Bachelor / Master Thesis

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

Proof-of-Concept ICS Feldbus Exploit

ICS, MSF

BACKGROUND:

Key target of this project is to demonstrate known vulnerabilities of ICS communication protocols. The demonstration will exploit lack of integrity protection, lack of secrecy protection and the injection of malware. On the Master level, the work will generalise the demonstrated exploits and provide automation support as well as substantial research into tools, threat context and mitigations. This thesis provides the opportunity to gain experience as security researcher in the field of industriel control systems (ICS). The final result is a demonstration on different categories for attacks, to demonstrate an ICS attack on a damn-vulnerable control device using ICS protocols.

OBJECTIVE:

The expected result is a setup of three devices, two devices communicating and one malicious device interfering with the communication. The demonstration should show the shortcomings of „classical“ ICS communication protocols at the field level, e.g. IEC 60870-5-104. The proof-of-concept should be implemented using the metasploit framework (MSF) which provides a wide set of tools to support post-compromise. The MSF also provides fundamental support for the -104 protocol.

The prospective Bachelor/Master Thesis has to be described in a proposal agreed between advisors and student.

YOUR PROFILE:

- Command of the Ruby programming language or ability to learn this quickly.
- Basic knowledge network communication, protocols and implementation.
- Willingness to acquire knowledge of the ICS domain, especially on power systems.
- Ability to work in a team, taking up responsibility for the project.

CONTACT:

Dr. Lars Fischer
OFFIS - Institute for Information Technology
Escherweg 2, 26121 Oldenburg
phone: +49 441 9722-422
E-Mail: lars.fischer@offis.de

Björn Siemers
OFFIS - Institute for Information Technology
Escherweg 2, 26121 Oldenburg
phone: +49 441 9722-457
E-Mail: bjoern.siemers@offis.de