PTOLEMUS
Consulting Group

- Home
- About us
    - Our vision
    - Our management team
        - Frederic Bruneteau
        - Alexandra Willard
        - Hartmut Albers
        - Sergio Tusa
        - Frederic Lassara
        - Thomas Hallauer
    - Our experts & analysts
        - Matthieu Noel
        - Valerie Shuman
        - Maria Grazia Verardi
        - Meinrad Zeller
        - Justin Hamilton
    - Our events
    - Join us
    - Our blog
- Services
    - Strategy definition
        - Our experience
    - Business planning
        - Our experience
    - Due diligence
        - Our experience
    - Product development
        - Our experience
    - Partnerships & sourcing
        - Our experience
    - Business development
        - Our experience
- Clients
    - Smartphone vendors
        - Our experience
    - PND manufacturers
        - Our experience
    - Car OEMs / Suppliers and Insurance
        - Our experience
    - Commercial vehicle OEMs / Suppliers
        - Our experience
    - Mobile operators
        - Our experience
    - Content & Service providers
        - Our experience
    - Government & Regulators
        - Our experience
    - Financial institutions

        - Our experience
    - Transportation companies
        - Our experience
    - Sideways companies
        - Our experience
- ETC Global Study
    - Overview
    - Table of contents
    - Companies mentioned
    - Report highlights
    - Electronic toll collection timeline
    - ETC Supplier Rankings
    - Kapsch interview
    - Egis interview
- UBI Global Study
    - Overview
    - UBI supplier ranking
    - Table of contents
    - UBI Global Study 2013: Companies mentioned
    - Octo Telematics Interview
    - Progressive Insurance Interview
    - Q&A with Jonathan Hewett, Octo Telematics
    - Telematics insurance infographic
- Case studies
    - Location Study
        - Main results
        - Download
        - Details
        - Companies mentioned
        - Table of Contents
    - Usage Based Charging
        - Pay as You Drive
        - Road Pricing
    - The Mobility Ecosystem
- Contact

You are here: Home / Blog / OBD dongle hacking highlights 4 weaknesses

OBD dongle hacking highlights 4 weaknesses

September 14, 2015 by Thomas Hallauer
Filed under Blog

Leave a Comment

OBD hacking needs to be
considered by insurance carriers

We all saw the string of reports about various attacks on vehicles via the OBD dongle. Considering the device is now used in applications ranging from eco driving to road charging to usage-based insurance, we wanted to know the extend of the problem.

We caught up with **Mobile Devices Ingenierie (MDi)**, one of the dongle providers involved in an attack affecting their C4 OBD Dongle V2. From talking to them, we concluded that security threats could come from weaknesses at 4 levels:
– The device itself (if attacked physically)
– The cellular network
– The bluetooth (BT) connection between the smartphone and the OBD dongle
– The dongle’s architecture

The University of California (UCSD) had published a paper identifying what they could do with some of the C4 OBD Dongle on the market.
UCSD found some of the Metromile devices deployed in “development mode”, meaning security features completely disabled to allow 3rd parties developers build their own apps. They then hacked one physically by unsoldering the flash memory. After this long and arduous hack, they were able to control the OBD device wirelessly and send direct messages to the CAN of the Corvette they were testing.

They were also then able to use that first hack to access other devices remotely providing they were not using a SIM from wireless carrier using NAT (Network Address Translation) as it is most typically the case for Telematics. The details of the attacks can be found here

A bigger risk however comes from the Bluetooth dongles. MDi’s GSM-connected devices are generally well protected as long as the access from the server to the device is encrypted and firewalls over the inbound/outbound connection are put in place.

In the case of the bluetooth connection, there is only one communication protocol between a phone and any OBD devices from one specific brand. So hackers managing to access one would be able to find any of them from their phone and access them as long as the dongle is powered and in a 10 meters radius. (Note: most decent dongle companies use single sign-on secure silent paring. So in theory at least, it’s one dongle to one car only.)

Once the dongle is accessed, it could be used to send messages to the CAN and potentially open the door and start the car. Although, to do that hackers would need the OEM’s library for that specific car models and years which is not trivial. Also, OEMs are increasing the level of security around that area, making it more difficult to start a vehicle from the OBD port.

This is where the fourth security major flaw lies: on some low-end dongles, a lot of the intelligence actually resides on the smartphone app itself, particularly the CAN commands and updates have been seen to come straight from the phone over bluetooth with very limited security.
So as soon as a hacker controls the app, he can then control the dongle and use messages on the CAN to potentially open the door or activate the brakes.

Another potential risk is that hackers send diagnostics requests through the OBD port at a very high baud rate and crash the CAN. This would have dramatic consequences on the vehicle and passengers, as systems would not be able to communicate anymore. In the best scenario the engine will stall and the vehicle will slow down, while in the worst case, drivers won’t be able to control it anymore.

The effect of these recent hacks has been felt right across the industry but nowhere more clearly than on MDi themselves. Working with a new OEM partner, they were required to go through a full threat modeling process to ensure:

– that their cloud server cannot be attacked
– that security is embedded into all their development processes
– that they are prepared in the unlikely scenario of a physical attacks
– that dedicated measures are taken to protect access to car data, driver data and anonymisation

The process is then followed by a “penetration testing” where white hats have to hack into the suppliers systems.
Who can say that their dongle provider has gone through that in the UBI world?

MDi was not entirely to blame for the hack: the devices found by UCSD were unprotected for a “good” reason; like every other manufacturer, MDi had to send some of its devices to customers for the purpose of integration and testing. Regretfully some devices were then rolled out still unlocked.

Since the hack, MDi changed their policy on “open devices”. Instead of leaving it to the customer or integrator to close the devices before they are deployed, they now force their customers to use a “deployment security package” that secures the devices before they are distributed. At the same time, all the open devices on the road today have been patched with OTA updates.

The real difficulty is to balance the open and secure aspects of the device. An example of service that requires that balance is car sharing where the dongle needs to be able to open the cars doors while being accessed through BT by any new customers.
Closing the device to everything is not an option and manufacturers need to find ways to isolate the critical functions of the dongle from the open ones.

MDi’s architecture -like most top end providers- runs a virtual machine on its device that separates the Bluetooth commands from the CAN commands. It is like if there was 2 computers in the dongle,
– One, secured and accessing the cloud via encrypted protocols (SSL), used to access the car data and manage user data.
– The other, open and enabling developers and integrators to install their apps and customise the device to its required functionalities.

On the other hand, we believe OEMs should take responsibility for protecting the safety critical features of their cars. The OBD port is an open gateway to the CAN, yet it is mandatory and must be opened to all players. OEMs should develop security features to ensure that 3rd party dongles cannot send CAN requests affecting doors, ABS, airbags, brakes, accelerator or any security systems.

Ultimately we think OEMs will take charge of car data and ensure it stays in the hands of the drivers, allowing them to share part of the sets to get benefits. To enable secured services while running a fairly open platform, they will need to consider the 4 weaknesses above.

For their part, dongle providers should take full responsibility about what may happen after their devices gave access to the CAN. It’s not secure and it’s not meant to be public access. In fact, a direct CAN connection is in contravention of the vehicles homologation status and therefore is a “modification” to the car. OBD is in the public domain, CAN is not.

And for insurance carriers, the clock is ticking even faster;
– They should do a complete analysis of the risks involved at each supplier levels
– They should require from their dongle manufacturers that the relevant patches are sent to their active customers.

This article was the result of an interview with Mobile Devices’ product director as well as conversations with PTOLEMUS’ experts Matthieu Noel and Alexandra Willard

PTOLEMUS and Mobile Devices will be participating and speaking at the Telematics Insurance Europe conference on the 29-30 September

Be Sociable, Share!

+ MORE

Tweet Like 4 G+1 0 Share 29 • St

Tags:

Speak Your Mind

Tell us what you're thinking...

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

-

- ETC Global Study 2015

PTOLEMUS
Consulting Group

2015
EDITION

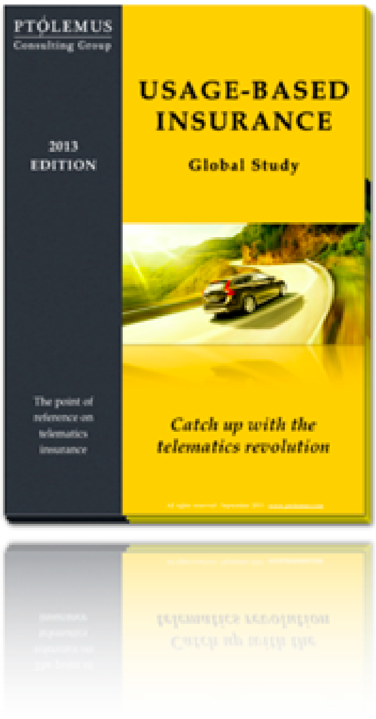
Free
abstract

The point of
reference on
electronic tolling

ELECTRONIC
TOLL
COLLECTION

*Transforming road
charging into a connected
vehicle service*

- 2013 Usage-based Insurance Study


PTOLEMUS
Consulting Group
2013
EDITION
USAGE-BASED
INSURANCE
Global Study
The point of reference on telematics insurance
Catch up with the telematics revolution