FOSDEM'21

ntopng for IoT

How to profitably use ntopng in Smart Homes: The Case of the TOTEM project

ntop

FOSDEM 2021, ntop Stand

Saturday, 06th, February, 2021

Antonis Gotsis (FERON TECHNOLOGIES) & Simone Mainardi (ntop)

antonis.gotsis@feron-tech.com & mainardi@ntop.org

feron TECHNOLOGIES

SUPPORTED BY NGI

Agenda

- Introduction: Project Team & Context
- Background: IoT & Connected Home Challenges
- Use of ntopng in IoT: Applying ntopng in Connected Home
- Live Demo & Initial Experiences from our Testbed
- Roadmap

Project Context

NGI TRUST – EU-funded partnership for innovative technological solutions to ensure privacy & enhance trust for the human-centric Internet (Dec 2018- Nov 2021)

- ❑ **Data Management**
- ❑ **Data Ethics**
- ❑ **Securing the Internet of Things**
- ❑ **Advancing Identity**

NGI OPEN CALLS

TOTEM: Trust-Enhancing TechnOlogies CommodiTization for IncrEasing Security Awareness in Connected HoMes (09/2020 – 05/2021)

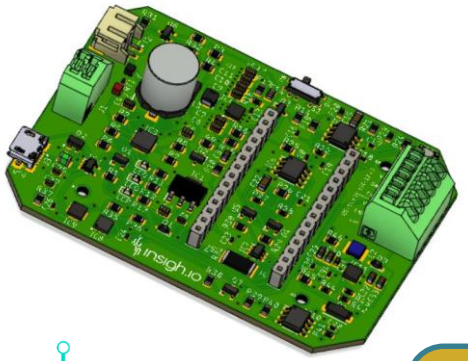
Project Team

feron TECHNOLOGIES

Tech Developers & Integrators

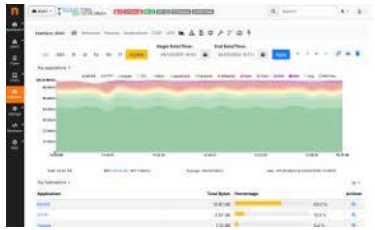
Opensource Developers

ntop



insigh.io embedding intelligence

In-house Full-Stack IoT



Network Visibility Solutions

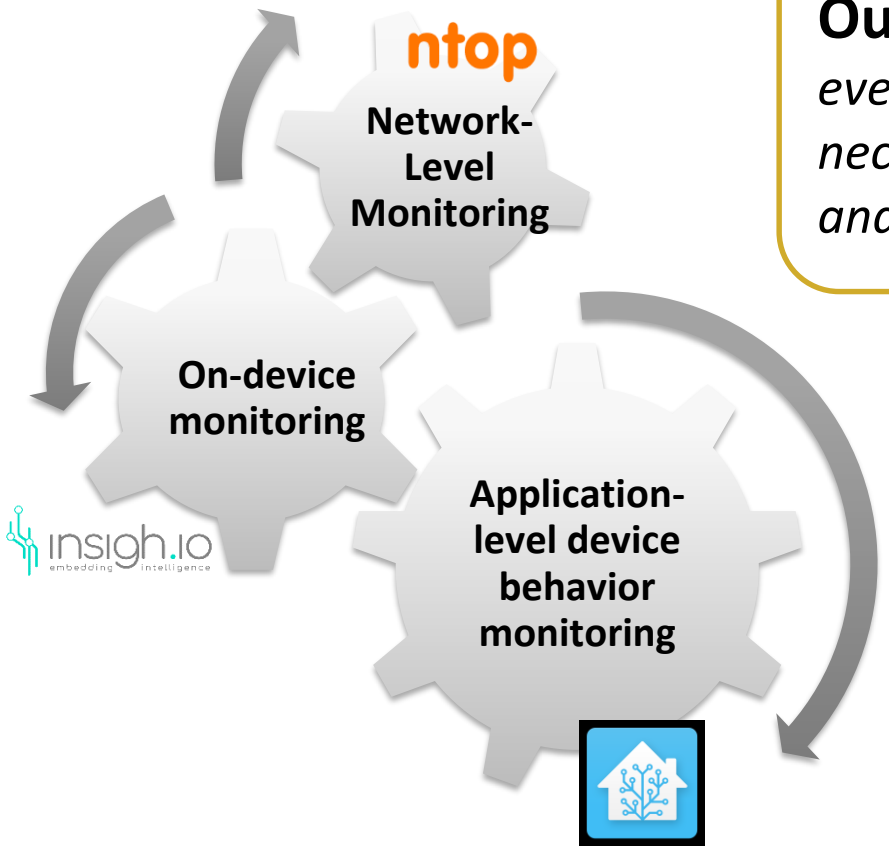
Background: IoT in Connected Homes

A Connected Home with many heterogeneous end-points for
Connectivity, networking, media-entertainment, physical security, energy monitoring, healthcare, fitness, wellness, tele-working

As more and more connected things are incorporated in our digital environment, there is a need to develop new robust, open, and easy to use tools to help users increase trust and achieve greater control over fleets of connected home end-points.

- ✓ Firewalls blocking incoming traffic
- ✓ Low-end end-points lacking security-by-design features not able to warn for misbehavior
- ✓ Various chip manufacturers, device makers, and solution integrators are involved in the creation of a commercial IoT solution, each one bringing his own security design

The TOTEM Approach & Value Proposition

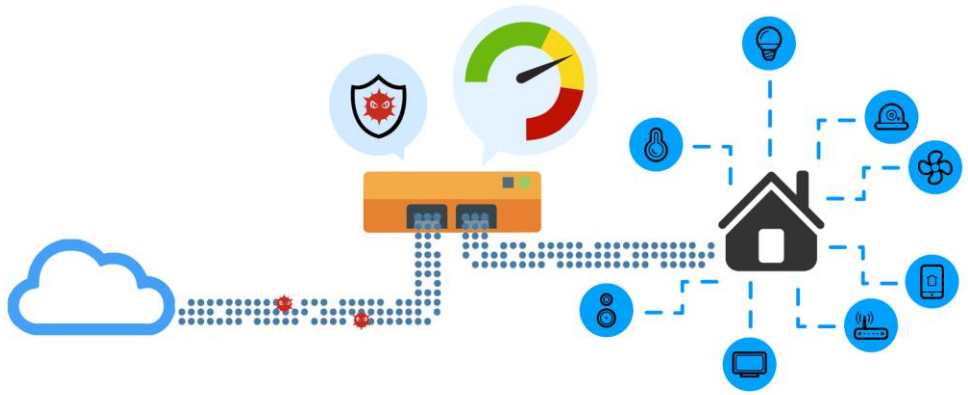


Our Value Proposition: *Simplify, automate and eventually make accessible to non-expert users all the necessary tools required for proper control of end-points and early identification of potential malicious operation.*

Main Expected Outcomes

- ☑ **Extensions to existing products:** insighio, ntopng
- ☑ **End-User Tools :** Web-based UI, Dashboards, Alerts
- ☑ **Community Contributions :** Open-Source Tools & Datasets
- ☑ **Demonstration:** Smart-home testing environment

ntopng in Connected Homes



Main Challenges

- ❑ IoT traffic originating from the “inside”
- ❑ End user not having the skills to detect, prevent or remove potential security threats

Highlights

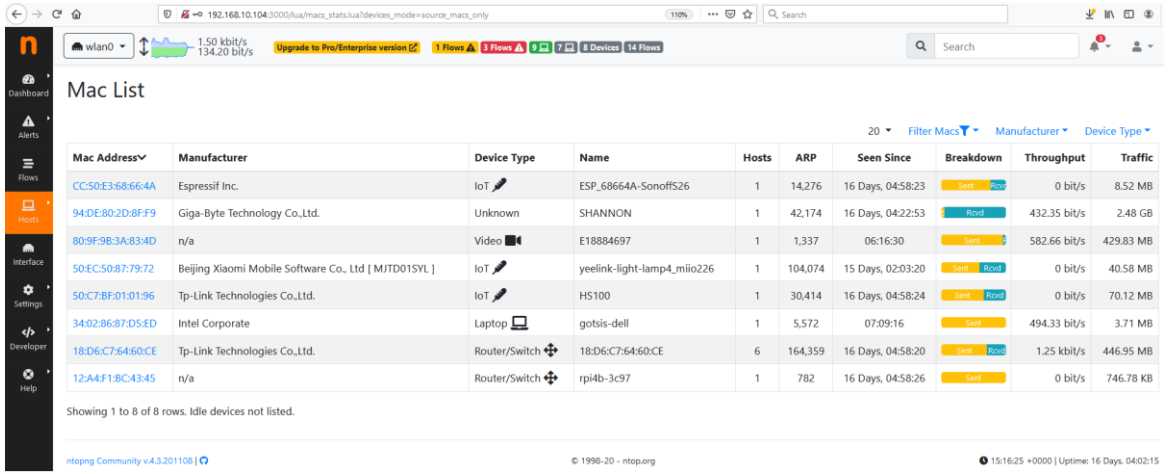
- ✓ Monitoring & Policy Enforcing Tool for Connected Home Traffic
- ✓ No need to change existing network equipment and topology → Fully transparent
- ✓ Minimal hw/sw requirements → Runs in a 30 euro Raspberry Pi board hosting generic RPi OS
- ✓ ntopng stack: inline, appliance-oriented software stack.
- ✓ Installation completes in a few steps
- ✓ Fully configurable via a Web UI

Deploying & Operating ntopng in a Connected Home Environment

Burn OS in SD and Install Packages

Configure RPi as Bridged Access Point through Web UI

Force Connected Home Devices to Connect to RPi WiFi network



Main Capabilities

- ✓ Accurately and regularly discovering all devices connected to a network and their types
- ✓ Profiling the utilized protocols
- ✓ Getting a highly accurate per-flow view of the connected home traffic
- ✓ Enforcing Policies

The TOTEM Connected Home Test-bed

Connected Home Devices

- ✓ Off-the-shelf
- ✓ In-house

Project Monitoring Tools & Platforms

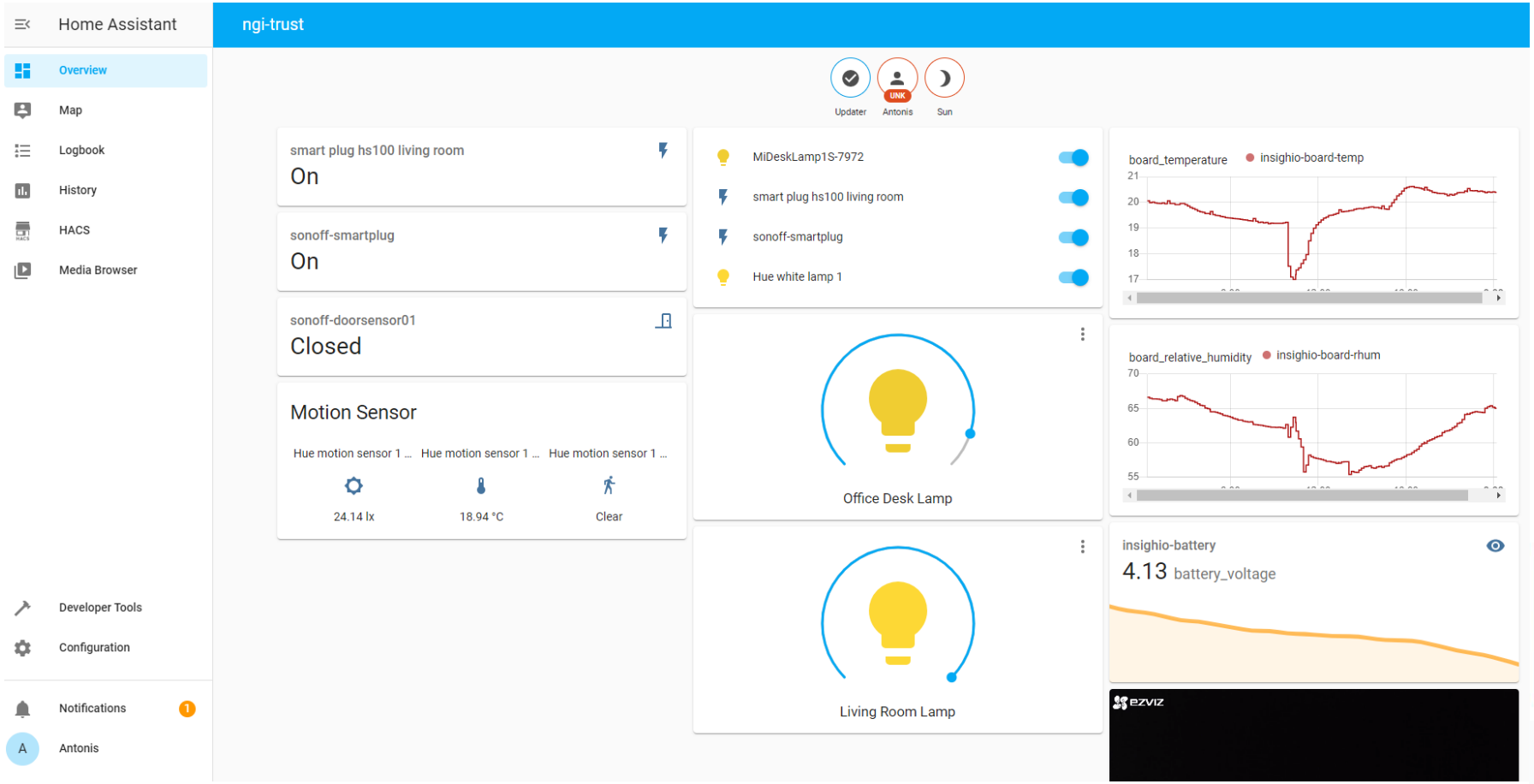
- ✓ ntopng stack
- ✓ Insighio back-end
- ✓ Home-Assistant instance
- ✓ Influx Cloud Instance

Type of Device	Manufacturer	Model	Control App	Approx. Cost (€)
Smart Plug	TP-Link	HS100	Kasa	15
Smart Plug	Sonoff	S26	eWeLink	20
Door sensor	Sonoff	DW2-WiFi	eWeLink	15
Desk Lamp	Xiaomi	Mi LED 1S	Mi Home	50
Camera with PTZ	Ezviz	C6CN	Ezviz	50
Smart Bulb	Philips	Hue E27	Hue	20
Motion Sensor	Philips	Hue MS	Hue	40
Zigbee Bridge	Philips	Hue Bridge	Hue	60
Custom IoT board	FERON	insighio	Web UI	50

6 different manufacturers, device types & control apps

The TOTEM Testbed Control Panel

* based on the Open Source Platform "Home-Assistant"



Device Change States

influxdata

home-assistant/home-assistant

6,300

Watch 1.3k Star 40.1k Fork 13.2k

Live Demo

- Testbed Control Panel
- ntopng Tool
- Connected Home Devices Events Database

Roadmap

- ✓ **Technical Developments**
  - Analyze connected home traffic (network activity) and derive rules using the ntopng stack
  - Analyze devices behavior (physical activity) using the events database
  - Develop end user tools
- ✓ **Open-Source Contributions**
  - https://github.com/ntop/ntopng/
  - https://github.com/insighio
  - Other third party projects
- ✓ **Dissemination**
  - ETSI IoT Week 2021
  - IoT Forum's IoTWeek 2021
- ✓ **Exploitation Opportunities**
  - ntop: cost-effective device monitor and policy network traffic of the connected-home
  - FERON TECHNOLOGIES: low-cost multi-modal tool for alerting end-users about potential malicious behavior

Thank you

Contact us:
antonis.gotsis@feron-tech.com
mainardi@ntop.org