On the road to secure car-to-car communications

September 14 2009

(PhysOrg.com) -- A European research project works out how to keep car-to-car data transmissions private and secure from malicious hackers.

You pull out to overtake a slow lorry. Suddenly the lorry swerves into your path. You hit the brakes hard and avert a full-on collision by a whisker.

Thanking your luck, you drive on. But little do you know that the crash was not prevented by your lightening reflexes. Instead it took clever collaboration between the lorry, your car and the cars behind.

While you were stuck behind the lorry, a communications system mounted on your car had connected with one on the lorry. When the lorry swerved, your car immediately knew that it was in your path and automatically applied the brakes.

The extra fraction of a second's braking before you took over made all the difference. And a multi-car pile up was prevented by similar messages as they were relayed from your car to the vehicles behind.

The future in the fast lane

ICT is driving forward a new era of more efficient and safer road travel for European citizens. Just as ABS brake technology dramatically cut accidents and fatalities in the 1980s, vehicle-to-vehicle and vehicle-to-

infrastructure communication will make our roads safer still.

But there is a big question to answer before the technology becomes widely adopted: is the communication link secure?

Imagine the chaos that a hacker could cause by sending bogus messages to vehicles. They could tell one car of an accident ahead, make the driver brake hard and actually cause an accident behind. They could invent fake traffic jams, encourage drivers to take alternative routes, then enjoy speeding along clear roads. Insecure communication systems could also let criminals track individual cars (e.g. celebrities, politicians) or harass drivers with unwanted alerts or spam messages.

“Car-makers and equipment manufacturers have to be certain that communication channels between cars and roadside infrastructure are secure from hackers and criminals and that their privacy is maintained,” explains Trialog’s Antonio Kung, coordinator of a European research project that has proposed a blueprint for secure car-to-car (C2C) connections.

The SEVECOM project brought together leading car and equipment manufacturers and ICT research institutes to agree on a security architecture that everyone could easily 'bolt on' to their proprietary C2C applications and ensure secure data transmission.

“The idea was to develop a general solution that conformed to all existing industry standards,” says Kung. “We have developed a way to add a security module to C2C systems.”

“We are interested in the communication 'tube' used to exchange messages among cars and between cars and infrastructure. Our project has looked at technologies and policies that will make the tube secure. We have not developed any new encryption systems,” Kung stresses.

“There's plenty of secure encryption methodologies, but what doesn't exist is the architecture. SEVECOM brought together stakeholders to agree what building blocks to use, where they should go and when they should be used.”

Automobiles anonymous

One of the project's most important proposals is that car communication should not use a fixed ID tag in its transmissions, which would open up the potential for cars to be tracked.

“Instead,” says Kung, “we think that cars should use pseudonyms which get changed several times, for example every time the ignition is turned on or at regular times during a trip. This would make malicious wireless communication tracking of individual vehicles almost impossible.”

The project was made more complicated because an international standard protocol for C2C communication has still not been agreed.

“We had to design a flexible architecture so that it could easily be adapted to conform to a standard once it has been agreed,” explains Kung. “The security module had to be independent of all the other communication technology and protocols involved in transmitting data.”

SEVECOM is now promoting its architecture to other EU-funded projects working in car-to-car and car-to-infrastructure communication systems, like CVIS. CVIS is developing integrated solutions for installation in the vehicle and roadside equipment to allow vehicles to interact with each other and with operators of road infrastructure. CVIS will use SEVECOM’s architecture to provide security in its applications.

More information: www.sevecom.org/

Provided by ICT Results