Long Term Cybersecurity research
Summaries of projects granted in the second NWO call for proposals (2014)

Project number	CYBSEC.14.014 / 628.001.012	
Main Applicant	Prof. dr. ir. B.R.H.M. Haverkort	Universiteit Twente Faculteit der Elektrotechniek, Wiskunde en Informatica Ontwerp en Analyse van Communicatiesystemen (DACS)
Project title	More secure SCADA networks through self-awareness (MOSES)	

Scientific summary

SCADA (Supervisory Control And Data Acquisition Systems) networks control physical processes, such as electricity grids, and are increasingly vulnerable to cyber attacks, due to unauthenticated and non-encrypted communication protocols. However, the continuous operation (dependability) of the physical processes is of utmost importance to society and industry. SCADA security has mainly been considered separately from the physical processes they control, even though attacks and countermeasures have a direct impact on the physical process. We propose to use predictive knowledge of the physical process (i) to improve intrusion detection capabilities, (ii) to assess the impact of security breaches, and (iii) to justify countermeasures.

The key idea of this proposal is to build process-aware intrusion detection techniques for Smart Grids, which requires, next to state-of-the-art network intrusion detection, an accurate model of the physical processes that can be evaluated in real time. Due to the complex nature of Smart Grids, the model of the physical process has to combine discrete and continuous characteristics with stochastic behaviour (so-called 'stochastic hybrid models'). This model is then combined with a model that describes 'normal' network traffic. Together this allows for anomaly detection in both the network traffic and the behaviour of the physical system.

This so-called self-awareness monitor (SAM) will detect malicious behaviour that cannot be detected solely from SCADA traffic. Furthermore, it can predict future behaviour of the smart grid and quantify the impact of security breaches and different counter-measures on the physical process.

Applicable NCSRA themes

- Malware and malicious infrastructures
- Attack detection, attack prevention and monitoring