

Leadership and New Technologies. New Security Issues for Management of Internet Connectivity and Remote Control in Automotive Industry

~ Ph. D. **Cosmin Cătălin Olteanu** (University of Bucharest, Faculty of Business and Administration, Romania)

E-mail: contact@olteanucosmin.ro

Abstract: The main purpose of the paper is to illustrate the importance of implementing new security policies for infotainment systems in automotive industry. A car is full of technology and is easier today to control car systems through an internet connection linked to car system infotainment. This is how it is possible to gain control of critical car systems. More than 84% of users doesn't even know the risk of remote control of the car in the presence of Internet connection.

Key words: car infotainment, security of car systems, remote control of car systems

The automotive industry develops more and more advanced systems, sensors and actuators for cars. The sensors and actuators can communicate with car computers and their parameters can be changed in order to be more efficient.

In the modern cars there are a lot of systems, called infotainment where you can

set or view heat, air conditioning, fuel, parking sensors, rear camera, front radar and of course you can pair your mobile phone, you can listen to your favorite music or even see movies. Advanced systems have even Internet connection for your driving experience to be more fun or just for service stations to see what is wrong with your car.

Fig. 1 Infotainment system of a car



Source: http://img.omidoo.com/sites/default/files/stock/mytouch_infotainment_system.jpg

Fig. 2 Infotainment of a car with autonomous systems



<http://static4.businessinsider.com/image/528a898eeab8eafb4621ed51-960/infotainment-system.png>

There is common today even to have autonomous parking system and driving ones.

If we read again all those functions you can imagine that a car with Internet connection, an infotainment linked by OBD II or other system, to car computer, an electronic parking system that means actuators to wheel, brake and acceleration and you will finally see that someone with technical abilities can identify your car and control it by Internet remote. Someone can brake or accelerate when you don't want.

If we start digging information of these systems we will find information even for developing code for making our own onboard applications.

We have infotainment systems that are based on windows or by Linux kernels.

As a test, if your car has Internet connection and deliver Wi-Fi Internet to devices

just test your system if it has a ssh active service and you can make changes even to speed restrictions.

SSH into the car and Run following two commands:

```
/jci/scripts/set_lvds_speed_restriction_config.sh disable
```

```
/jci/scripts/set_speed_restriction_config.sh disable
```

<http://www.mazda3hacks.com/doku.php?id=hacks:disable-speed-restriction>

Or you can modify disclaimer time:

```
mount -o rw,remount /
```

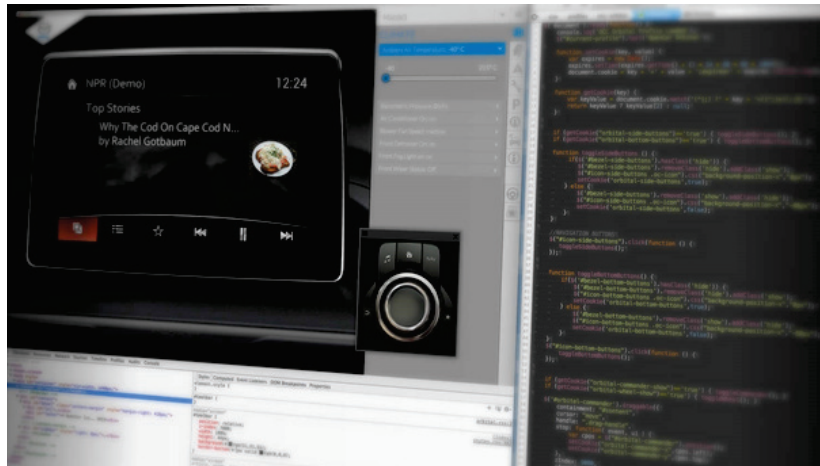
```
chmod 755 /jci/gui/apps/system/js/systemApp.js
```

```
sed -i 's/this._disclaimerTime.remaining = 3500/this._disclaimerTime.remaining = 100/g' /jci/gui/apps/system/js/systemApp.js
```

In 2014 at Consumer Electronics Show (CES), Mazda infotainment had presented a SDK Open Car software to see or to develop new applications. This showed us that a car

can suffer changes to their factory software. Some explaining procedures can be found in <http://www.mazda3hacks.com/doku.php?id=apps:opencar>

Fig. 3 Open Car SDK

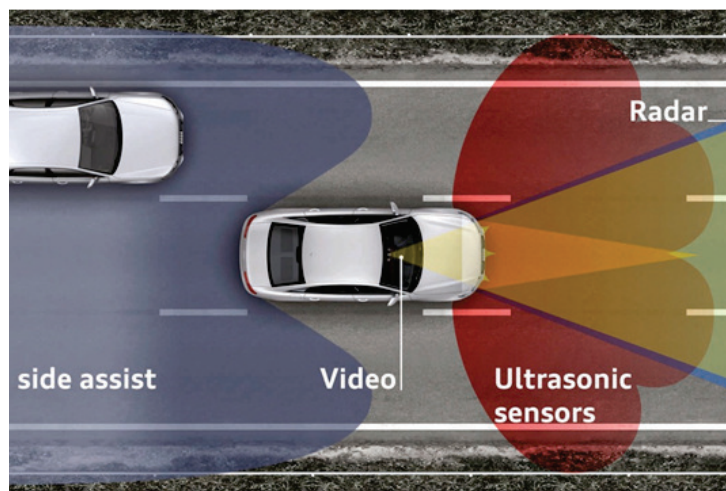


<http://www.mazda3hacks.com/doku.php?id=apps:opencar>

If you can control a system by ssh is easy to start or stop critical systems or to modify an actuator position.

An external application can be written and can be implemented to entertain the driver but no one can assure you that is the only thing it does.

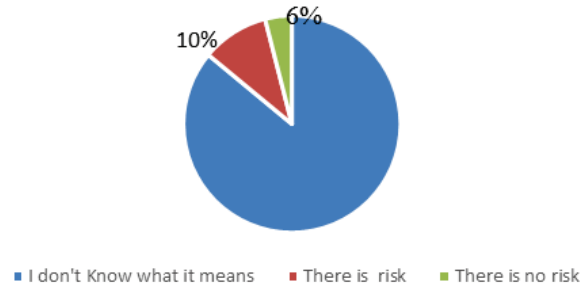
Fig. 4 Active Driving



<http://www.autotrader.com/car-tips/must-have-automotive-technology-for-2014-216735>

A survey has been applied to 50 drivers of a modern car and the results are the following:

Fig. 4 Survey of Car Infotainment Internet Security



The 84% of total users means that they even don't know that bad things can occur through Internet connection to their car.

Conclusions

Policies for the security of infotainment systems are only on the verge of developing and more research should be made on this

issue. Remote control of car systems opens the Pandora's box to hackers and new technologies in security like firewalls should be developed. Another issue is if infotainment should be linked to car critical systems and read their status or settings. On the other hand, the driver had to know what an open Internet Connection can do to his car and to his safety.

REFERENCES:

1. <http://www.autotrader.com/car-tips/must-have-automotive-technology-for-2014-216735>
2. <http://www.jdpower.com/cars/articles/car-news/modern-infotainment-systems-top-reported-problem-new-vehicles>
3. <http://techland.time.com/2014/03/04/the-wide-confusing-world-of-car-infotainment-systems/>
4. <http://www.mazda3hacks.com/doku.php>
5. <http://www.broadcom.com/blog/ces/in-car-infotainment-not-just-a-head-unit-any-more/>
6. https://en.wikipedia.org/wiki/Automotive_electronics