Anomaly Detection on Vehicle Networks

Kyle Kastner

October 11, 2013

Presenter

Mark Brooks, of the Automation and Data Systems Division at Southwest Research Institute (Division 10).

What is the research trying to do?

This research is testing vehicles for software vulnerabilities, how those vulnerabilities can affect the performance of the vehicle, and how to detect if a software intrusion has occurred.

Articulate the objectives using absolutely no jargon

The objectives of the research were to find ways that attackers could get access to a vehicle's computer system wirelessly, and what methods could be used to see if the system had been compromised.

How is it done today, and what are the limits of current practice?

This is a brand new technology area, and while a few vehicle companies are testing against external attack, none of them (to the presenter's, and my, knowledge) are attempting to detect if software has been compromised internally.

What's new in the approach and why do we think it will be successful?

This approach has several new angles, and SwRI's expertise in penetration testing gives them a significant edge over previous research attempts. The application of monitoring to the internal communications of the vehicle is also very novel.

Who cares?

Every car manufacturer and vehicle owner in the world *should* care... whether they actually do is another matter.

If successful, what difference will it make?

This research will make vehicles safer and better defended against software intrusions. This is important, especially as we begin to move into the realm of fully automated driving and "smart" cars.

What are the risks and the payoffs?

The risks are fairly minimal, as this is an internally funded research project with no profit expectations. The payoff if successful would be enormous and greatly outweighs the risk.

How much will it cost?

Implementing the detection system, while not high cost, will be very expensive if installed in the millions of cars manufactured every year. The intrusion testing could be fairly cheap, as these will simply require updates to existing vehicle software before they are released. If a serious flaw was found, however, the cost to update all the cars currently "in the field" could be enormous.

Is it economically feasible?

This project is not yet economically feasible, largely due to the priorities of the vehicle manufacturing industry. While many people feel these types of vulnerabilities are incredibly dangerous and should be prioritized, the industry feels differently.