Safety and Security Aspects of Connected and Automated Vehicles

TNO Workshop

Alexandru C. Serban[1,2]

[1]Digital Security
Radboud University, Nijmegen

[2]Research Team
Software Improvement Group, Amsterdam

i-CAVE P6 Topics

- Functional Safety
- Security
- Software Architecture Design
- Software Quality

In the context of connected and autonomous vehicles.

The talk today will be a cocktail of these topics.

Our initial assumptions

- It's been some time since we've heard about a car software crash.
- Car manufacturers do a good job.
- Therefore, we concentrate on the impact of co-operative and autonomous features on classic platforms.

Safety

- Everything is centered around ISO 26262.
- ISO 26262 sees safety as a *functional property* of a system and enforces safe operation in response to *inputs*, *hardware failures* or *environmental changes*.

What lies ahead of ISO 26262?

Safety

- Everything is centered around ISO 26262.
- ISO 26262 sees safety as a *functional property* of a system and enforces safe operation in response to *inputs*, *hardware failures* or *environmental changes*.

What lies ahead of ISO 26262?

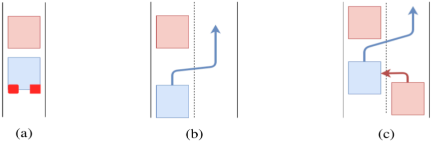
A definition of safety for autonomous:

- planning and execution of driving manoeuvres
- response to traffic events
- driving task fall-back

(A.C. Serban, E. Poll, J. Visser - Tactical Safety Reasoning, 2018)

Some challenges for tactical safety

We can not specify all traffic situations. So an autonomous car will have to *learn to reason* about a new situation.

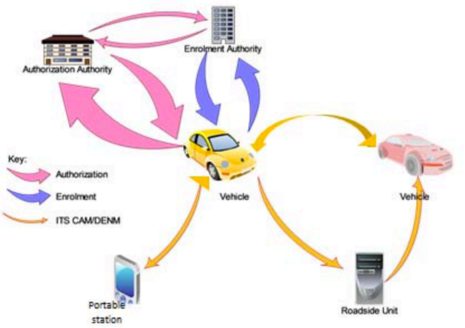


- Robust algorithms for environmental monitoring and understanding
- Human control transfer (if available)
- Reasoning about safety when accidents can not be avoided
- Align safety objectives between manufacturers

Environmental Monitoring/Understanding

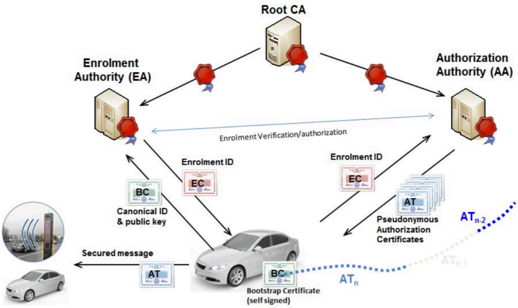
1. Exchange information between vehicles - co-operative driving
   - requires deployment of large infrastructure
   - performs less reasoning about safety
2. Perceive and understand the environment with dedicated sensors - autonomous driving
   - can be deployed only on one device
   - performs intense reasoning about safety

Information exchange between vehicles



- V2X, V2I is standardised by ETSI ITS
- The protocol embeds security primitives and APIs

Gaps in the ETSI ITS protocol


Root CA
Enrolment Authority (EA)
Authorization Authority (AA)
Enrolment Verification/authorization
Enrolment ID
EC
BC
Canonical ID & public key
Enrolment ID
EC
AT
Pseudonymous Authorization Certificates
AT$_{n-2}$
AT$_{n-1}$
Secured message
AT
BC
Bootstrap Certificate (self signed)
AT$_n$

- Mostly secure, except one gap
- Some messages can be replayed, leading to denial of service

(A.C. Serban, E. Poll, J. Visser - A Security Analysis of the ETSI ITS Communication Protocol, 2018)

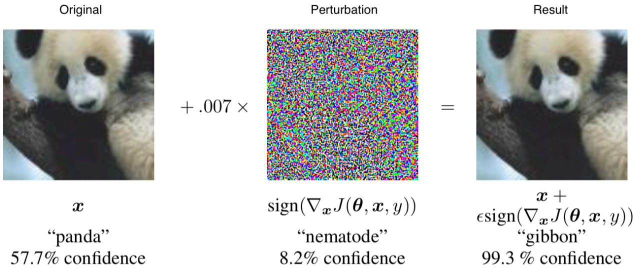
Is this all?

- The protocol is mostly secure, but its implementation can have bugs (with security/safety consequences)
- The security aspects in the protocol are not mandatory for service providers
- Some threats can be mitigated by separating sensitive software components (architecture design)

Understanding the environment

Relies heavily on computer vision algorithms.

Proven not robust:


Original
Perturbation
Result
$+ .007 \times$
$=$
$\boldsymbol{x}$
"panda"
57.7% confidence
$\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$
"nematode"
8.2% confidence
$\boldsymbol{x} + \epsilon\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$
"gibbon"
99.3 % confidence

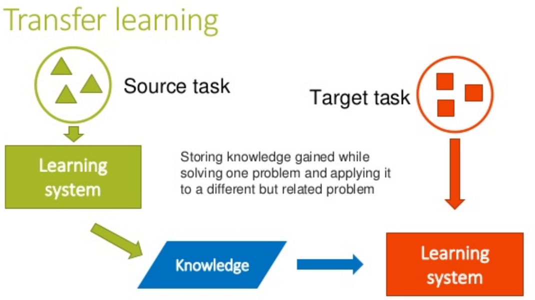
A.C. Serban, E. Poll, J. Visser - Adversarial Examples - A Complete Characterisation of the Phenomenon

Autonomous safety reasoning

What to do when a crash can not be avoided?

- Will probably rely on statistical learning algorithms
- Dependent on training data
- Hard to decide on safety objectives (or how to guide the learning process)
- Hard to verify/prove properties before deployment

Some work we do in this direction


Transfer learning
Source task
Target task
Learning system
Storing knowledge gained while solving one problem and applying it to a different but related problem
Knowledge
Learning system

Transfer learning from small, formally verifiable, models to large ones.

Can software architecture help?

From a system perspective, learning systems are treated as black boxes.

It is hard to reason about their safety or give guarantees needed in order to certify a system to a safety standard

Can software architecture help?

(A.C. Serban - Designing Safety Critical Software Systems to Manage Inherent Uncertainty)