



Institut
Mines-Telecom

If I secure my car, will it still brake?

Ludovic Apvrille
ludovic.apvrille@telecom-paristech.fr

Hack.lu 2014



In cars, they first care about safety, not security . . .
(*and privacy is hardly known ;-)*)

Insecure over-the-air and in-car channels

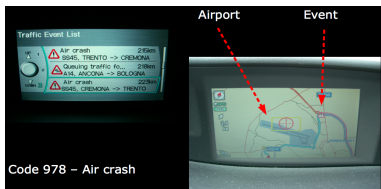
- ▶ Eavesdropping, replaying, impersonating, faking

Consequences

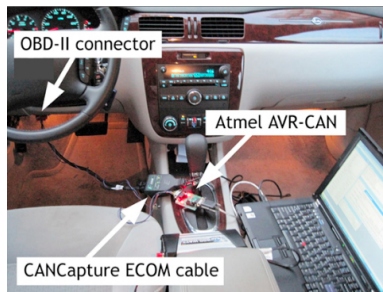
- ▶ Car safety: e.g., brake system corrupted
- ▶ Economy: e.g., toll bill overcharged
- ▶ Privacy: e.g., personal driver information disclosed to insurance companies

A few known attacks on cars

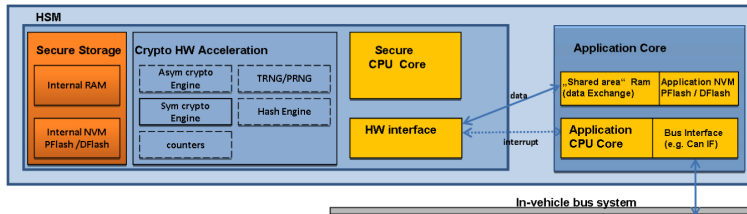
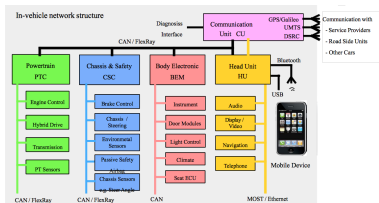
- ▶ Inject bogus traffic signals [Andrea,07]
 - ▶ Deception (bad weather, full car parking, road works, accidents,)



- ▶ Digital car hijacking [Koscher 2010]
 - ▶ Car control by malware
 - ▶ Changing parameters and firmware



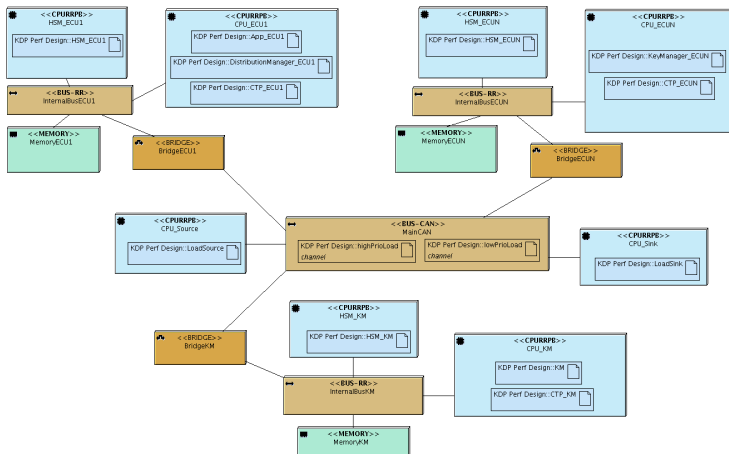
Towards secure car architectures



(BTW: Is attacking cars of the organizers part of the CTF?)

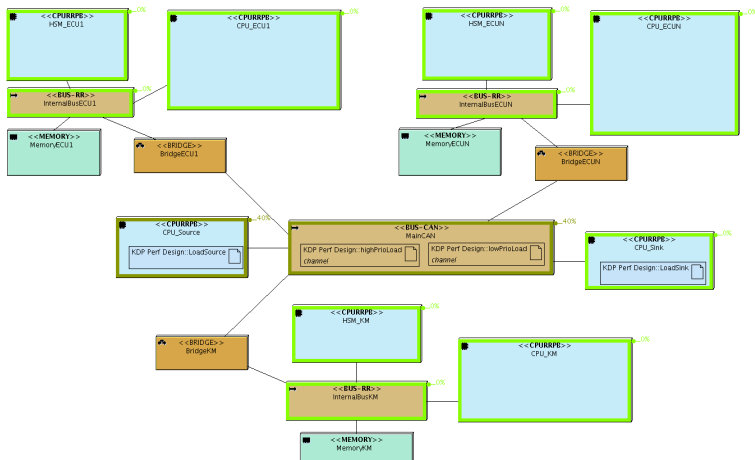
The car is now better secured ... But can it still brake on time?

Use of models and simulations (TTool/Diplodocus)



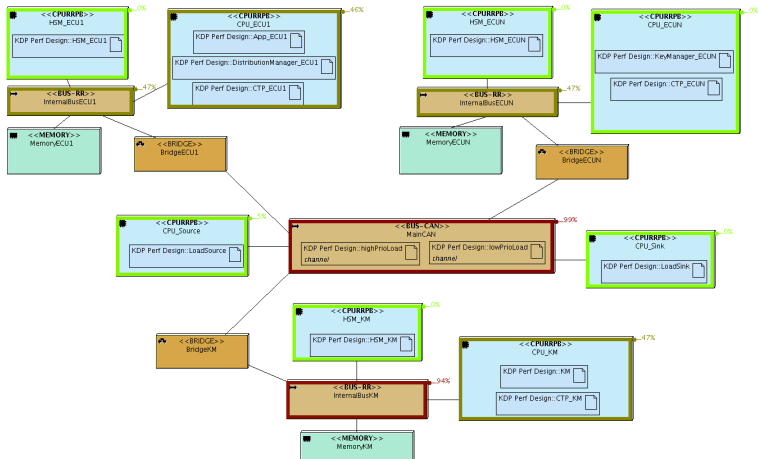
The car is now better secured ... But can it still brake on time? (Cont.)

Simulation WITHOUT security



The car is now better secured ... But can it still brake on time? (Cont.)

Simulation WITH security





TTool/DIPLODOCUS

ttool.telecom-paristech.fr



The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement EVITA no 224275 and TRESCCA no 318036.