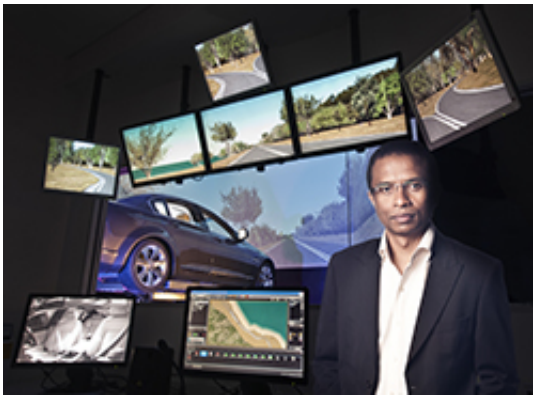
Car hacking: The security threat facing our vehicles

September 17 2014, by Sandra Hutchinson



QUT Professor Andry Rakotonirainy has researched the threat of car hacking.

The car of the future will be safer, smarter and offer greater high-tech gadgets, but be warned without improved security the risk of car hacking is real, according to a QUT road safety expert.

Professor Andry Rakotonirainy will speak at the Occupational Safety in Transport Conference (OSIT) on the Gold Coast on September 18-19 on the security threat facing drivers as vehicles become computers on wheels.

Professor Rakotonirainy, from QUT's Centre for Accident Research & Road Safety - Queensland (CARRS), has researched the security systems of existing fleet, future autonomous and connected cars and found there

was little protection against hacking.

"The security protection on cars is virtually non-existent, it is at a level of protection that a desktop computer system had in the 1980s, the basic security requirements such as authentication, confidentiality and integrity are not strong," he said.

"What this means is that as vehicles become more and more connected and autonomous, with the ability to communicate to other vehicles and infrastructure through wireless networks, the threat of cyber attack increases putting people's safety and security at risk."

Professor Rakotonirainy said while most vehicles built within the last decade had features allowing them to connect to the internet and communicate with devices within the vehicle, the development of intelligent transport systems meant future cars would be connected to wireless networks as standard and would offer a higher level of automation.

He said all new cars were equipped with technology, called CAN-BUS, located under the steering wheel, allowing anyone to check the health of a vehicle and to control it.

CAN-BUS provides access to the "brain" of a car.

"This CAN-BUS allows all microcontrollers within a car to communicate to each other and is accessible via a mere plug," he said.

"It can be used to control almost everything such as the airbags, brakes, cruise control and power steering systems. CAN-BUS can be accessed locally or remotely with simple devices.

"This is just the tip of the iceberg as future cars will feature a

tremendous mix of wireless networks and offer numerous opportunities to improve safety, entertainment and comfort.

"For example, cars will be wirelessly connected to other cars. If a vehicle stops ahead, a warning can be issued to drivers behind to slow down, or vehicles can automatically take control and slowdown without the driver's intervention.

"It will also be possible for vehicles to connect with infrastructure. For example, if a light turned red, but an approaching vehicle failed to slow, perhaps because the driver was distracted, a warning could be issued or action taken to automatically control the vehicle."

Professor Rakotonirainy said while these features had the potential to improve road safety, if hacked people's lives could be put at risk.

"If someone hacks into a vehicle's electronics via a wireless network and exploits the current security loophole, they can track or take control of it," he said.

Professor Rakotonirainy said it was vital for car makers, government and road safety experts to turn their attention to this global security threat.

"We need to be analysing the types of risk that that these intelligent vehicles are facing and work to provide a secure, reliable and trusted protection system," Professor Rakotonirainy said.

"A vehicle's communication security over wireless networks cannot be an afterthought and needs to be comprehensively considered at the early stages of design and deployment of these high-tech systems from the hardware, software, user and policy point of view."

More information: The OSIT conference, hosted by CARRS-Q,

brings together experts from all facets of transport safety including roads, rail, fleets, and mining to improve workplace health and safety. For more information on the conference, visit ositconference.com/

Provided by Queensland University of Technology