20º WRNP

Workshop RNP

IoT-Flows: Lightweight Policy Enforcement of Information Flows in IoT Infrastructures

José Augusto **Suruagy** Monteiro

Centro de Informática - UFPE

Centro de Informática UFPE

VIRTUS IMPAVIDA UFPE

UNIVERSITY OF MICHIGAN

RNP

IoT-Flows: US Subteam (PIs)

Prof. Atul Prakash (UMich)

Expert on security and IoT

Prof. Darko Marinov (UIUC)

Expert on software testing

IoT-Flows: BR Subteam (PIs)

Prof. José A. Suruagy – Expert on network monitoring and architectures

Prof. Paulo Gonçalves – Expert on wireless threats

Prof. Marcelo d’Amorim – Expert on program analysis

Prof. Kiev Gama – Expert on adaptive middleware for IoT

Problem: IoT devices security

- Hardware limitations make IoT devices vulnerable to exploitation, for example, in launching DDoS attacks
- IoT devices in homes are also vulnerable to attacks, which could lead to loss of privacy, data theft, financial losses, and even physical harm
- Security issues with IoT systems are a significant concern in many other domains, e.g., autonomous cars or industrial systems

Proposed Solution: Cross-Layer Defense

- We propose to explore a novel approach of **cross-layer defense** in which we:
    - Monitor the IoT device’s network in a distributed manner;
    - Combine information from all network TCP/IP layers;
    - Use this information applying Complex Event Processing (CEP) rules to detect network attacks;
    - Enforce actions such as blocking **flows** or generating alerts once an attack is detected.

IoT-Flows: Initial Steps

Understanding the IoT Context

- Initial focus on Smart Homes
- Overall message: *Manufacturers lack security concerns when developing IoT apps*
- Publications:
  - Davino Mauro Junior, Luis Melo, Harvey Lu, Marcelo d'Amorim, Atul Prakash. *Beware of the App! On the Vulnerability Surface of Smart Devices through their Companion Apps.* CoRR, 2019.
  - Davino Mauro Junior, Luis Melo, Harvey Lu, Marcelo d'Amorim, Atul Prakash. A Study of Vulnerability Analysis of Popular Smart Devices Through Their Companion Apps. SafeThings, 2019 (Pending publication)

What can we do to help IoT apps become more secure?

- We extended a framework used to develop secure IoT apps for the Android platform (*FlowFence*)
- The extended framework enables fine-grained control of sensitive UI data on the app
- Publication:
  - Davino Mauro Junior, Kiev Gama, Atul Prakash: *Securing IoT Apps with Fine-grained Control of Information Flows.* SBSeg, 2018.

IoT-Flows: Current Work

IoT-Flows: Security Network System for IoT

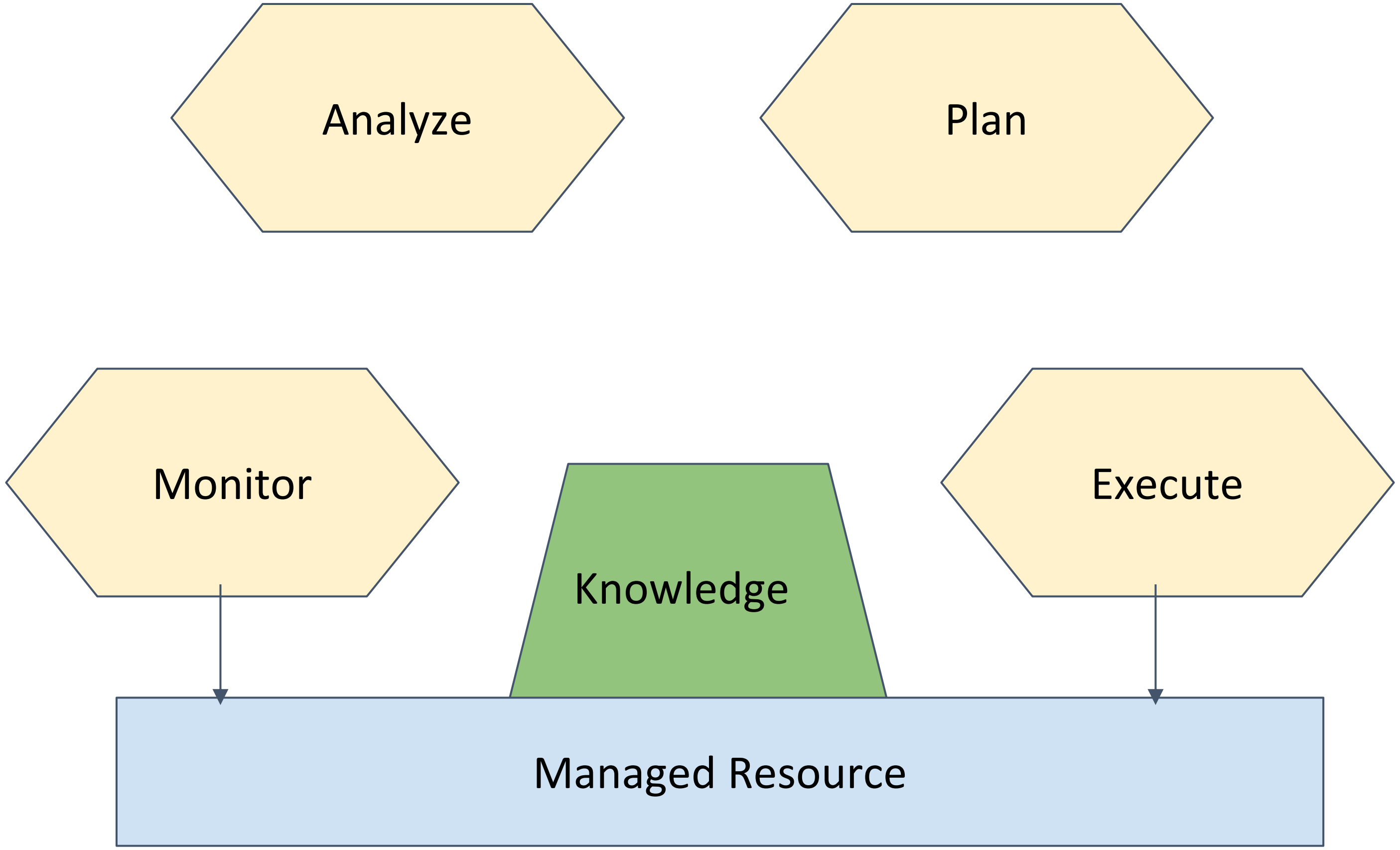
- Enable distributed network monitoring of IoT devices using a multi-layer approach
- Detect traditional Security attacks using IoT devices
    - e.g., ARP Spoofing, SYN flood, etc.
- Extensible platform with user-friendly interface via app
- Publication:
    - Davino Mauro Junior, Walber Rodrigues, Kiev Gama, José A. Suruagy, Paulo André da S. Gonçalves: *Towards a Multilayer Strategy Against Attacks on IoT Environments.* SERP4IoT, 2019 (Pending publication).

Usage of autonomous computing principles

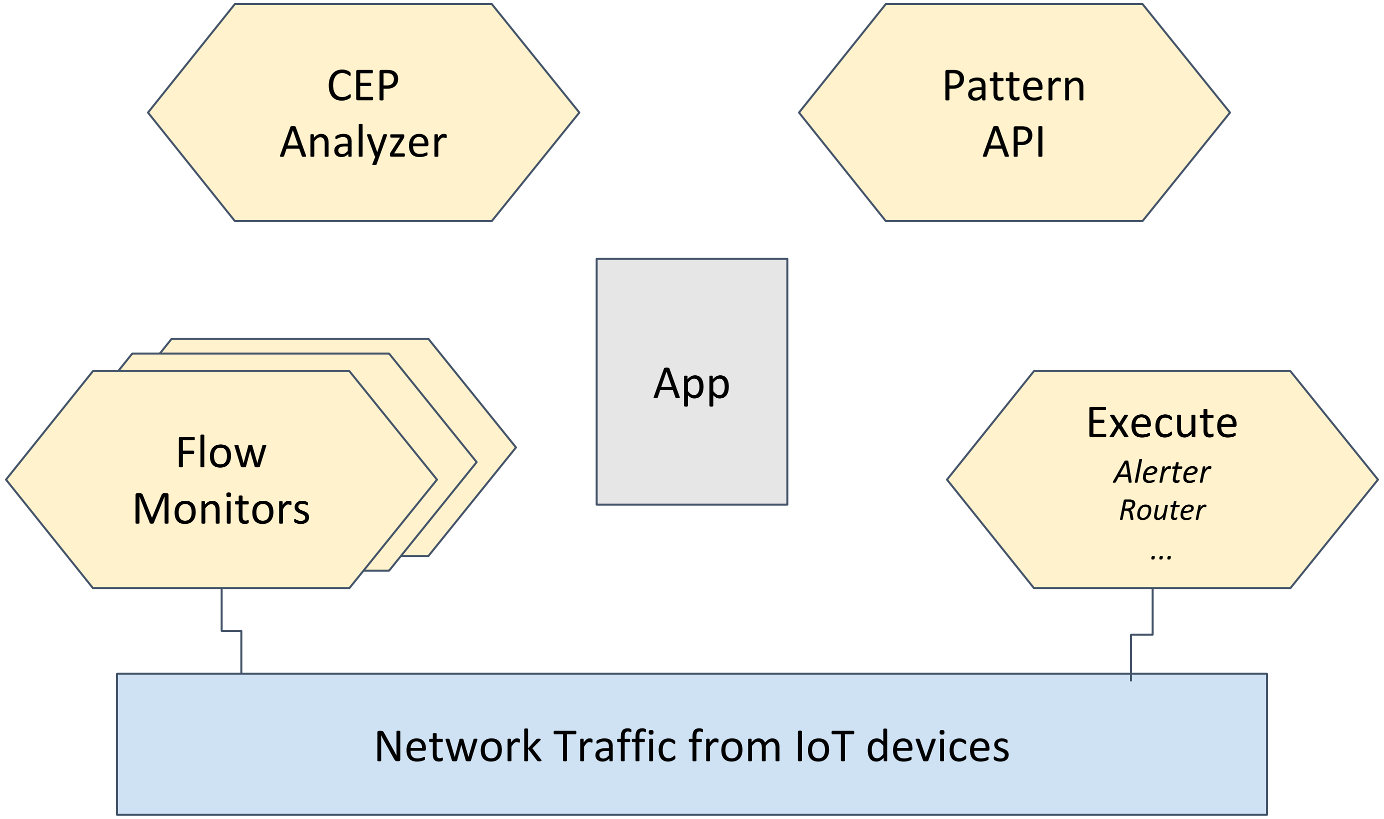
- MAPE-K architecture blueprint was originally introduced by IBM
- Designed with autonomic computing in mind
- Largely used on self-* systems (e.g., self-managing, self-adaptive)
- Ideal for event-based systems

https://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf

Original MAPE-K Components

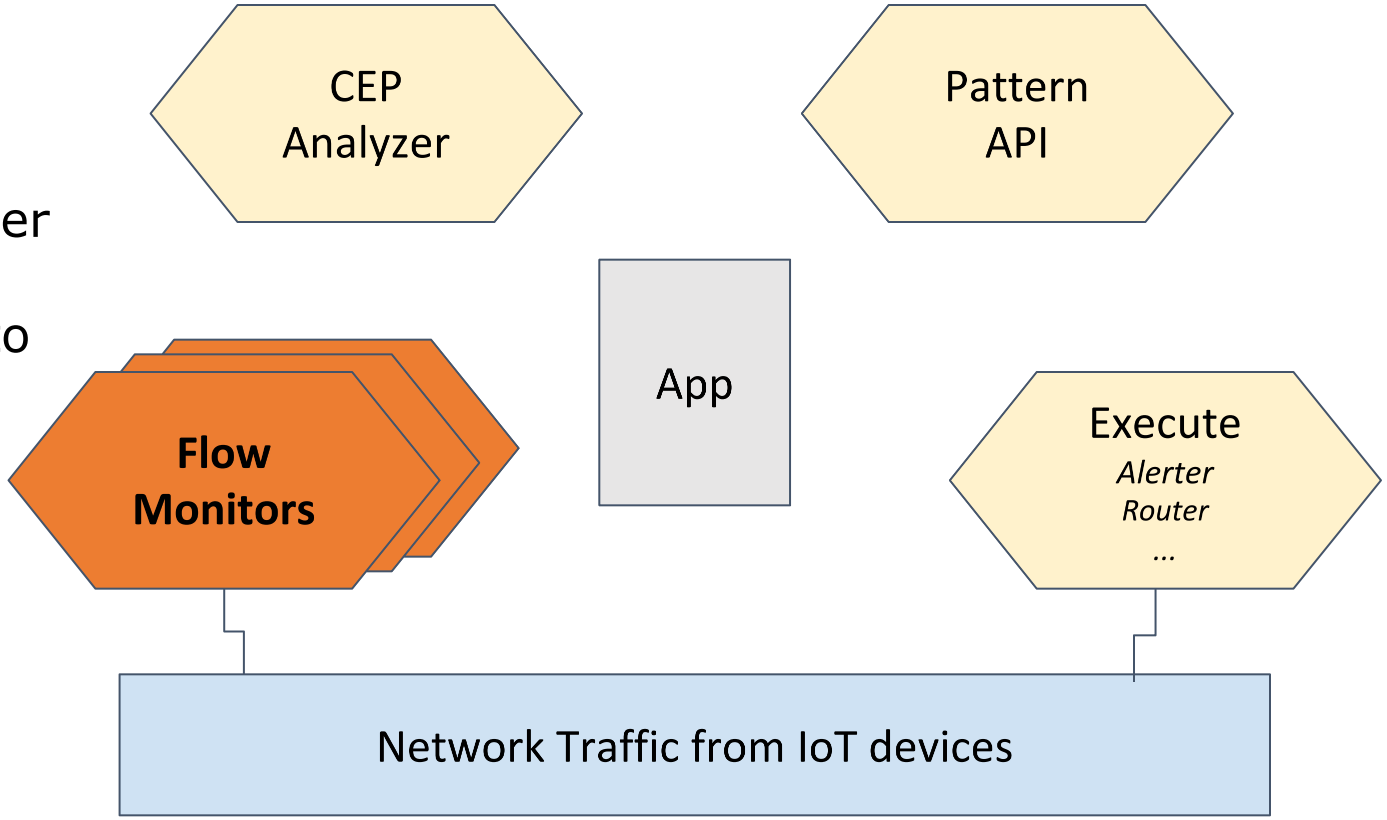


Our Architecture



Our Architecture

Aggregate and filter traffic data. Generate events to be analyzed.



CEP Analyzer

Pattern API

App

Flow Monitors

Execute

Alerter

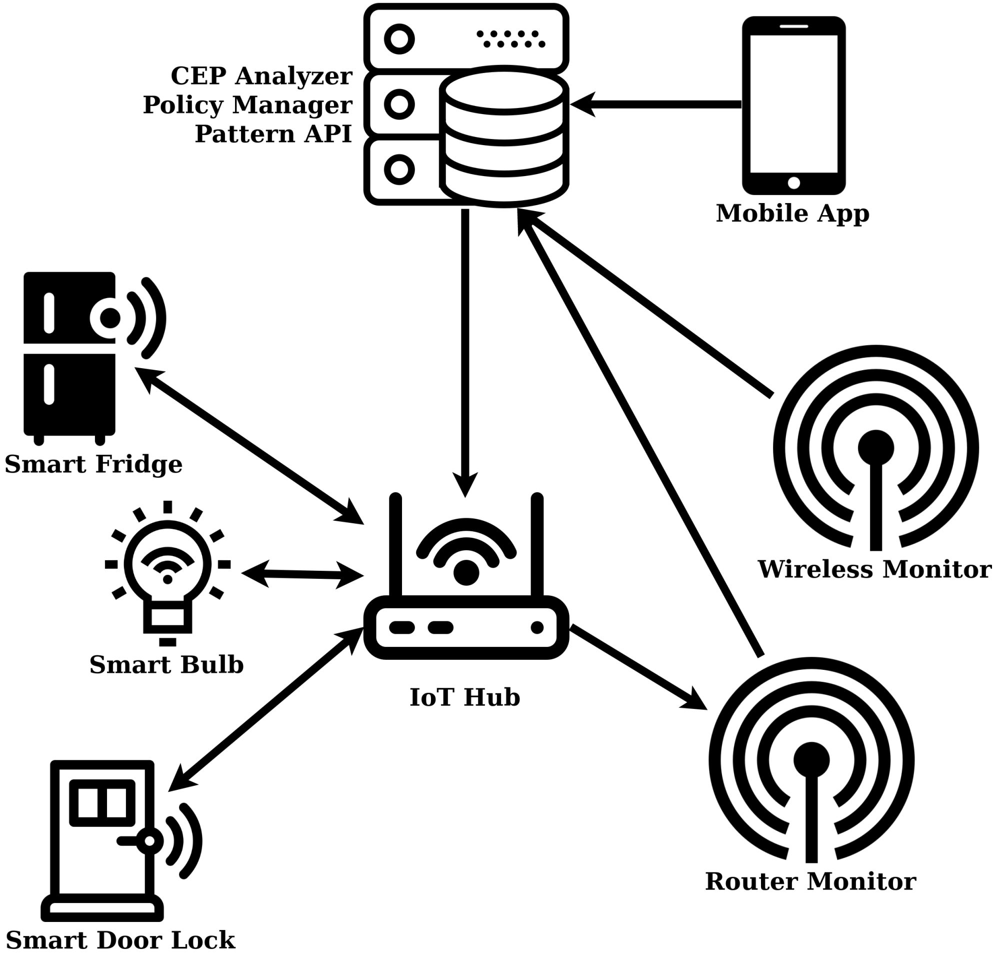
Router

...

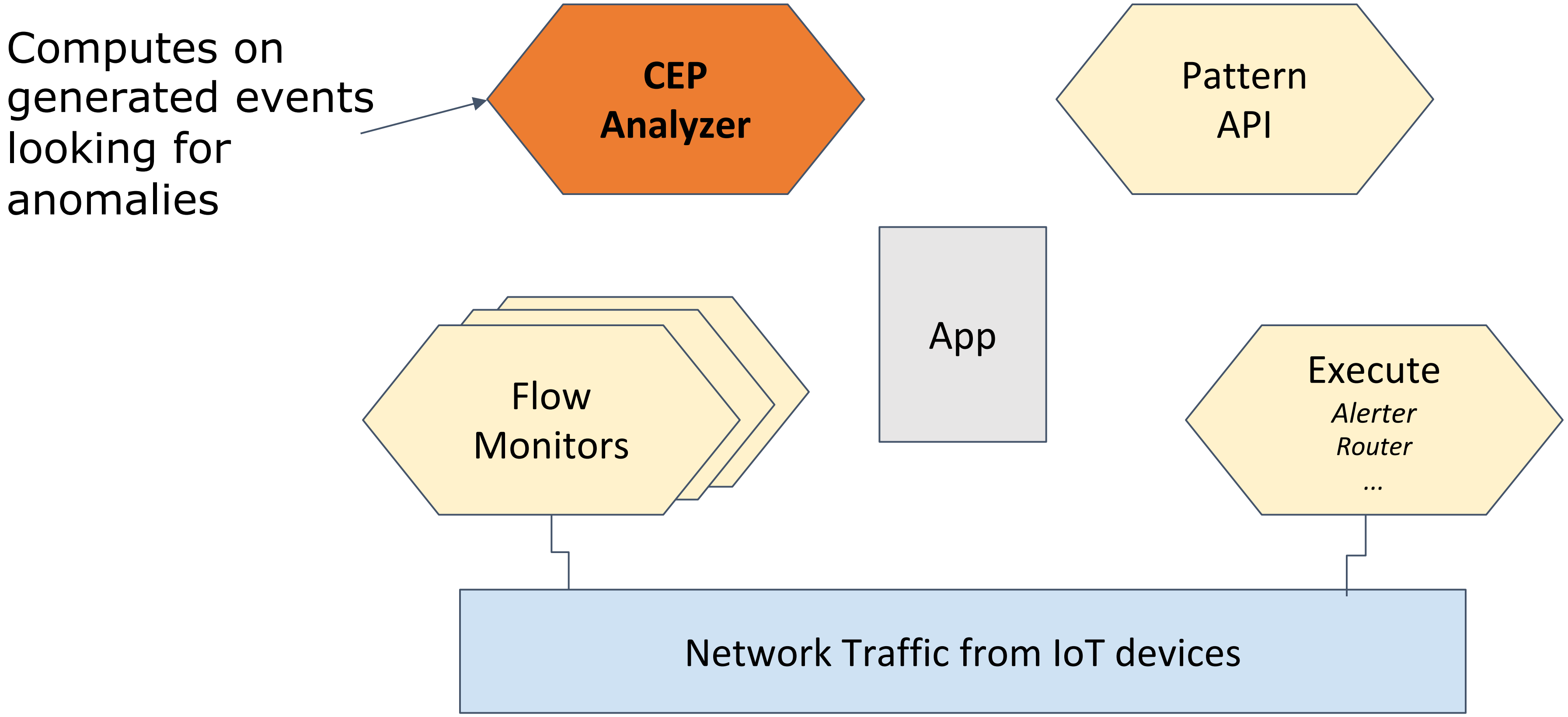
Network Traffic from IoT devices

Monitoring

- Two types of Monitoring:
  - Monitoring surrounding WLANs traffic
  - Monitoring Ethernet traffic
- Network packets are collected and mapped to a common structure
  - Structure is shared among architecture components, e.g., the CEP Analyzer
  - Structure resembles a Network packet



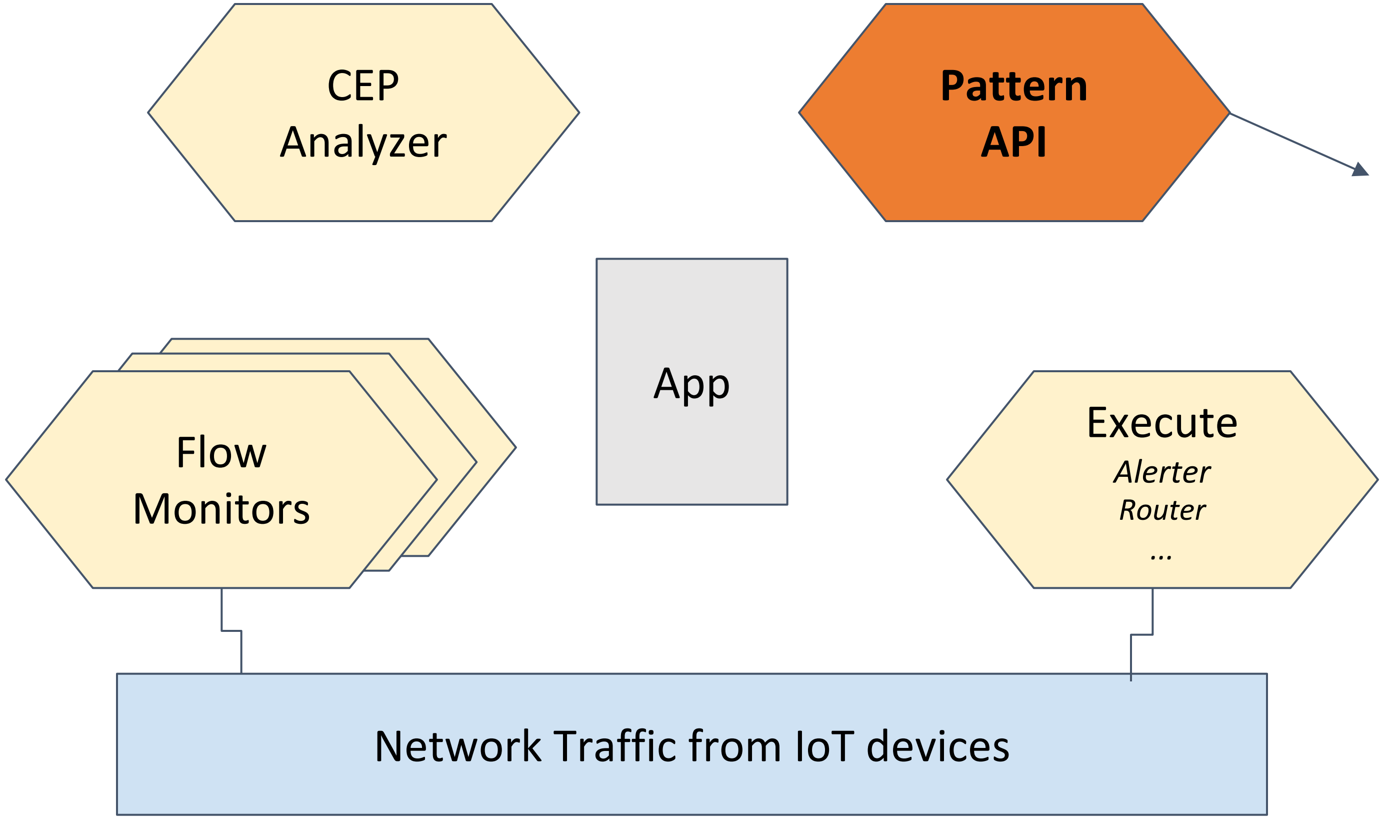
Our Architecture


Computes on generated events looking for anomalies
CEP Analyzer
Pattern API
App
Flow Monitors
Execute
Alerter
Router
...
Network Traffic from IoT devices

Analyzer

- Based on Complex Event Processing (CEP)
- Analyzes network data coming from the monitors which were mapped to events
- Rules (*patterns*) are applied to these events
  - Detect preconfigured attacks
  - Once detected, each pattern maps an enforcement action
  - Enforcement action is requested by the analyzer and disconnects a device from the network, generates an alert, etc.

Our Architecture

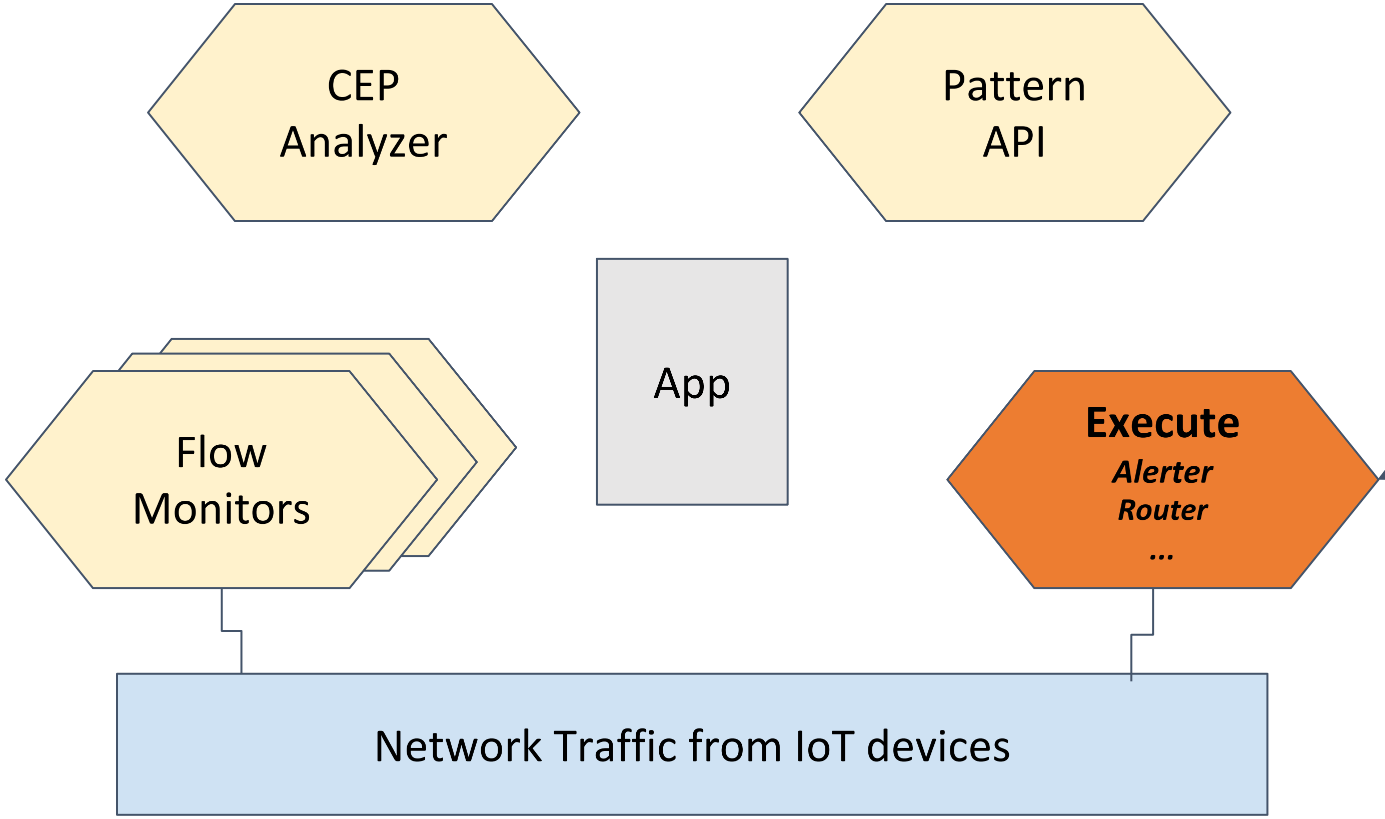


Extensible Patterns (rules) configured by the app

Pattern API

- Restful (REST) API
- Maintains Patterns (**Rules**) that identify an attack
- **Rules** are based on packet information
  - Ex: A rule to detect a SYN flood attack would involve checking if the count of captured network packets with the SYNFlag activated surpass a given threshold
- Every rule has 1..N predefined enforcement actions
  - Ex: Once a SYN flood attack is detected, one of the enforcement actions involves disconnecting the attacker's device from the network

Our Architecture

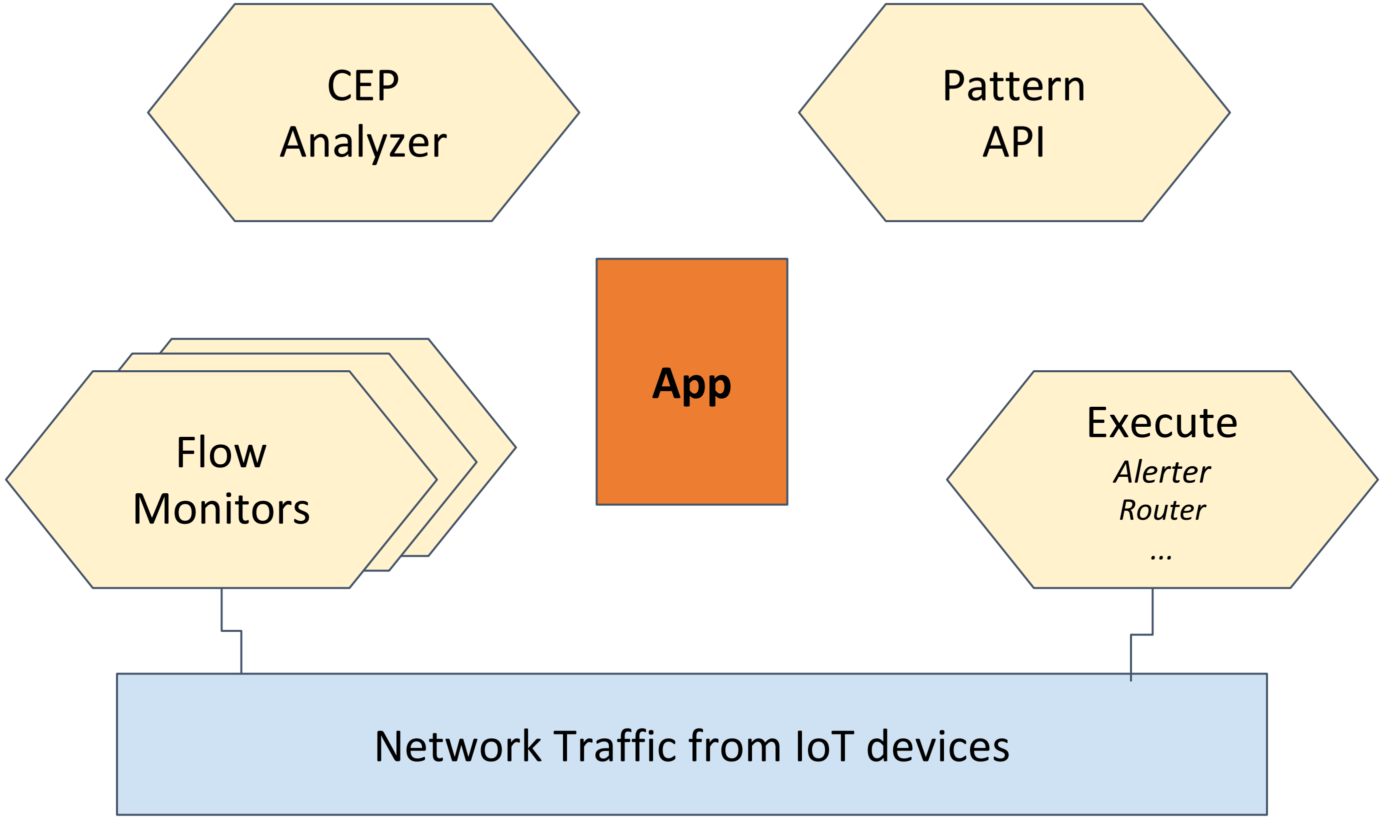


Execute the action, e.g., block a request

Execute

- Different enforcement actions can be performed once a suspicious behavior is detected
  - Generate an alert sending an email or SMS to the user
  - Request the router to disconnect a compromised device from the local network
  - Block the IoT device from making requests to unwanted endpoints, e.g., in a DDoS attack

Our Architecture



App

- Includes creation and management of rules even by non-specialist users
- Enables configuration of enforcement actions upon the rules
  - Ex: Send a SMS once a suspicious behavior is detected
- Enables visualization of recent activities involving the system
  - Ex: Recent rules matched by the Analyzer

Attacks we already tackle

- SYN Flood
- ARP Spoofing
- DeAuthorization
- Slowloris
- Black Nurse
- … More to come

Work in progress

20º WRNP Workshop RNP

- Development of the mobile application for generating patterns/policies
  - App should be user-friendly to non-specialist IT users
- Evaluation of platform against state-of-the-art solutions
  - Ex: Traditional network Intrusion Detection Systems (IDS)
- Tests generation to evaluate platform capabilities
  - Tests should emulate both traditional and new IoT attacks
- Evaluate how to use AI tools to generate new patterns automatically
  - Ideally, these patterns would match new attacks, e.g., learning from network traffic monitoring

20º WRNP
Workshop RNP

Obrigado!

José Augusto **Suruagy** Monteiro

suruagy@cin.ufpe.br

RNP MINISTÉRIO DA DEFESA MINISTÉRIO DA CIDADANIA MINISTÉRIO DA SAÚDE MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES PÁTRIA AMADA BRASIL GOVERNO FEDERAL