# Autonomous mitigation of Cyber Attacks

## Demonstration at Ciena booth #2523

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

## 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

In this demonstration we let the viewers **initiate one of the pre-implemented attacks**. The touch interface shows the virtual **network** to attack and **attack controls**. An additional **metrics screen** provides various metrics of the network and displays a simplified **SARNET control loop**. When these metrics **violate** certain **observables** the network **responds autonomously**.

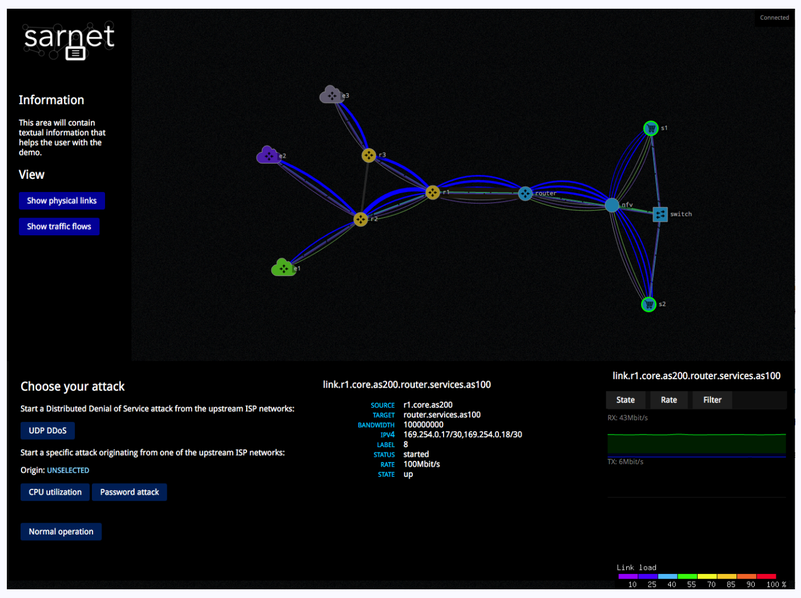
The **defences** are implemented by **deploying Virtual Network Functions** (VNF) between attackers and the service.
When a defence is initiated, a VNF is started as a **container**, the underlying **Software Defined Network** then directs the attack traffic to the VNF that can apply **additional monitoring** or **mitigate** the effects of **the attack** traffic on the service.

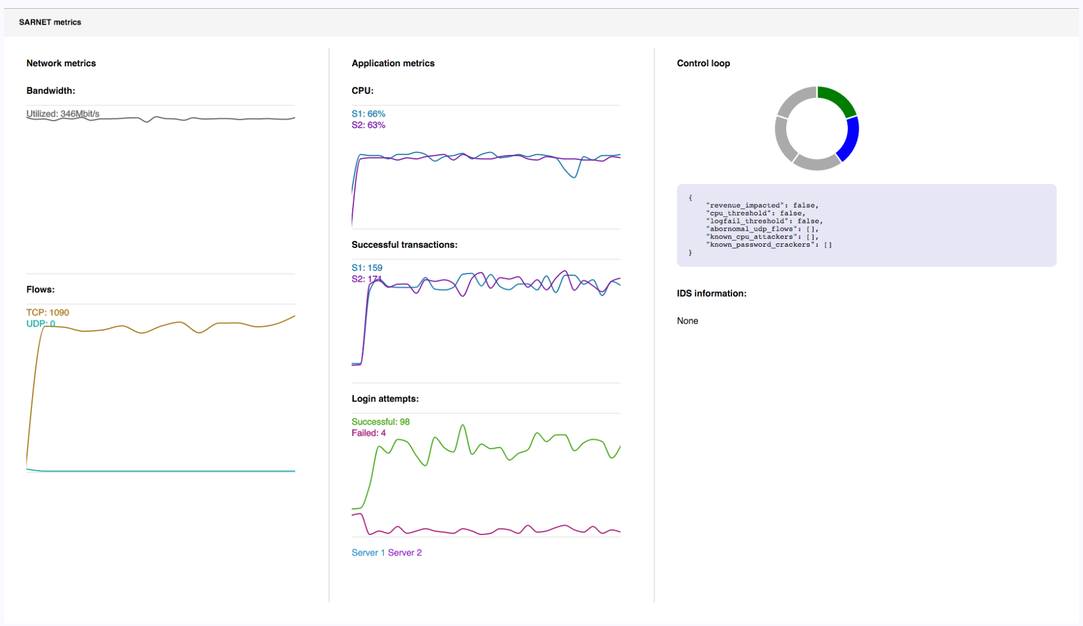
**Touch interface**

The right column shows general information, instructions and some toggle switches for the view.

The left side shows the network under attack, the bandwidth consumption and the active network flows

The bottom includes attack controls and some statistics about the selected network element.




**Metrics screen**
The graphs show the current state of the network. The right column shows a simplified version of the control loop showing the current phase and the detected events.

## Key takeaways:

- A single attack can be addressed at different network layers, the preferred defence layer is dictated by policies of the network.
- SDNs can insert VNFs in the path that can be used for monitoring and traffic manipulation.
- DDoS attacks require actions from upstream, therefore response requires multi-domain coordination.

## Infrastructure

For the demo we use small scale but **realistic** attacks that are executed and contained inside **ExoGENI,** an international federated cloud testbed. A **Ciena 8700** switch is used at the UvA and Ciena sites to provide additional traffic isolation. We extended the testbed to include a link to via a Ciena 8700 at SuperComputing to allow **live traffic manipulation from the Ciena booth**.

Ralph Koning <R.Koning@uva.nl>, Ben de Graaff <b.degraaff@uva.nl>, Paola Grosso <P.Grosso@uva.nl>, Cees de Laat <delaat@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