V2X security, privacy and trust overview

Dr. José María de Fuentes
(jfuentes@inf.uc3m.es)
COSEC Lab
University Carlos III de Madrid
Agenda

• Intro: Vehicular communications (V2X), what for?
  o Real-world news
• V2X stakeholders
• Security, privacy, trust issues
• Our previous results
• Conclusions
V2X – what for?

- Part of **smart cities**
- Road safety + infotainment

Image source: Telematicsnews.org, arm.com
Lower Your Car Insurance Bill, at the Price of Some Privacy

MARCH 13, 2014

An increasing number of the nation’s auto insurance companies have a new proposition: Let them track every second of your driving in exchange for an annual discount that can reach into the hundreds of dollars if you behave yourself on the road.

In theory, everyone wins here. Progressive, Allstate and State Farm — among the most aggressive of the larger companies that are pursuing this strategy — attract better drivers who crash less often. Customers who sign up for the optional programs can pay premiums based more on how they drive and less on their age, gender or credit history.

But usage-based insurance, as the program is known, generates vast amounts of data. While insurance companies are pledging to keep it to
V2X security in the real world

BMW sounds alarm over tech companies seeking connected car data

Concerns over fine line taken by the automotive industry between functionality and privacy

Ian Robertson introduces BMW’s new line of 6 Series cars at the North American International Auto Show in Detroit. Photograph: Scott Olson/Getty Images
V2X sec&priv&trust in the real world

Germany's Autobahns Say "Willkommen" To Robocars

By Philip E. Ross
Posted 30 Jan 2015 | 18:00 GMT

Photo: Jochen Eckel/AP

Parts of Germany's A9 Autobahn, which runs from Berlin to Munich, will be open to experimental robocars.
V2X sec&priv&trust in the real world

Senator: Your futuristic car is putting your privacy and security at risk
V2X stakeholders

- Automakers & car industry
- Governments
- Consumers

- What about V2X security, privacy, trust?
V2X active stakeholders

• Automakers
  o Increasingly involved – proof-of-concept, experimental settings
  o R&D efforts

• Governments
  o Legal framework for ITS: EU directive & action plan on ITS, also in the US…
  o Also initiatives in the National level: Spanish ITS initiative…

• Research community
  o Reliable connection
  o Bandwidth improvements
  o Protocol design
  o … security, privacy and trust
  o Standardization (IEEE, SAE…)
V2X – design constraints

• Short-range communications
  o Dedicated Short Range Communications (DSRC) – IEEE 802.11p
  o 1 km nominal range – 300 mts in practice

• Short communication period
  o Vehicles driving at 140 km/h or higher

• Embedded platform
  o Not PC… low computation resources

• Lack of global infrastructure
  o Ad-hoc nature

• Regular sec/priv mechanisms cannot be applied “as is”
V2X – security

• Data may be privileged
  o On-trip services (e.g. next gas station pre-booking)
  o Need for confidentiality
  o IEEE 1609.2: use of elliptic curves

• Data must come from authorized entities
  o Road safety announcement (e.g. bottleneck ahead)
  o Need for source authentication
  o IEEE 1609.2: public-key certificates

• Some actions must be accountable
  o Illusion attack – forcing a collision
  o Someone has to be liable! Need for non-repudiation
  o IEEE 1609.2: elliptic curves digital signature (ECDSA)
V2X – privacy

- Beacon permanently sent
- Signed with public key certificates
- **Hot topic** – use pseudonyms? Anonymous certificates? How to deal with accountability?
V2X – trust

• Data must be **trustworthy**
  - Avoid false alarms
  - Building plausibility checks
  - Data-centric trust establishment

• (Low) in-vehicle data security
  - CAN bus: efficiency vs. Security
  - Cheap sensors

• Safety is at stake! Secure on-board platform
  - Car-to-car consortium
  - EU R&D projects: EVITA, OVERSEE
  - Use of Hardware Security Modules (HSM)

**BMW fixes security flaw in its in-car software**

Jan 30 (Reuters) - German luxury carmaker BMW has fixed a security flaw that could have allowed hackers to unlock the doors of up to 2.2 million Rolls-Royce, Mini and BMW vehicles, it said on Friday.
V2X sec/priv/trust miscellaneous issues

• Over-the-air updates
  o Flexibility against security

• Non-repudiation of receipt
  o Future issue: “I was not aware of the speed limit in force!”

• Data aggregation
  o Good for efficiency, what about security?
V2X sec/priv/trust at COSEC

• Overview of security issues in V2X
• Hindering false event dissemination in V2X
• V2X for enforcement
  o Privacy-preserving speed control
  o V2X-based fine notification
  o Evidence management to report misbehaving vehicles
  o Use of steganography to hide information in V2X communications
  o Patent: Privacy-preserving check of driving authorizations without stop
Summary

• V2X security, privacy and trust deserve attention in the near term
  o Industry – upcoming developments
  o Research – open challenges
• Existing state-of-the-art technologies call for a final step ahead
• In this talk, a short overview on security, privacy and trust in V2X has been presented
V2X security, privacy and trust overview

Dr. José María de Fuentes (jfuentes@inf.uc3m.es)
COSEC Lab
University Carlos III de Madrid