Long Term Cybersecurity research
Summaries of projects granted in the first NWO call for proposals (2012)

Project number	CYBSEC.12.008 / 628.001.005	
Main Applicant	Prof. dr. B.P.F. Jacobs	Radboud Universiteit Nijmegen Faculteit der Natuurwetenschappen, Wiskunde en Informatica Computer Science
Project title	OpenSesame: opening backdoors on embedded devices	

Scientific summary

Networked embedded devices like routers, switches, firewalls, sensors and actuators are part of our critical infrastructure. These devices are often assembled and programmed overseas -- beyond our control -- and placed within our trusted networks or even used for military applications. But can we really trust them? There have been several incidents where backdoors have been found in the firmware (also on silicon) of these devices. Such a backdoor allows an adversary to gain (remote) access to the device.

The OpenSesame project addresses this problem by developing novel automated techniques to test the software and firmware of embedded devices for the presence of such backdoors. Standard protocol fuzzing techniques -- like feeding programs invalid or random data to test for unexpected behavior –- are not very effective as the chances of hitting the right input are tiny. Our approach consists of first recovering the (read-protected) firmware from the device. Having access to the firmware enables us to apply smarter techniques, like symbolic execution, to backdoor detection. Symbolic execution searches for the presence of a backdoor in any possible execution path. This technique does not scale very well when addressing large computer programs. However, embedded devices -- with their smaller code bases -- are exactly the right target for symbolic execution.

Applicable NCSRA theme

- Operational cyber capacities