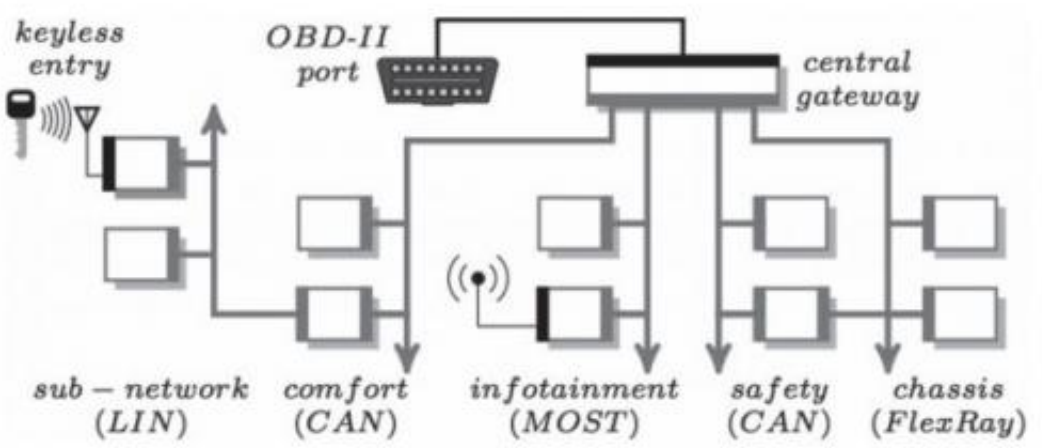
Time for cyberattack conversation on automated cars

November 13 2014, by Nancy Owano



Schematic of a typical in-vehicle network architecture of a modern automobile. Credit: *Intelligent Transportation Systems, IEEE Transactions on*

Jonathan Petit and Steven E. Shladover have written a paper for the *IEEE Transactions on Intelligent Transportation Systems* that sends a message about the potential of cyberattacks in automated vehicles.

With all the talk and design work under way for intelligent transport systems and connected cars, it is time to think about cybersecurity implications, they said, of automated cars. "The ITS industry has already been focusing much of its attention in recent years on the concepts of 'connected vehicles' (United States) or 'cooperative ITS' (Europe)," they said.

The two concepts are based on communication of data among vehicles (V2V) and/or between vehicles and the infrastructure (V2I/I2V). The authors focused their discussion on "systems that provide a high enough level of automation of the dynamic driving task that the driver is no longer required to monitor the driving environment for external threats. This means that the driver's attention is likely to be focused on other subjects while the vehicle is being driven, so that some significant time (at least multiple seconds) is likely to pass before the driver is able to re-engage to take any corrective actions that may be needed. The driver can therefore not be assumed to be available all the time as the ultimate fallback to ensure safety."

Regarding their paper, "Potential Cyberattacks on Automated Vehicles," IEEE Spectrum Senior Editor Philip Ross wrote that "They recommend far more layers of cyberprotection than manufacturers have thought necessary." He also commented that robocar engineers "will need to wrap smart cars in massively overlapping armor—what a soldier would call a defense in depth."

The authors said the study "identifies GNSS (global navigation satellite systems) spoofing and injection of fake messages as the most dangerous attacks (i.e., most likely or most severe)." In autonomous automated vehicles, GNSS play a key role in positioning vehicles on an accurate map. Therefore, manipulating GNSS data could provoke erratic and inaccurate maneuvers, which could endanger passengers' lives. Hence, they said, secure GNSS signal is mandatory.

Medium threats were identified as electromagnetic pulse (EMP), map poisoning, radar confusion, lidar confusion, infection of in-vehicle devices, and the manipulation of in-vehicle sensors.

Petit is a research fellow at University College Cork, Ireland. Shladover serves as program manager, mobility, with the California PATH

Program, Institute of Transportation Studies, University of California, Berkeley.

In September, a Bloomberg article addressed security concerns regarding hackers taking control of driverless cars. Quoted in the article, Wil Rockall, director of information protection at KPMG, London, said that a hacker could redirect traffic such that it could gridlock a city or even kidnap people. "The risk goes from being one of human error on the part of the driver or road user to being human error on the part of a developer."

More information: Potential Cyberattacks on Automated Vehicles, *Intelligent Transportation Systems, IEEE Transactions on* (Volume:PP , Issue: 99) ieeexplore.ieee.org/xpl/articl … jsp?arnumber=6899663

Abstract
Vehicle automation has been one of the fundamental applications within the field of intelligent transportation systems (ITS) since the start of ITS research in the mid-1980s. For most of this time, it has been generally viewed as a futuristic concept that is not close to being ready for deployment. However, recent development of "self-driving" cars and the announcement by car manufacturers of their deployment by 2020 show that this is becoming a reality. The ITS industry has already been focusing much of its attention on the concepts of "connected vehicles" (United States) or "cooperative ITS" (Europe). These concepts are based on communication of data among vehicles (V2V) and/or between vehicles and the infrastructure (V2I/I2V) to provide the information needed to implement ITS applications. The separate threads of automated vehicles and cooperative ITS have not yet been thoroughly woven together, but this will be a necessary step in the near future because the cooperative exchange of data will provide vital inputs to improve the performance and safety of the automation systems. Thus, it is important to start thinking about the cybersecurity implications of

cooperative automated vehicle systems. In this paper, we investigate the potential cyberattacks specific to automated vehicles, with their special needs and vulnerabilities. We analyze the threats on autonomous automated vehicles and cooperative automated vehicles. This analysis shows the need for considerably more redundancy than many have been expecting. We also raise awareness to generate discussion about these threats at this early stage in the development of vehicle automation systems.