Privacy and Integrity Considerations in Hyperconnected Autonomous Vehicles

S. Karnouskos (SAP) and F. Kerschbaum (University of Waterloo)

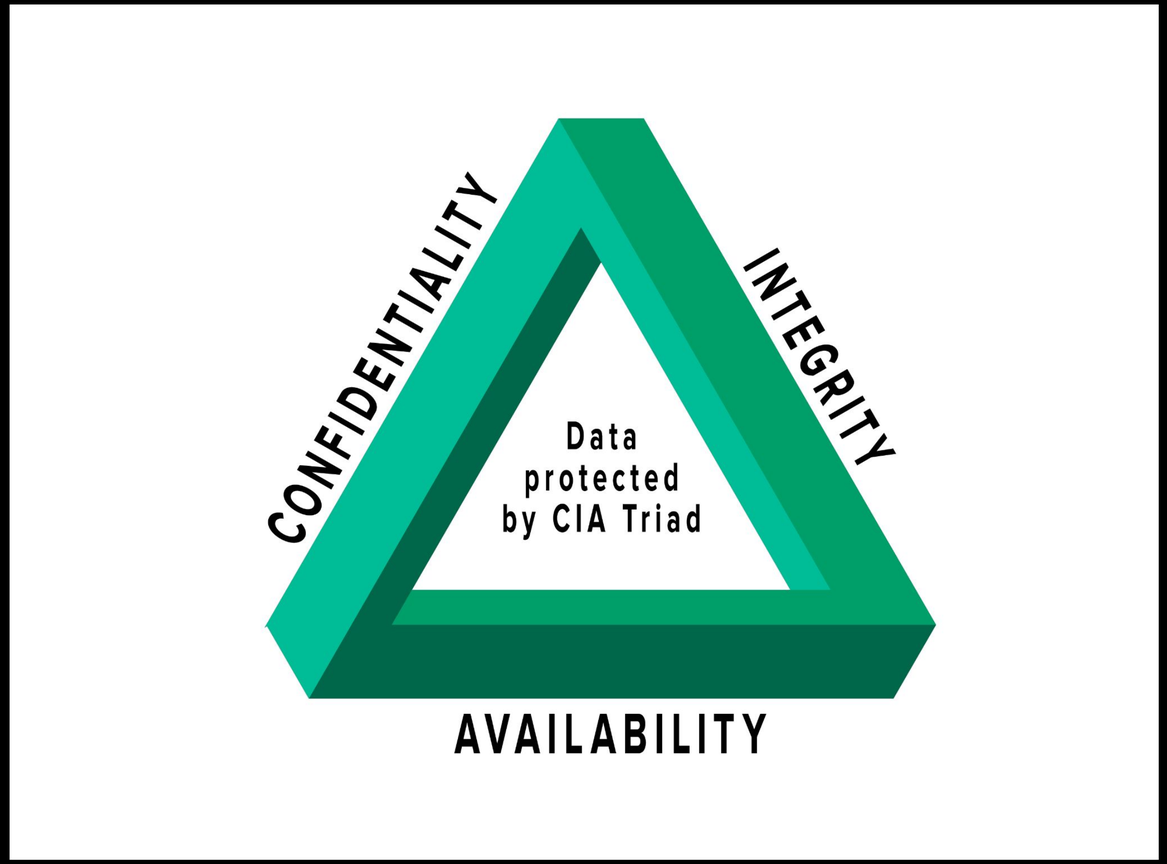
Presented by: Yuan Gao
12/01/2022

Acknowledgments: slide material derived from authors and internet.

Introduction

Problem of hyperconnected vehicles

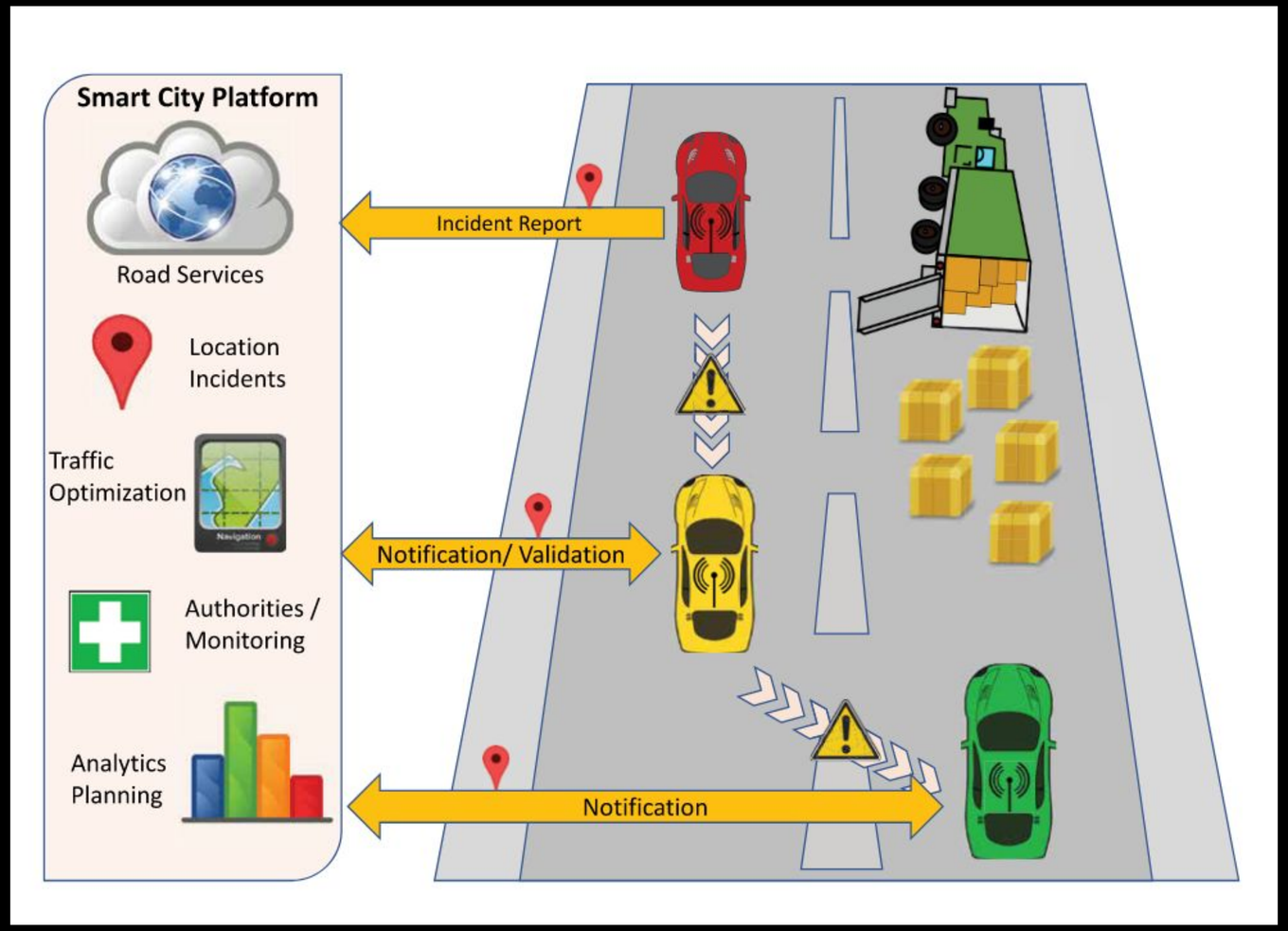
As hyperconnected vehicles at large and autonomous driving are relative new, security, trust, and privacy aspects are not well addressed



Inherent conflict in security objectives

- **In multistakeholder interactions the integrity of the sensed data is key toward ensuring a safe and stable system**
  - e.g.: smart meter readings are often wrong
- **Privacy is founded on the principle of data minimization**
  - led to the “privacy by design” principle

Example Scenario: Real-Time Map Updates



Autonomous vehicles in V2V/V2I

Example Scenario: Real-Time Map Updates

- **In-vehicle detection:** Such situational info will be eventually picked up by the hyperconnected vehicle sensor systems.
- **V2V:** A preventive measure would be to propagate such info as quickly as possible via V2V communication, realizing cooperative maneuver planning and cooperative driving
- **V2I:** A complementary measure would be that the vehicle uses its communication facilities (V2I) to inform the respective services that keep high-precision maps on that road segment.

The challenge of securing the future hyperconnected vehicles

- **Privacy and Service Offering:**
  - Computation on encrypted data
  - Data perturbation

- **Privacy and Data Integrity:**
  - Privacy-preserving reputation systems
  - Partial observability
  - Privacy and Service Offering

- Spontaneous Interactions: Context-Based Authentication
- Safety: Mandatory Access Control

Strawman security and privacy architecture

- An incorrect map can significantly increase the physical risks to passengers

- A centralized infrastructure, e.g., in the cloud creates the opportunity for effective mass surveillance and poses a threat to the passengers' privacy.

Strawman security and privacy architecture

- **Threats by the Update:**
  - Forged identification
  - Forged location
  - Forged event
  - Privacy

- **Threats by the Map Information:**
  - Bulk download
  - Unsafe map information

NOTE: The map service provider has two options of verifying the updated information: **passive and active.**

Threat	Countermeasure	Deployment Challenge
Forged identity	Anonymous credentials	Secure issuance
Forged location	Partial observability	Parameter setting
Forged event	Anonymous reputation system	Parameter setting, updates of cryptographic protocols
Privacy	Encrypted map updates	Currently infeasible due to data amount

Map Updates: Threats, Countermeasures and Challenges

Conclusion

- discusses upon the hypothesis that it is feasible to ensure integrity, while preserving privacy.
- various approaches that can be taken to strike the balance between “privacy by design” and added value offered by hyperconnected vehicles
- Sociotechnical aspects need to be adequately discussed and considered, if the visions of autonomous self-driving cars and their expected benefits are to materialize.

Q&A

Discussions

Any other possible solutions can be used for the callenage mentioned in the paper?

How many of you share your personal data with tech companies?