing of vehicles to build an optimal route map using an off-board system

- information distributed to vehicles is organized in polygons
- improves driving experience
- privacy: huge amount of data collected
  - unnecessary information must be kept confidential

key security and privacy requirements

- integrity and authentication with high level of robustness: mandatory for all use cases
- privacy and confidentiality: depending on the use case
- secure update / revocation of software and authentication credentials in vehicles: security features should remain robust over time
Overview

- **Complexity**: V2X ecosystem
- **Multiplicity**: Use cases
- **Diversity**: Security requirements

**Software-Defined Vehicular Networking (SDVN)**

applies benefits of SDN to vehicular systems and networks

- Simpler approach for security management
- **Risks**
- Opportunities for cybersecurity services

- **Overview** of SDVN approach and architectures
- Assess **security impact**: benefits and risks
- Highlight **security service opportunities** for telcos
what is SDVN?
  - principles
  - architectures
  - examples: 5G, edge computing

which security impact?
  - threats
  - security benefits

which security opportunities for telcos?
SDVN principle

- scalability
- QoS (latency, mobility)
- flexibility, programmability
- cost effectiveness
- inefficient resource use
- internetworking
- security
- reliability

VANETs deployment challenges

SVDN = SDN + VANETs
programmability and flexibility
in vehicular distributed wireless substrate

SDVN architecture

- data plane: vehicles and RSUs abstracted as “network switches”
- control plane: SDN controllers oversee the vehicular network

SDVN benefits and challenges

**benefits:** making VANETs more flexible and programmable
- **path selection:** optimization of packet routing
- **channel selection:** better management of heterogeneous vehicular communications (e.g., reducing interference)
- **safety services:** emergency traffic gets priority over other traffic
- **isolation and slicing**

**challenges:**
- **inefficient control for high mobility**
- **open development environments**
- **SDN security and dependability**
new use cases in 5G magnify several vehicular challenges

- low-latency
- network heterogeneity: HetNet architecture
- mobility, dynamic topology
- resilience

SDVN benefits in 5G context

- dynamic nature of vehicular networks
- trade-offs between performance, vehicle density, radio coverage

applications

- adaptive vehicle clustering: cluster heads
- beamformed transmission
- vehicle location prediction
- cooperative communication

Sample architecture: 5G-SDVN

- 5G introduces more complexity but the SDVN model is still applicable
- **Fog cell**: define broader geographical zones for vehicular communication between vehicles using multiple hop relays in the cells
- improves scalability, flexibility, and solves handover issues

SDVN and edge technologies

CAV = "Smart Connected Community"

- examples: smart city, connected health, IoT, smart home, smart grid, ...
- challenges: low-latency, context-awareness, scalability, CAV networking challenges

SDVN + edge technology benefits

- simpler, smarter, more efficient management
- CAV benefits: scalable video streaming, real-time roadside computing, efficient mobility

Tough problems

- cascading failures
- inter-edge and inter-cloud collaboration and orchestration ⇒ SDWAN?
- cyber-threats on decision-making points (e.g., smart car intelligence)

Orange – unrestricted
what is SDVN?
- principles
- architectures
- examples: 5G, edge computing

which security impact?
- threats
- security benefits

which security opportunities for telcos?
**SDVN threats**

Some key points of security vigilance in an SDVN architecture:

- **centralized SDN controller**
- DoS attacks
- Intricate software layers
- MiTM attacks
- open architecture

- distributed multi-controllers
- configuration conflicts
- illegal access

**SDVN threats**


- Centralized SDN controller
- DoS attacks
- Intricate software layers
- MiTM attacks
- Open architecture
  - Distributed multi-controllers
  - Configuration conflicts
  - Illegal access

**some key points of security vigilance in an SDVN architecture**

- Need for defense-in-depth approach
- Limit threat propagation with hardened, standardized APIs
- Secure data plane to limit amplification of SDN threats

*Orange – unrestricted*
SDVN security benefits

**SDN security benefits**: manage security more flexibly and simply for vehicular networks

<table>
<thead>
<tr>
<th>SDN feature</th>
<th>root cause</th>
<th>security service</th>
</tr>
</thead>
<tbody>
<tr>
<td>overall network</td>
<td>centralization, statistics</td>
<td>network-wide IDS, network</td>
</tr>
<tr>
<td>view</td>
<td>on traffic</td>
<td>forensics, switch anomaly</td>
</tr>
<tr>
<td>self-healing</td>
<td>conditional rules, statistics on traffic</td>
<td>packet dropping, packet redirection</td>
</tr>
<tr>
<td>increased control</td>
<td>flow-based forwarding</td>
<td>access control</td>
</tr>
</tbody>
</table>

**for telcos**: services for automotive connectivity
- **in-vehicle**: intrusion detection, firewalls, device management
- **connectivity**: slicing, network anomaly detection
- **orchestration**: data protection, safety

**user safety**: Software-Defined In-Vehicle Networking (SDIVN)
- **resilience** against in-vehicle failures
  - without hardware re-design
- **in-vehicle** software network reconfiguration

what is SDVN?
- principles
- architectures
- examples: 5G, edge computing

which security impact?
- threats
- security benefits

which security opportunities for telcos?
a growing ecosystem

collaborative projects and testbeds
- V2X use cases
- security & privacy requirements
- 5G security architecture

multi-domain including for security

MEC potential for security & privacy

LINAS-MONTLHERY TESTBED
security service opportunities
machine-learning: towards the software-defined vehicle

- context-aware, continuous adaptation of functionality and protection
- driver, OEM, infrastructure and network provider requirements

approach: anomaly detection

security service opportunities
machine-learning: towards the software-defined vehicle

- context-aware, continuous adaptation of functionality and protection
- driver, OEM, infrastructure and network provider requirements

approach: anomaly detection
conclusions

**SDVN:** helps meeting many security & resilience requirements of automotive ecosystem
- a *simple* and *flexible* approach to vehicular security management
- SDVN addresses several key deployment issues
  e.g., scalability, mobility, network heterogeneity and variability, real-time (edge technologies)

**security impact:**
- protect SDN controller, standardize APIs, secure lower data plane, real-time authentication
- enhance user safety and security

**opens security opportunities through value-added services:**
- mitigation of long-range attacks and IoT vulnerabilities
- **new services:** security audit, attack detection, secure update (eSIM), resilience
outlook

autonomic security loops

- **services:** security monitoring/prevention - in-vehicle (SoC), vehicle-to-network, end-to-end
- **resilience:** bridge safety-security gap

SDVN highlights the potential of machine learning/AI for automotive

- high mobility, strong dynamics, QoS requirements, safety and security
- advanced modelling/simulation of cyber-physical systems

outlook to other verticals

- « systems-of-systems »
- cross-vertical approach to security and safety
Thank you

Marc Lacoste
Orange Labs
Senior Research Scientist
marc.lacoste@orange.com