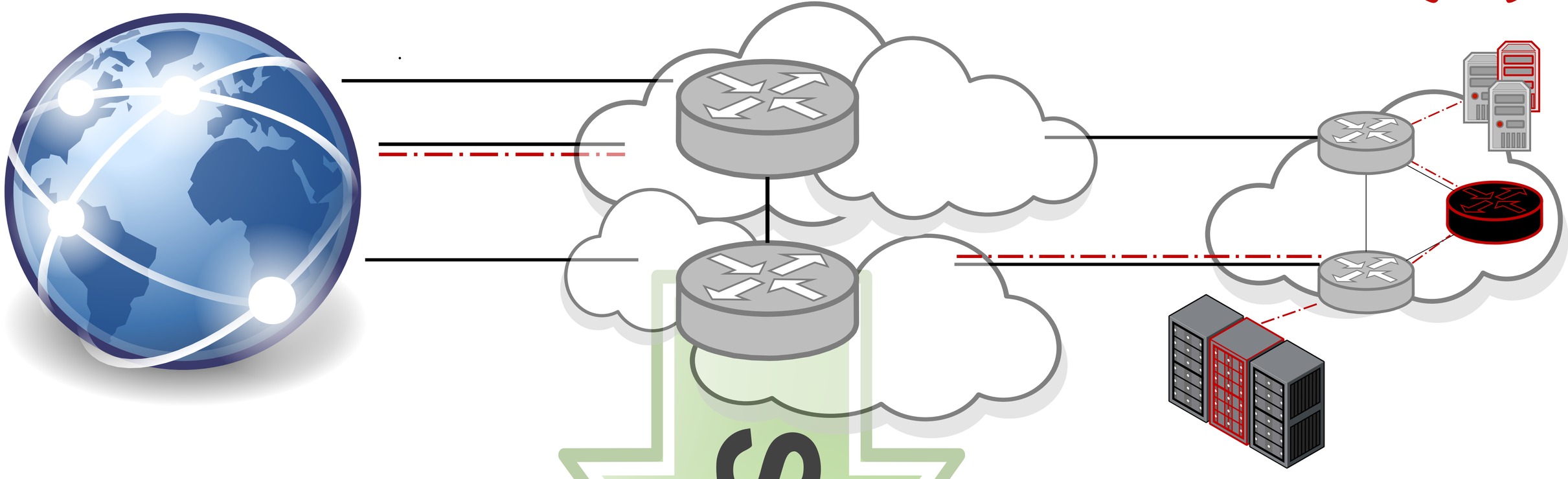
SSHCure: SSH Intrusion Detection using NetFlow and IPFIX

Luuk Hendriks, Rick Hofstede, Anna Sperotto, Aiko Pras

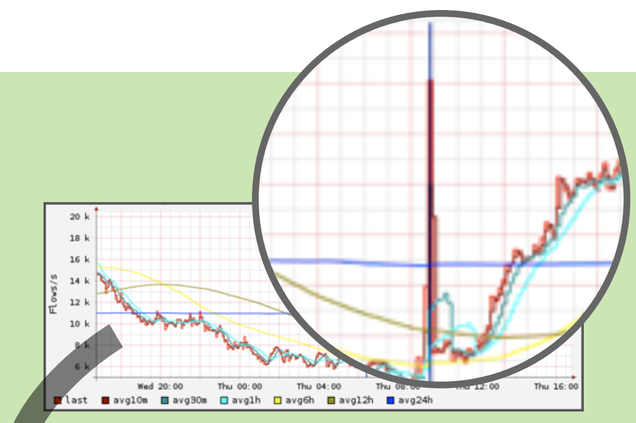
Design and Analysis of Communication Systems, University of Twente
{luuk.hendriks,r.j.hofstede,a.sperotto,a.pras}@utwente.nl

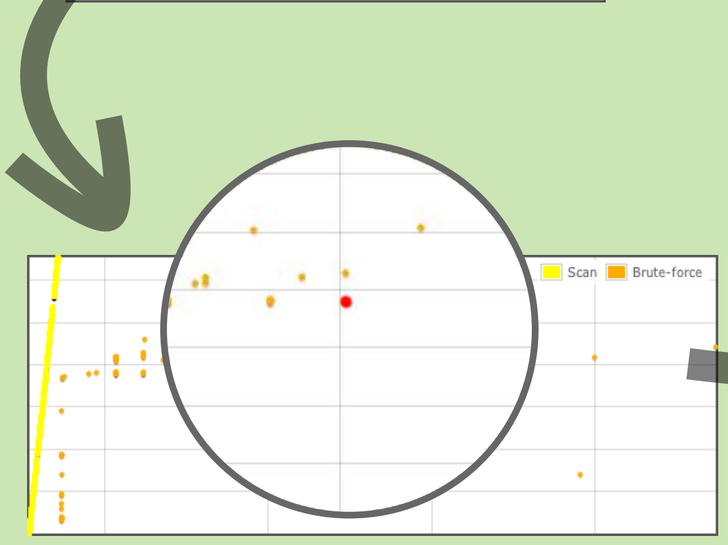


We see an **increasing number of SSH attacks.** Measurements show that a typical NREN enables for **more than 1000 attacks per day**. While few of these are successful (i.e. end in a **compromise**), the ones that do succeed can cause **severe damage** in a plethora of different ways.

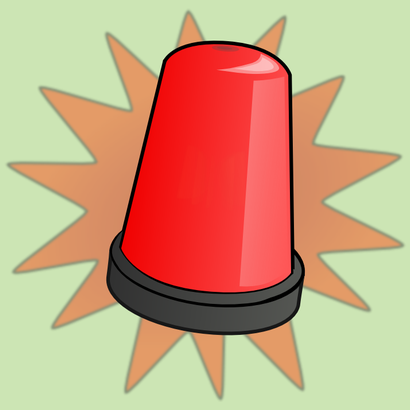
SSHCure

- Scalable, deployed in NREN with up to 13 backbone links
- Privacy preserving
- No performance impact on the network level
- Accurate detection for different phases within an attack
- Easily deployed as an NfSen plugin





SSHCure is able to analyze large amount of flow data and show what is really going on in the network, **alerting administrators in real time.**



Get SSHCure at **http://sshcure.sf.net**

Adoption and deployments:

Hogeschool van Amsterdam
Media, Creatie en Informatie

CESNET

SURFnet

UNIVERSITY OF TWENTE.

SURFnet UNIVERSITY OF TWENTE.