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

Project number	CYBSEC.14.029 / 628.001.018	
Main Applicant	Prof. dr. ir. A. Pras	Universiteit Twente Ontwerp en Analyse van Communicatiesystemen (DACS)
Project title	D3 - Distributed Denial-of-Service Defense: protecting schools and other public organizations	

Scientific summary

The goal of this project is to develop an architecture to detect and mitigate Distributed Denial of Service (DDoS) attacks on public organizations, e.g., schools. Since summer 2013 the number of such attacks has increased rapidly, primarily due to availability of booters, i.e., web-based facilities that offer “DDoS-as-a-service”. Booters find their origins within the Internet gaming community, and can be used for a few euros by people without any technical skills. Since booters use general Internet services such as DNS and NTP to amplify their attacks, they can operate without an underlying botnet.

Although DDoS attacks are well-known in literature, it took the Wikileaks “operation payback” (2010) until the general audience understood the potential power of such attacks. Since then we've witnessed attacks on banks and crucial Internet services; some of these attacks even reached traffic peaks of 400 Gbps. Since summer 2013 the Dutch Research Network provider (SURFNet) sees a trend that students use booters to attack schools, often at times of exams. Also other public organizations and services, e.g., tax offices, DigiD, municipalities, hospitals are increasingly being targeted.

The novel approach of this project is to detect DDoS attacks at an early stage, within the core network. The scientific contribution is in two areas. First, Software Defined Networking (SDN) principles (OpenFlow) will be applied to re-route at an early stage attack traffic towards filtering systems that employ sophisticated anomaly detection mechanisms (e.g., HMM and SVM). Second, business modeling will be an integral part of the research, including economic, regulatory and ethical aspects.

Applicable NCSRA themes

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