CRYPTOGRAPHIC SECURITY FOR AUTOMOTIVE SYSTEMS

Author: Bogdan GROZA

Abstract

The thesis addresses 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). 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. 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 software. As an immediate consequence, 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 brakes, 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 signatures. While some of these protocols proved highly efficient in sensor networks, this does not seem to be the case for in-vehicle networks that require extremely small authentication delays for preserving the real-time nature of the system. To assess efficiency, 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. Finally, our results also address the security of several in-vehicle 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 alternative 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.

The full abstract at:
http://www.upt.ro/img/files/2015-2016/doctorat/abilitare/groza/j_summary_en_BGroza.pdf

Habilitation Commission

Prof.univ.dr.ing. Victor PATRICIU
Academia Tehnică Militară;
Prof.univ.dr.ing. Sergiu NEDEVSCHI
Universitatea Tehnică Cluj-Napoca;
Prof.univ.dr.ing. Vladimir Ioan CREȚU
Universitatea Politehnica Timișoara;
Prof.univ.dr.ing. Liviu MICLEA
Universitatea Tehnică Cluj-Napoca.