Summary

The thesis addresses our research between 2010-2015 at Politehnica University of Timisoara, focusing on the design of cryptographic protocols for assuring security on in-vehicle buses (e.g., the CAN bus) and various automotive components or functionalities (e.g., tire pressure monitoring sensors, vehicle access control by smart-phones). This constitutes only a part of our research which targeted several directions ranging from theoretical cryptography and formal methods up to more practical subjects such as network and mobile systems security (these are briefly accounted in an overview section).

In the recent years, it has become increasingly obvious that vehicle evolution brings many similarities to that of modern computers. Not more than a century ago, computers were mere mechanical machines, then they turned into complex electronics and today they are loaded with complex software that (arguably) surpasses the complexity of the electronics behind it. This of course does not diminish the importance of the hardware without which they cannot function, but opens an entirely new vista for applications that have tremendously improved the quality of our life. Similarly, in the past decades, cars turned from mechanical devices into complex electronic devices and now they are loaded with hundreds of functionalities that are implemented in the software. These functionalities reside on dozens (even hundreds) of miniature devices, called Electronic Control Units (ECUs), that are spread inside the car and connected via a complex internal network. To make things even more interesting from a security perspective, part of this network is exposed to outsiders (i.e., potential adversaries) via wired channels (e.g., OBD ports) or via wireless interfaces (e.g., 3G, Bluetooth). The number of reported attacks has drastically ascended in the past years, with recent reports showing how one can lock the engine, steering wheels or the brakes, listen to passengers conversation, etc., even from hundred of miles away. The dull security landscape of cars from the past, dominated by small frauds (mileage modification, car theft, etc.), turned interesting in the recent years once it become clear that adversaries can takeover a car and use it at will.

Surprisingly, security mechanisms are completely absent from vehicular buses, starting from traditional ones such as the CAN bus (Controller Area Network) up to the most recent developments such as CAN-FD or FlexRay. This is mostly due to several technical challenges: low bandwidth and processing power, low cost margins, slow standardization, etc. Our work is focused on the design of efficient broadcast authentication protocols taking into account the three most promising techniques: TESLA-like protocols based on key chains and time synchronization, group keying protocols where keys are shared between groups of nodes and one-time signature (an alternative which is quickly discarded). While TESLA-like protocols proved highly efficient in sensor networks, this does not seem to be the case for in-vehicle networks as authentication delays need to be kept small and this raises synchronization problems, if we increase the delays we hit memory issues as large amounts of data need to be buffered. Moreover, the busload is also increased by the release of the

authentication keys. The most promising solution appears to be group keying, i.e., LiBrA-CAN. This protocol is based entirely on simple symmetric primitives and takes advantage of two interesting procedures which we call key splitting and MAC mixing. Rather than achieving authentication independently on each node, we share keys between groups of nodes which leads to a higher security level in case of compromised nodes forming only a minority. Based on practical arguments, we recognize this assumption to be realistic for automotive networks. Subsequently, amalgamating regular message authentication codes with systems of linear equations increases the chances for a forgery to be detected. We present several protocol variants that are extremely flexible and set way for different trade-offs on bus load, computational cost and security level, taking into account the most recent developments such as the recently released CAN-FD standard. To asses the efficiency of the proposed solution the proposed protocols were tested on automotive-grade micro-controllers as well as via simulation with industry standard tools. By the use of the CANoe tool we were able to simulate bandwidth allocation for the proposed protocols on state-of-art buses such as CAN-FD and FlexRay. The practical results proved our intuitions from the synthetic comparison of the protocols, i.e., group keying (LiBrA-CAN) is the preferred protocol design.

Departing from in-vehicle buses, there are so may other automotive sub-systems that are still deprived of security functionalities, e.g., wireless sensors inside wheels, car keys, etc. Moreover, even when components have certain security features, the security threats are far from being removed, e.g., car theft and millage modifications are still common issues. Clearly, a system cannot be more secure than its weakest link and we need to design security for these components as well. Here our results are dispersed and address several subsystems starting from the generation of random numbers on embedded devices, smart-phone based vehicle access and security for wireless sensors. We do present our most recent contributions in the security of wireless communication interfaces used in Tire Pressure Monitoring Systems (TPMS). Our work starts from designing an efficient authentication protocol based on lightweight cryptographic designs and block cipher based message authentication codes. The experimental results show that the proposed solution can be handled by real world sensors and is more efficient than related proposals. The works on smart-phone based car access and on randomness for automotive grade controllers, are recent developments and joint works with the industry.