Multi-Domain Autonomous mitigation of Cyber Attacks
Demonstration at Ciena booth #1281
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.

Multi-Domain Autonomous Response

In this demonstration we let the viewers initiate one of the pre-implmented attacks. The touch interface shows a multi domain network and services. Each domain is autonomous and implements the SARNET control loop to that maintains its own security state. Additionally, domains can collaborate with each other by allowing certain remote actions that fellow collaborators can invoke.

By adjusting levels of collaboration we demonstrate the effect on response capabilities and response times.

Autonomy is achieved by invoking informational requests and defensive actions from the victim. This gives the victim the autonomy to make decisions over its destined traffic and it gives the collaborators the autonomy to decide on how to handle the requests.

Key takeaways:

- Domains can collaborate and maintain autonomy.
- Different levels of collaboration influence attack response times; more collaboration does not necessarily mean faster response times.
- Collaborative defence strategies are better in defending against heavy attacks.

Infrastructure

In this 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 also implemented a SARNET on a physical domain that is part of the automation demo at SURF booth #857.