Report on: Modern Automotive Vulnerabilities: Problems, Causes and Outcomes

By: Stefan Savage, University of California, San Diego

Being a great automobile enthusiast, I found the talk very enthralling. Professor Stefan made the talk extremely eye catchy and there was not even a single moment that the mind shifted to some other things. The best thing of the talk was how in-depth knowledge of the inside functionality of the automobile was described as well as the complete procedure how the research took place. He also never failed to give the credit to his Masters students who helped him out with the same, which is refreshing as not many other professors it.

Getting started with the content, it was interesting to know the details of the car, the system, RAM which it uses, the diverse distributed system, detailed door system and how it operates. He describes in detail how the vulnerability of the software's may become an issue for us, for e.g. how connecting our phones with Bluetooth on the car, can lead to hijacking of the car or giving controls to unwanted people if they successfully hack our phones.

He tested how attaching a small device to the beneath of the car can give full access to person with software, i.e. one can easily control the doors, the system, breaks, acceleration etc. The professor not only just talked about these things but rather showed us the practical implementation of it. This is what made this talk separate itself from the rest of them. No matter as to where you are geo-located, if you have access to the software of the car, you can drive a car in san Francisco while sitting in Seattle.

This is a cause of worry, as if fallen into the wrong hands, it can easily cause havoc. There can be 3 main types of attacks namely: indirect physical where access from cell phones as people usually connect it with their cars, can be hacked easily. The second being short-range wireless being Bluetooth, Wi-Fi, which usually tells you about the collision or cars in your own lanes etc. Finally, the last attack being long range wireless like cellular, HD radio, PAT radio etc.

Just getting access is not sufficient for a car hijack. One needs to understand as how to how the car communicates with the entire system using a network. How the commands and orders are passes. So, this reduces the risk factor in the network hijacking. They researched on cars like Chevy Impala 2009, Toyota Prius 2010, Ford Escape and many more.

As a car is nothing but a hardware with at least a dozen microprocessors attached to it which networks internally, are the reason as to why there are vulnerabilities in the automobile system. The professor explained the internal structure of the network in detail as well. This is very interesting to know if you have keen interest in the functionality and associativity of the automobiles in today's time.

Professor also explained the main reason behind including computers in the automobiles. Briefly they are as follows: they are cost effective and have extremely high efficiency as compared to other materials. A car is nothing but a big distributed network with computers.

Overall, I found the talk very interesting. It has motivated me to create a software which can control the different parts of my car. I would love to see how the outcome finally comes. It would be really exciting to connect hardware with a software which you have written yourself .I look forward on more lectures from Professor Stefan.