Determining the effectiveness of countermeasures against cyber attacks

Ralph Koning, Ben de Graaff, Robert Meijer, Cees de Laat, Paola Grosso

SARNET

SARNET, Secure Autonomous Response NETworks, is a project funded by the Dutch Research Foundation. The University of Amsterdam, TNO, KLM, and Ciena conduct research on **automated methods against attacks** on computer **network infrastructure**.

Autonomous Attack Mitigation

The **SARNET control loop** continuously monitors the network using observables. When an attack starts, metrics **violate** the baseline of certain **observables.** The network **responds autonomously** using the countermeasures that are available.

Using VNET[1], we emulated **three types of attack**: DDoS, Password Bruteforce, and CPU utilisation, on a virtual overlay network. We implemented **four responses** to these attacks: placing filters, increasing link capacity, a CAPTCHA, and a honeypot. To **decide** we currently use **a rule based system** that maps the response to the attack. For each of the responses we recorded the intervals ***time_to_detect***, ***time_to_implement*** , and ***time_to_recover*** in relation to the attack size.

[1] Koning, R., de Graaff, B., de Laat, C., Meijer, R., & Grosso, P. (2016, June). Interactive analysis of SDN-driven defence against distributed denial of service attacks. In *NetSoft Conference and Workshops (NetSoft), 2016 IEEE* (pp. 483-488). IEEE.

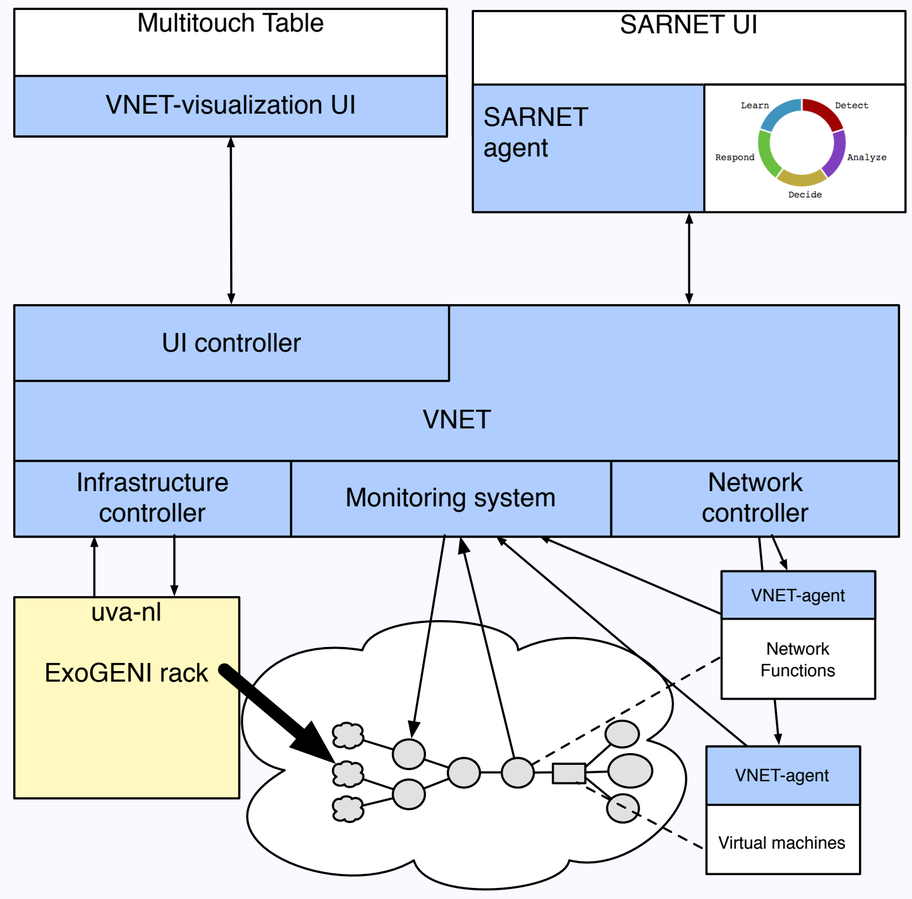

Fig. 1 Overview of the VNET framework
VNET uses a network controller and monitoring system to interact with the virtual network. The SARNET agent implements the control loop and has the knowledge to implement the countermeasures

Impact and Effectiveness

We define the **Impact** as the integral (blue triangle) in the graph. The impact is effectively the loss off service between detect and recovered. **Effectiveness** can be determined by adding the cost of the countermeasure.

Impact and effectiveness can provide the basis for a **standardised** and agreed upon **set of metrics** when comparing different SDN-based response systems. They are also **necessary inputs for learning** and **choosing the best suitable countermeasure** to achieve more advanced autonomous responses against cyber attacks.

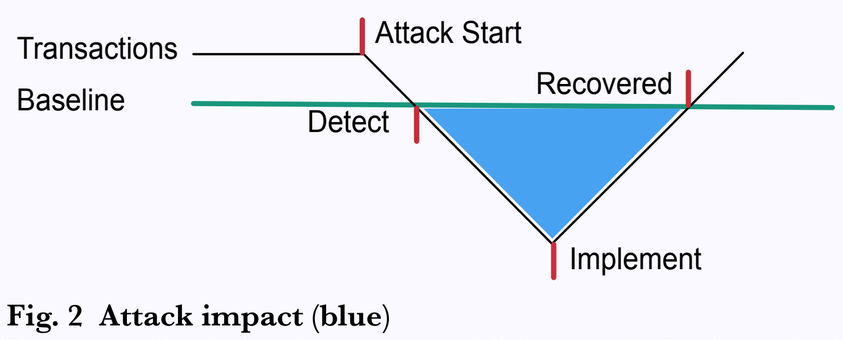

Fig. 2 Attack impact (blue)
Impact can be depicted on a graph with time on the horizontal axis and the amount of transactions on the vertical.

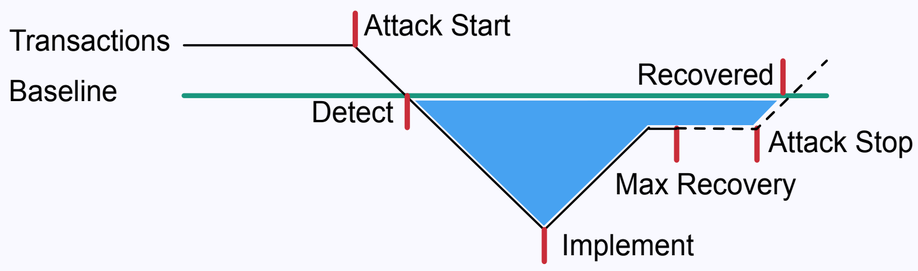

Fig. 3 Attack impact (blue) with partial recovery
In case the countermeasure does not provide full recovery we can still determine the impact and rank the defence by considering the distance between max recovery and the baseline.

Ralph Koning <R.Koning@uva.nl> | http://sne.science.uva.nl | http://www.delaat.net/ | http://sarnet.uvalight.net

University of Amsterdam · SNE · NWO Netherlands Organisation for Scientific Research · COMMIT/ · TNO innovation for life · AIRFRANCE KLM · ciena · ExoGENI