IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Intent-Based Attack Mitigation through Opportunistic Synchronization of Microservices

Authors

Do Duc Anh NGUYEN

Fabien AUTREL

Ahmed BOUABDALLAH

Jérôme FRANÇOIS

Pierre ALAIN

Guillaume DOYEN

Project

SuperviZ

Partners

cea

GRENOBLE INP UGA POLYTECH GRENOBLE

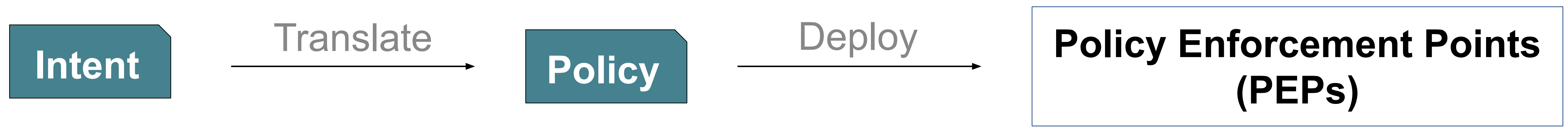
Inria

UMR IRISA

UGA Université Grenoble Alpes

Context: the Case of Intent-Based Networking (IBN)

IBN System: allows expressing objectives expressed in high level languages or natural language to modify the behavior of network operations



e.g. Stop propagation of malware

- Drop packets from infected host X
- Isolate network Y

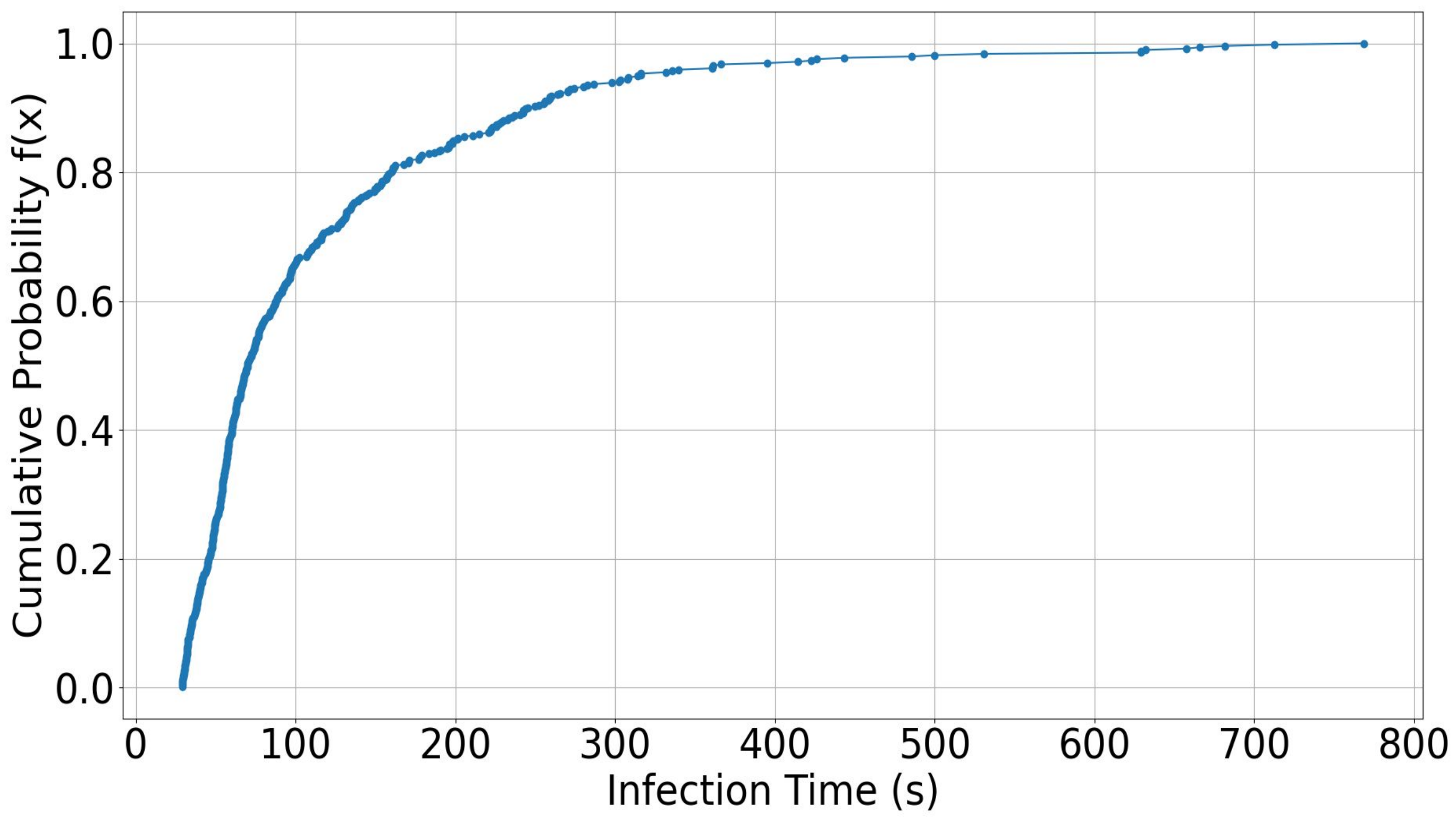
- Firewall
- Intrusion Detection System

➡ Avoid error-prone and time-consuming tasks and facilitates the expression of a security policy

Problematic and Research Question

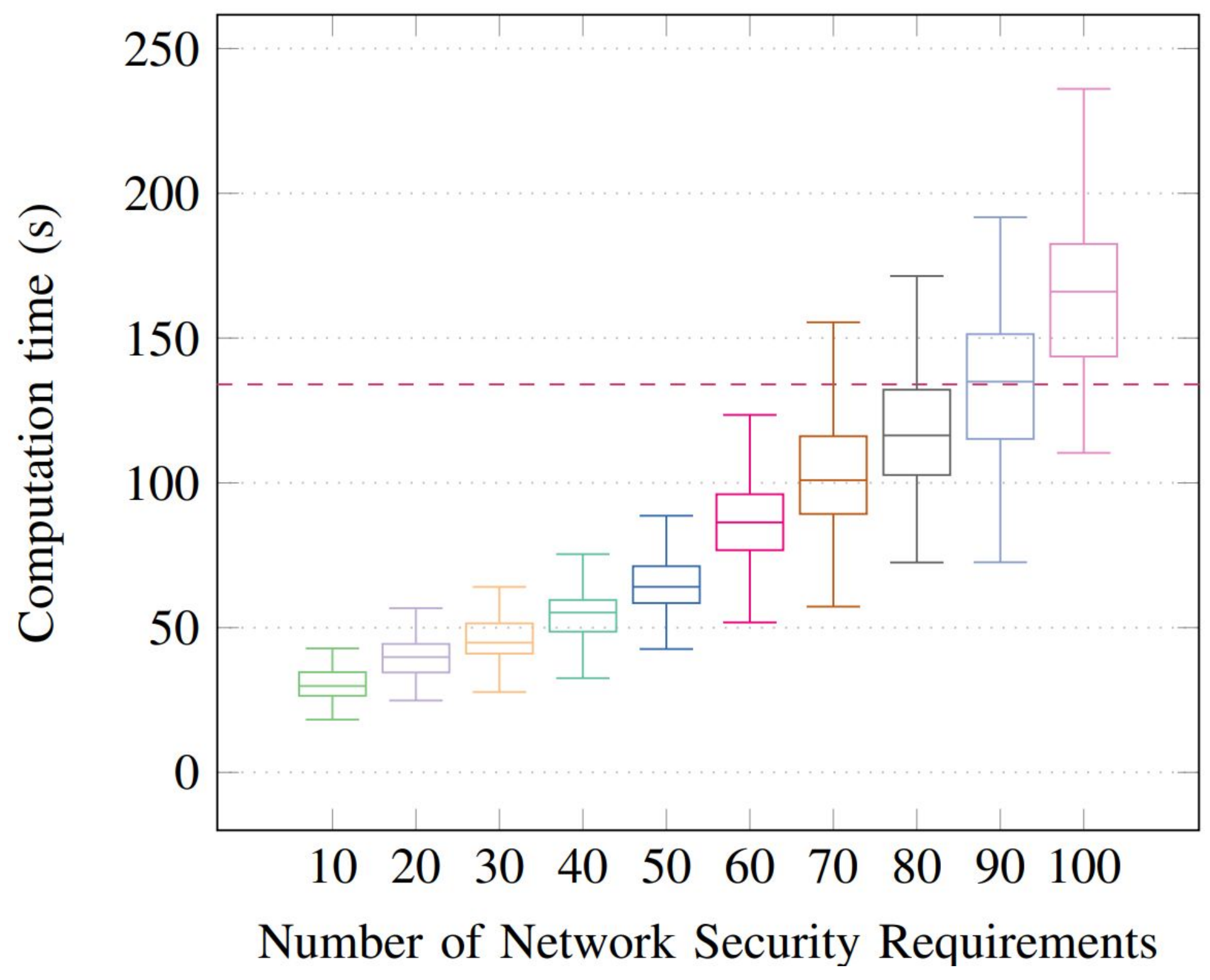
IBN systems may experience degraded performance and limited scalability

Question: Can state-of-the-art IBN systems deploy reaction policies fast enough in the context of fast propagating malwares?



Our empirical cumulative distribution function of infection times of WannaCry in 50-host networks [1]

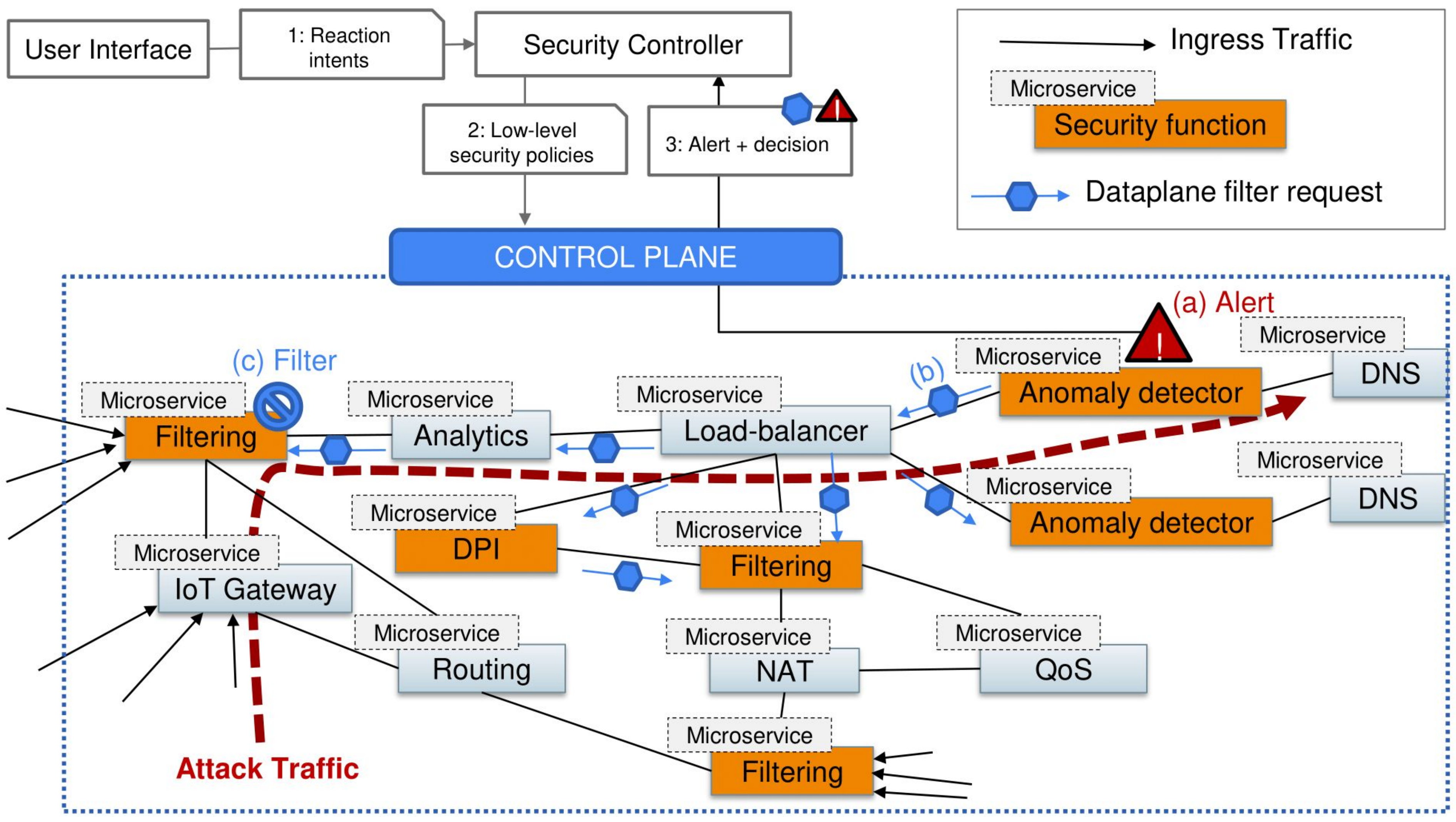
~20% of infections are processed in ≤50 seconds



Computation time of optimal firewall rules from user requirements [2]

>100 seconds required to compute 100 security requirements

An Opportunistic Approach Using Microservices



Target architecture using opportunistic approach

We propose to leverage

- Microservices as PEPs to enable
  - ➢ Scalability
  - ➢ Flexibility
  - ➢ Independent development and deployment
- A fast synchronization mechanism between microservices to
  - ➢ Share attack information
  - ➢ Autonomously response to attacks

The opportunistic approach is fast for synchronization

- Reuse existing packets to embed attack information

  e.g. The anomaly detector embed “filtering” decisions on detected malware propagation traffic

- Microservices with appropriate security functions update their response as soon as they receive these packets

  e.g. The “filtering" microservices update their response based on received decisions

Reference:

[1] Do Duc Anh Nguyen et al. ”How Fast do Malwares Leveraging EternalBlue Propagate? The case of WannaCry and NotPetya“. In: SecSoft Workshop. 2024.

[2] D. Bringhenti et al., “Automated firewall configuration in virtual networks,” IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 1559–1576, 2022.

Contact: do-duc-anh.nguyen@imt-atlantique.fr