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

Project number	CYBSEC.12.006 / 628.001.004	
Main Applicant	Prof. dr. S. Etalle	Technische Universiteit Eindhoven Faculteit Wiskunde en Informatica Informatica
Project title	Visualization and deep protocol analysis to detect cyber espionage and targeted malware (SpySpot)	

Scientific summary

Cyber-attacks have grown in number and sophistication, achieving unprecedented success in reaching their target. Advanced Persistent Threats (APTs) such as data exfiltration attacks are both dangerous and difficult to detect. These targeted and stealthy attacks using specifically developed malware circumvent classical detection systems based on signatures or statistical anomalies in network traffic. Only by looking in detail at the actual content of communication it would be possible to detect APTs. A method is thus needed to analyse the huge amount of data involved in an effective way. SpySpot proposes a solution which combines deep packet analysis with visualization of the analysis results enabling an end user to easily spot anomalies created by APTs like digital espionage. While automated analysis is needed to manage the huge amount of data, no automatic method can match the ability of the human mind in recognizing deviations and evaluating these. It is thus important to integrate automated analysis with visualization of results for human-based evaluation.
In the deep packet analysis the meaning of communication is recovered using protocol syntax and semantics, abstraction brings additional structure to this meaning and anomaly detection finds patterns deviating from the norm. The visualization takes the results from the automated analysis, presenting them to the end user. The user can, in an interactive way, investigate potentially harmful anomalies, get more in-depth information, tweak the analysis based on experience, and provide feedback on the discovered anomalies, such as discarding harmless ones in future traffic.

Applicable NCSRA theme

- Malware