Bachelor Thesis

The group Power Systems Intelligence from OFFIS R&D division Energy has an announcement for an immediate bachelor thesis.

RTU Vulnerability Analysis Demonstration using a virtual vulnerable virtual RTU

vvvR, MSF

BACKGROUND:

This project will use docker-containers for the development, configuration and installation of the vvvR on laboratory hardware. The contained Linux-based system has to be extended by including versioned services with known vulnerabilities. The demonstration should make use of the general testing framework metasploit (MSF) to develop a full host compromise and functional modification of the target service. The produced artefacts are a customized MSF-exploit script, machine-readable specification of the vvvR as versioned source-code, alongside a thesis paper written according to scientific standards.

OBJECTIVE:

The objective of this thesis is to demonstrate the compromise of an RTU demonstrator in the SESA-Lab. The striving hacker should setup a versioned vulnerable virtual RTU (vvvR) and demonstrate how the compromise of one common service leads to compromise of a critical target service runnning on the vvvR.

YOUR PROFILE:

- We expect the student to bring sufficient experience with fundamental programming languages, especially C and Assembler, to understand how to modify existing processes.
- Basic abilities to handle the scripting language Ruby have to be acquired.
- Clean Code Development processes are mandatory.
- Technical curiosity and a „security mindset“ are crucial to successfully finish this thesis.

CONTACT:

Dr. Lars Fischer
OFFIS - Institute for Information Technology
Escherweg 2, 26121 Oldenburg
Tel: 0441 9722-422
Mail: lars.fischer@offis.de