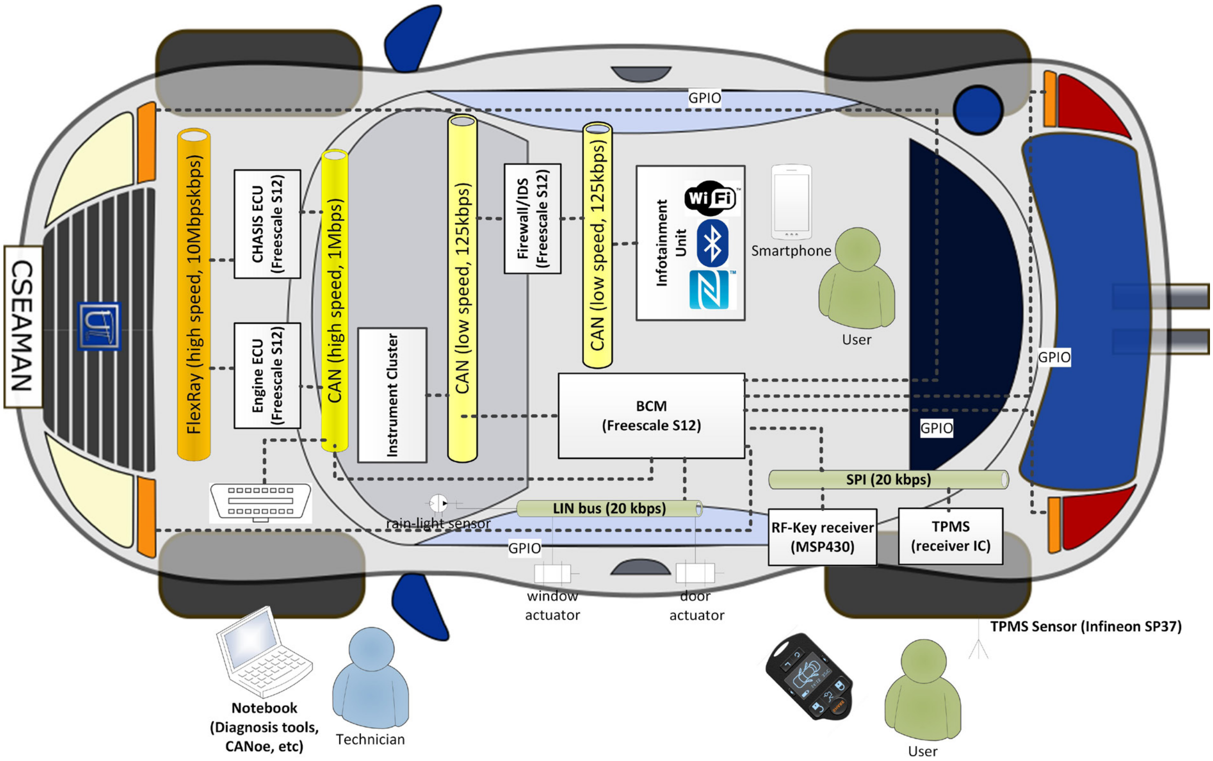
CSEAMAN - CRYPTOGRAPHIC SECURITY FOR AUTOMOTIVE EMBEDDED DEVICES AND NETWORKS

Goal of the project:

The design and analysis of cryptographic security solutions for automotive embedded devices and networks



Short description of the project:

The project aims at the design and analysis of cryptographic security solutions with applications in the automotive domain. Our main challenge is to accommodate cryptographic security on automotive-grade devices with low computational and memory resources that communicate over in-vehicle networks with constrained bandwidth. We focus both on wired and wireless channels that open cars to outsiders and bring a complex adversarial setup. Existing security sub-systems in cars (e.g., wireless keys, TPMS units) are also within reach.

Project implemented by

Research Group on Embedded Systems and Security, Department of Automation and Applied Informatics, Faculty of Automatics and Computers (UPT)

Implementation period:

Oct. 2015 – Sept. 2017

Main activities:

- Implementation and security analysis of cryptographic functions on automotive grade embedded devices, e.g., AUTOSAR compliant cryptographic libraries,
- Design and analysis of cryptographic protocols for wired in-vehicle networks, e.g., CAN bus, J1939, FlexRay, etc.
- Design and analysis of cryptographic protocols for wireless in-vehicle connectivity, e.g., RF keys, TPMS systems, etc.
- Implementation of an experimental platform for security critical subsystems inside the car: communication buses linking various ECUs with potentially insecure third-party devices (e.g. infotainment units)
- Risk analysis and security implications within new automotive paradigms: optimized traffic flows, vehicle-to-vehicle communications, etc.

Results:

- Comprehensive performance analysis of cryptographic primitives on automotive-grade controllers
- Analysis of fingerprinting and randomness extraction mechanism from SRAM state
- Design of new security solutions for wireless vehicle access
- Design of new security solutions for the CAN bus
- Security analysis and fixes for the J1939 commercial-vehicle bus protocol
- Analysis of traffic models with adversarial vehicle behavior
- Risk analysis and security implications for attacks on BCM units

.

Applicability and transferability of the results:

Various applications in the automotive industry for securing critical vehicular systems and networks, e.g., wireless keys, CAN bus, ECU fingerprinting, etc.

Financed through/by

Romanian National Authority for Scientific Research and Innovation (CNCS-UEFISCDI) Project No. PN-II-RU-TE-2014-4-1501

Research team

Habil. PhD. Eng. Bogdan Groza - director
Phd. Eng. Stefan Murvay (postdoctoral researcher)
Phd. Eng. Horatiu Gurban (postdoctoral researcher)
Eng. Diana Pop (PhD student)
Eng. Catalin Briciu (PhD student)
Eng. Tudor Andreica (student)
Eng. Alexandru Matei (student)
Inf. Roxana Farcasescu (PhD student)

Contact information

Assoc. Prof. Bogdan GROZA, PhD
Faculty of Automatics and Computer,
Bd. V. Parvan, No. 2, 300236, Timisoara
Phone: (+40) 256 403242
E-mail: bogdan.groza@aut.upt.ro
Web: http://www.aut.upt.ro/~bgroza/Projects/cSEAMAN