Smart car cyberattack warning as research finds flaws in security systems

October 16 2015, by Sandra Hutchinson

Calls to protect the future smart car.

How Australia acts today will determine the security and safety of driverless cars, autonomous vehicles and intelligent transport systems in the future, with QUT academics warning there is a risk of in-vehicle cyberattack without appropriate safeguards.

QUT information security expert Dr Ernest Foo is presenting his paper today at the 2015 Australasian Road Safety Conference titled Security Issues for Future Intelligent Transport Systems, highlighting the need to protect the future smart car.

The three-day conference hosted by QUT's Centre for Accident, Research & Road Safety - Queensland (CARRS-Q) on the Gold Coast finishes today.

"When talking about the car of the future we are talking about connected vehicles, vehicles that exchange information to facilitate warnings and improve on-road safety," Dr Foo said.

"The connection could be as simple as alerting a driver of an impending crash or as complex as allowing driverless cars on our roads.

"For vehicles to connect there needs to be a secure system to allow the safe transfer of information.

"Public key infrastructure is a security system that is already used to facilitate the safe transfer of information such as banking details.

"Without a secure system there is the potential for vehicles to receive misinformation or more critically for car hackers to maliciously take control of a vehicle."

Dr Foo said public key infrastructure was a combination of hardware, software, people, policies and procedures to create, manage, distribute, use, store and revoke digital certificates that supply public key encryption.

He said to date Australia had no guidelines to control public key infrastructure for intelligent transport systems.

"While the US and Europe have developed public key infrastructure guidelines, our research has found these guidelines have limitations when used in safety-critical vehicle environments," he said.

"The sheer amount of vehicles to be connected poses safety concerns, along with privacy, security and scalability under different traffic scenarios."

Dr Foo said public acceptance of connected and autonomous vehicles would depend on appropriate levels of security, and users' trust in a new intelligent transport system was crucial.

"The proposed systems in the US and Europe are too complex and pose potential risks for security and privacy flaws," he said.

"What we need to be doing in Australia is developing a system that offers an acceptable level of privacy, security and autonomy, while being flexible enough to work effectively in a complex environment."

Provided by Queensland University of Technology