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

Project number	CYBSEC.12.017 / 628.001.009	
Main Applicant	Prof. dr. F.W. Vaandrager	Radboud Universiteit Nijmegen Faculteit der Natuurwetenschappen, Wiskunde en Informatica Institute for Computing and Information Science
Project title	Learning Extended State Machines for Malware Analysis (LEMMA)	

Scientific summary

A central challenge in detecting and analyzing malicious behavior on computer networks, eg. due to intrusions or botnet infections, is how to make sense of the vast amounts of data generated in monitoring such systems. The LEMMA project will develop automated tools to tackle this challenge by combining three innovations in learning technology:
1. state machine learning methods that are able to learn timed state machine models with parameters,
2. methods for learning these models from large amount of streaming data, and
3. fusion of information contained in models learned a different network locations.
This unique combination of innovative techniques can then be used to analyze patterns in the traffic of large and distributed networks, to detect suspicious activity, to locate infections, and to develop behavioral fingerprints of malicious (or normal) traffic. We believe that the time and technology is ripe for this project, as experiments in automated analysis of network data have already shown interesting results, despite using fairly basic learning techniques, and state machine learning has reach the stage where it can cope with systems of the required size and complexity.
The consortium combines expertise in states machine learning and security at the Radboud University, expertise in information fusion at Thales, and a vast experience in analyzing network traffic at Madison-Gurkha, Thales, and NCSC.
The research in LEMMA is centred around two main representative case studies; additional use cases are available from end-users SURFnet and the WODC at the Ministry of Security and Justice.

Applicable NCSRA theme

- Malware