Beware of Hackers Controlling Your Automobile

18 May 2010, by John Messina

GMC's Yukon hybrid, control software logic analyzes hundreds of inputs every 10 milliseconds, including vehicle load, engine operations, battery parameters, and the temperatures in the high-voltage electric components. Credit: GMC

(PhysOrg.com) -- A team of researchers led by Professor Stefan Savage from the University of California, San Diego and Tadayoshi Kohno from the University of Washington set out to see what it would take to control an automobile's electronic control units (ECUs); what they found out may surprise you.

The researchers focused their attacks of the automobile's ECUs which are located all over a vehicle and control the workings of many car components. The hackers created software called 'CarShark' to monitor communications between the ECUs and used fake packets of data to carry out the attack.

Access to the automobile's computer system was done through the computer's access port that is standard among cars and used by mechanics to diagnose car's performance before servicing.

The researchers launched a series of attacks against the automobile's ECUs in a moving and stationary vehicle to determine how much control they could have on the car.

The researchers stated; "We are able to forcibly and completely disengage the brakes while driving, making it difficult for the driver to stop. Conversely, we are able to forcibly activate the brakes, forcing the driver forward and causing the car to stop suddenly."

The researchers found that practically every system in the car, such as brakes, light, engine, cooling, instrument panel, radio, and door locks, were vulnerable to attack.

The conclusion the team came to is that the vehicle's software was "fragile" and easy to sabotage. In some cases simply sending imperfect packets of data, rather than specific control code, was enough for triggering a response from the vehicle.

Hacking into an automobile's computer system is nothing new and has been happening since car computers systems have appeared. Typically hacking into a vehicle's wireless key system or a car's ECUs to boost engine performance has been happening for years.

As technology advances in automobiles, the risk grows greater that hackers will one day develop a means of getting into a vehicle's control system remotely that will cause serious safety concerns.

More information: Experimental Security Analysis of a Modern Automobile