# WP3: Resilience mechanisms for infrastructures and endpoints

Yuji Sekiya, Ryo Nakamura and Daisuke Miyamoto

The University of Tokyo

## Outline

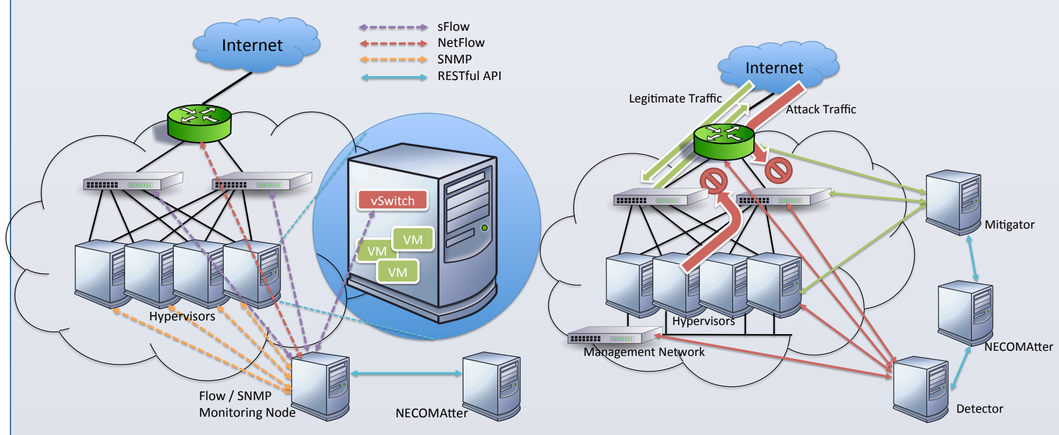
The main objective of WP3 (Cyberdefense) is to provide defense mechanisms against cyber attacks and malware, both on infrastructure and endpoint. This poster shows the status of Task 3.3 and Task 3.4 including D3.4

- Detection and mitigation of cloud-based threats
- Endpoint-level Cyberdefence Mechanisms
- Resilient Firewall

## Detection and Mitigation of Cloud-based Threats

There were several incidents or accidents on commercial public clouds in past times, such as the Amazon EC2 outage by botnets. Botnets inside a cloud and DDoS attacks can make fairly serious damages on the cloud infrastructure itself, not only user VMs. The typical treats of public clouds are

- information leak,
- VM hijacking,
- denial of services, and
- resource exhaustion.




Proposed Monitoring and Mitigation System Design

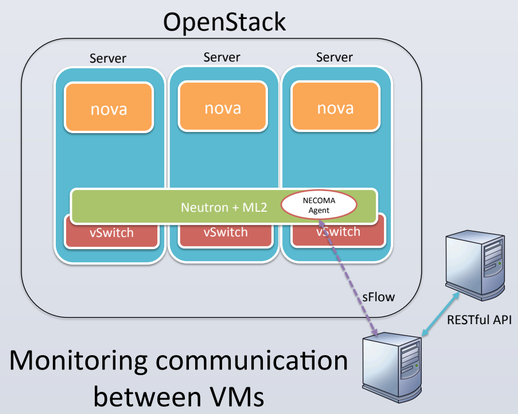
It is useful to poll and collect the status of hypervisors and VMs for finding abnormal behaviors inside a cloud. We should monitor traffic behaviors at each VM from other VMs, or outside a cloud, so that we can find changes in traffic behaviors.

## Monitoring Methods in a Cloud

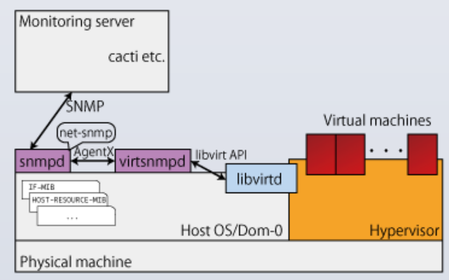
In order to counter such threats, the following methods are useful.

- polling the status of hypervisors and VMs
- monitoring the traffic flows inside and outside a cloud

In order to find changes in traffic behaviors, it is needed to monitor the traffic crossing not only physical network switches between hypervisors, but the traffic crossing virtual network switches (such as Open vSwitch) between VMs.



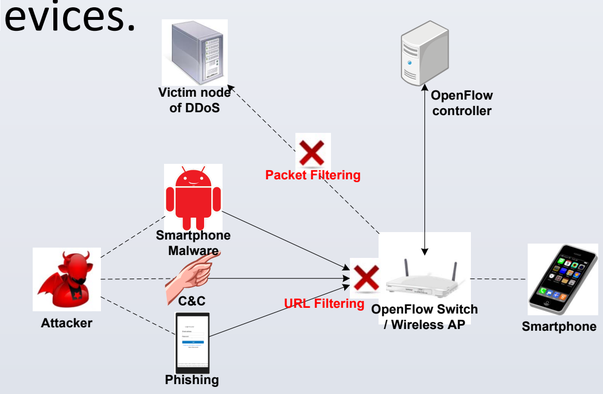

Monitoring communication between VMs




Monitoring HV status including I/O patterns

## Detection and Mitigation for Endpoint Devices

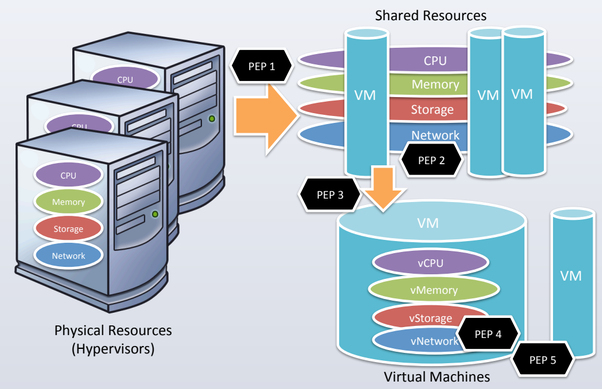
In order to provide a resilient protection for smartphone devices, we decided to utilize wireless access points (APs). The defense at the smartphone itself is difficult. Instead, we propose to offload smartphone firewalling function to network switching devices.




Endpoint Firewall using OpenFlow AP

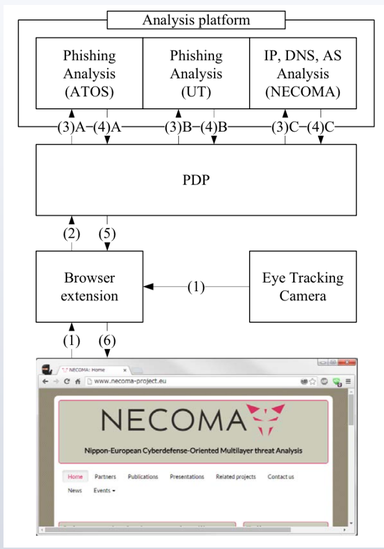
We decided to employ OpenFlow-capable wireless APs. Since OpenFlow provides powerful traffic control schemes, it facilitates the implementation of URL filtering based on the packet payload, as well as packet filtering based on header information.

## Linkages of PEPs and PDPs to implement Resilient Firewall




The linkages and cooperation of PDPs and PEPs in infrastructure and endpoint are necessary. PDPs are implemented by analysis modules and analysis modules send information to NECOMAtter. Each PEP module watches NECOMAtter timeline and detect related malicious behaviors, then each PEP module makes appropriate actions.

Based on the methodology, detection and mitigation of infrastructure and endpoint are working collaboratively.




Contacts :

Yuji Sekiya <sekiya@nc.u-tokyo.ac.jp>

Daisuke Miyamoto <daisu-mi@nc.u-tokyo.ac.jp>

東京大学 THE UNIVERSITY OF TOKYO

NECOMA