Attacking Contiki OS

Bachelor or Master Thesis – Studien oder Diplomarbeit

So far, attacks on sensor networks mainly focus on the link, network and transport layer. Malicious behavior like flooding, packet dropping or impersonation is widely studied. However, also the operating system (OS) could be used as a starting point for exploitation. A typical OS for sensor nodes is Contiki, its development began in 2003. Contiki is an open source, highly portable, multi-tasking operating system. Your challenge is to analyze Contiki for security vulnerabilities.

Task Description

Your task is to first analyze the state-of-the-art of security mechanisms for operating systems in wireless sensor networks. After getting familiar with Contiki, you would look for security vulnerabilities such as buffer overflows. Your thesis concludes with an evaluation of the security provided by Contiki.

Requirements

- All organizational requirements for the thesis are fulfilled
- Knowledge in reverse engineering
- Optional knowledge of Assembler
- Keen interest in wireless sensor networks and security issues

Start and Duration

As soon as possible with flexible duration (depending on the respective study plan)

Dipl. Wirtsch.-Inf. Michael Riecker
Secure Mobile Networking Lab – SEEMOO
michael.riecker@seemoo.tu-darmstadt.de

Mornewegstraße 32
64293 Darmstadt
06151 16 70925