SECURITY ENHANCEMENTS AND VULNERABILITY ASSESSMENT FOR INDUSTRY-STANDARD NETWORKS (SEVEN)

Goal of the project

Most attacks on industry-standard networks rely on vulnerabilities. In this context, the SEVEN project aims to assess vulnerabilities in protocols not yet analyzed and to increase the security of industrial networks by proposing mechanisms to assure basic security objectives (e.g. authenticity, confidentiality or key management). The project also focuses on the design of intrusion detection systems. Finally, we also consider a performance impact evaluation of the introduction of the designed security solutions.

Short description of the project

Vulnerability evaluation and development of protection mechanisms for in industry-standard networks.

Project implemented by

Pal-Ștefan MURVAY (Project leader)
Bogdan GROZA (Mentor)

Implementation period

02/05/2018-30/04/2020

Main activities

The project is structured around three main activities.

1. The first main activity focuses on vulnerability assessment of industry-standard communication protocols. Our goal is to identify industry-standard communication-protocols that were not analyzed from a security perspective and identify potential vulnerabilities.Our first approach for enhancing the security of industry-standard communication protocols is the development of mechanisms for assuring basic security objectives such as: authenticity, confidentiality or key management.

2. A second approach focuses on designing intrusion detection mechanisms for the early identification of attack attempts.

3. Finally, we intend to provide an evaluation of the performance impact of the proposed mechanisms.

Results

The first phase of the SEVEN project focused on the identification of vulnerabilities in two industry-standard protocols, i.e., FlexRay and DeviceNet. The findings have been published as part of two conference papers:

[1] Pal-Stefan Murvay, Bogdan Groza, Practical security exploits of the FlexRay in-vehicle communication protocol, presented at The 13th International Conference on Risks and Security of Internet and Systems (CRISIS 2018), 2018.

[2] Pal-Stefan Murvay, Bogdan Groza, A brief look at the security of DeviceNet communication in industrial control systems, presented at The second Central European Cybersecurity Conference (CECC 2018), 2018.

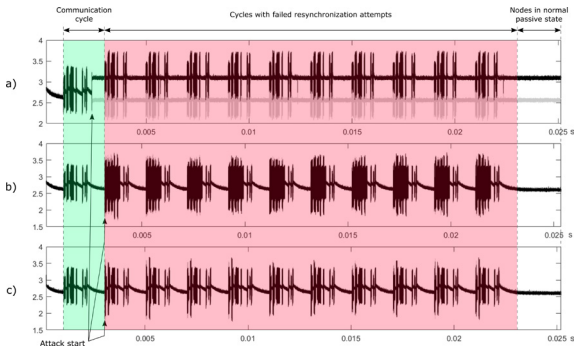

Figure 1. Three variants of the DoS attack for the entire communication.

We dedicated several lines of work to designing security mechanisms for enhancing the security of industry-standard protocols. The results obtained cover both secure communication mechanisms and intrusion detection systems for the Controller Area Network and FlexRay protocols. Papers presenting these results have been published in conference proceedings or journals:

[3] Pal-Stefan Murvay, Bogdan Groza, Accommodating Time-Triggered Authentication to FlexRay Demands, presented at The third Central European Cybersecurity Conference (CECC 2019), 2019.

[4] Camil Jichici, Bogdan Groza, Pal-Stefan Murvay, Integrating Adversary Models and Intrusion Detection Systems for In-Vehicle Networks in CANoe, presented at The 12th International Conference on Security for Information Technology and Communications (SECITC 2019), 2019.

[5] Pal-Stefan Murvay, Bogdan Groza, TIDAL-CAN: differential Timing based Intrusion Detection And Localization for Controller Area Network, accepted for publication in IEEE Access, 2020.

Applicability and transferability of the results

Our results add to the already known vulnerabilities of communication protocols used in industrial applications. Knowledge of the vulnerabilities is an important building block of designing proper security mechanisms for these communication protocols.

The proposed security mechanisms are efficient in preventing a series of spoofing and replay attacks as well as in the detection of attack attempts. These mechanisms focus on FlexRay, which was developed for the automotive industry and Controller Area Network, a communication protocol widely used both in the automotive domain and industrial control systems.

Financed through/by

This work was supported by a grant of the Romanian Ministry of Research and Innovation, CNCS - UEFISCDI, project number PN-III-P1-1.1-PD-2016-1198, within PNCDI III

Research Centre

Department of Automation and Applied Informatics

Research team

Assist. Prof. Stefan MURVAY, PhD
Prof. Bogdan GROZA, PhD

Contact information

Assoc. Prof. Pal-Ștefan MURVAY, PhD
Faculty of Automatics and Computers
Department of Automation and Applied Informatics
Address: Str. Vasile Pârvan, No. 2, Postal Code 300223, Timisoara
Phone: (+40) 256 403 242
E-mail: stefan.murvay@upt.ro
Web: http://www.aut.upt.ro/~pal-stefan.murvay/