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

Goal of the project

Since most attacks on industry-standard networks rely on vulnerabilities the SEVEN project aims to assess vulnerabilities in protocols not yet analyzed. For adding security to industrial networks we propose mechanisms to assure basic security objectives (e.g. authenticity, confidentiality or key management). The project will also investigate and design 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.

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.

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

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

Results

The results obtained in the first phase of the SEVEN project have been published as part of two conference papers. Both focus on the first main project activity, i.e., vulnerability assessment of industry-standard communication protocols.

Our first result covers the identification of vulnerabilities in the FlexRay communication protocol. We identified a set of denial of service attacks that can affect the entire communication or just targeted frames. We also found that FlexRay frames sent in the dynamic segment can be falsified.

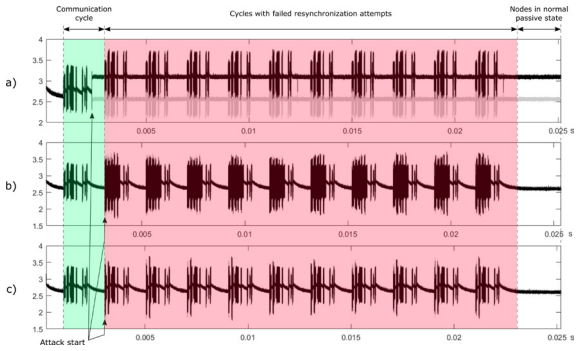

Figure 1. Three variants of the DoS attack for the entire communication.

A second line of research focused on the DeviceNet protocol. We found that DeviceNet is vulnerable to a set of denial of service attacks that can prevent a node from achieving communication on the network while not affecting the communication between other nodes.

Applicability and transferability of the results

Our results add to the already known vulnerabilities of communication protocols used in industrial applications.

Without proper mitigation mechanisms these attacks can be used by malicious parties to disrupt communication of safety critical systems in an automotive environment (in the case of FlexRay) or in an industrial control system (in the case of DeviceNet).

Knowledge of the vulnerabilities is an important building block of designing proper security mechanisms for these communication protocols.

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

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/