Title: Cyber security issues in automobile and highway systems

Authors: J. Rowe and K. Levitt, UC Davis, and G. Kesidis, PSU

2014 National Workshop on Transportation CPS, 23-24, Jan., 2014

In our proposed presentation, we will discuss cyber security issues for automobile and highway systems. Such transportation systems, from individual cars to traffic management systems to proposed coordinated electric-vehicle charging systems and car-platoon management systems, increasingly rely on computer-communication networking. As these cyber-physical systems have strict safety requirements, their security must be ensured, at a minimum against threats that are considered to be routine by the cyber security community.

In the case of a single vehicle, a typical architecture involves a number of sensors and device controllers (each a "computer" in their own right) communicating via a single (wired) bus. For convenient maintenance, an OBDII port is mandated by law to be easily accessible from the driver compartment, which can be read and written without an security controls. Very low cost OBDII-Bluetooth bridge devices are available to consumers that, in principle, allow complete access to the sensors and controllers connected to the communications bus. Also communicating with the bus is a host computer providing the front-end interface to the passengers. This host computer provides, among other interfaces, a (wireless) Bluetooth interface, a USB port interface, an interface for reading data from CD and DVD rom disks, and perhaps even a cellular network interface for providing remote assistance. An overly complex, general-purpose operating system is often used for the host computer for programming convenience. By conventional means with minimal associated work-factors, exploits of known vulnerabilities of the host were demonstrated via wireless interface, and it was shown that unauthorized commands could be easily dispatched to the device computers within the car (e.g., brakes system) that could have drastic consequences to both car and driver[1]. Clearly, there was no “specification based" defense deployed among the (wired) networked computers within the car, e.g., prescribing and policing permitted commands under certain operational circumstances. Clearly, to prevent such "standard exploits", a far simpler, special-purpose operating system could be employed in the host (so that specification-based defense is feasible), in particular prescribing allowed behavior for all wireless interfaces (i.e., guards at the doors). Assuming available computational ability, communication within the car can be further secured by use of sound encryption, access control and runtime monitoring, all standard techniques in the field of cyber-security.

Such security rules of thumb could be extended to cellular wireless networks, and vehicular ad hoc wireless network (VANET) extensions (the latter far more challenging as it involves multihop communications among less trustworthy intermediaries, i.e., other cars), used by highway authorities to issue traffic alerts or, possibly in the future, explicit traffic commands to car host-computers. Also, in the future, alerts could pertain to the availability of charging stations that are in range of an electric vehicle considering its residual energy supply. Moreover, highly reliable (low delay/loss) VANET car-to-car communication is proposed for car-platoon management, again with the aim to improve fuel efficiency and reduce highway congestion. Also, highly reliable communication would be required for disaster response.   Clearly, in these settings, threats to availability of resources for wireless communications (i.e., denial-of-service threats) need to be addressed.

[1] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", *USENIX Security*, August 10–12, 2011.