PROTECTION AGAINST MILEAGE FRAUD

A WORLD IN MOTION
• An everyday scam

• Approaches
  • Raising consumer awareness
  • National database
  • European database
  • Odometer protection
• The European Commission estimates that mileage fraud affects 5%-12% of used car sales, a yearly economic impact of €5.6 billion to €9.6 billion within the EU

• Figures are far higher in cross-border used car sales

• Ultimately, consumers are the victims, as mileage fraud artificially elevates the cost of used vehicles, often by thousands of euros
• Devices to tamper odometers can be found on the internet for less than €150

• Tampering odometers is easy and untraceable

Tampering with the mileage – done in the blink of an eye!

1. Original mileage
2. Plug tampering device into the OBD interface
3. Key in false new mileage
4. Mileage changed – in all control units
Approaches

Raising Awareness

National/European Database

Technical Solution
FIA video animation explaining the issue
Raising Consumer awareness throughout Europe

Public event in Brussels

FDM, in Denmark

IAM, UK

Czech Republic reacted to UAMK initiative to look into mileage fraud

OEAMTC, in Austria

RACC, Spain
Endorsement by MEP Mathieu Grosch & MEP Saïd El Khadraoui

Demonstration with European Commission representatives
• National databases like Car-Pass in Belgium are a first approach to tackle the problem.

HOWEVER:
national databases cannot prevent cross-border fraud
In the frame of the European roadworthiness package it was decided to record the mileage at every periodical technical inspection and to set up a European-wide database.

HOWEVER:
the first vehicle periodical technical inspection is mandatory after 4 years, while most fraud occurs before.
• While odometer readings have become easier to read through OBD access, the lack of protection makes them very easy to tamper with.

• A way to fight mileage fraud is to protect the odometer reading and make tampering so costly that it gets unattractive. A very successful example was the introduction of anti theft systems.
• Since UNECE Regulation 18 (anti-theft of motor vehicles) mandates systems to protect vehicles from unauthorised use
• For instance, systems such as the Secure Hardware Extension (SHE) or Hardware Secure Module (HSM) are fitted in vehicles
• Those systems provide physical protection of ECUs from non-authorised access.
• They contain high-value cryptographic keys that block non-authorised access
• Vehicle manufacturers have started to protect modules of ECUs against theft and chip tuning, but not against mileage fraud
• Such protected modules of ECUs allow secure communication between the system components involved by long cryptographic codes and secure key storage
• Similar systems are used to secure e-ticketing or credit card chips
• Modules, such as SHE and HSM, are approved and installed by several vehicle manufacturers and can also be used to protect vehicle odometers from being tampered with
• The current technology for the protection of ECUs can be adapted e.g. anti-theft cryptographic key technology can be used to manage the security of the odometer protection.

• The necessary software development, programming and management, provided the protection system is already installed, would come at a comparatively low cost.
Technical specifications for odometer need to be anchored in the vehicle type-approval

- Describing the quality of the odometer reading
- Setting the level of protection against mileage fraud;
- Proposing a periodical improvement of the protection according to the technical development
- Using standardised processes like IT-safety certification ISO/IEC 15408.
Thank you for the attention

Luca Pascotto,
FIA Global Public Policy Manager,
lpascotto@fia.com

For more information:
www.fiaregion1.com
www.fia.com

http://walksafe.myworld2015.org