

ntopng for IoT

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



FOSDEM 2021, ntop Stand

Saturday, 06th, February, 2021



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

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

SUPPORTED
BY



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

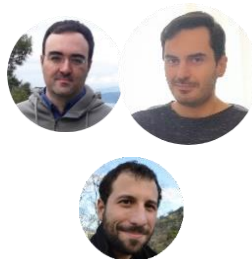
NGI OPEN CALLS

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

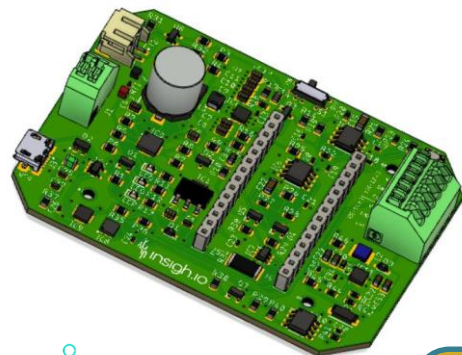
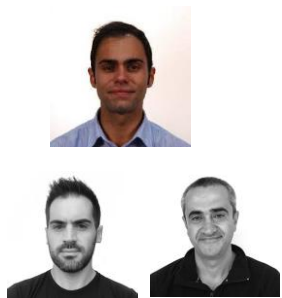
Project Team



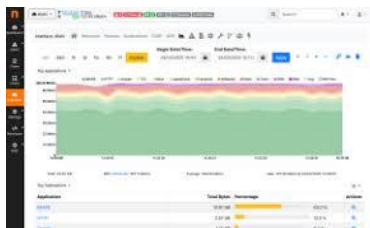
Tech Developers
& Integrators



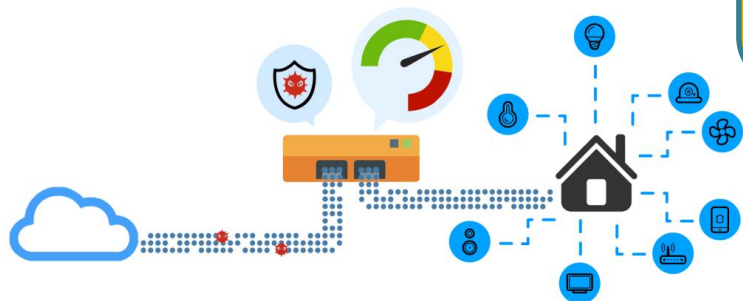
Opensource
Developers



In-house
Full-Stack IoT



Network
Visibility
Solutions



Background: IoT in Connected Homes



Landscape

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



Challenge

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.

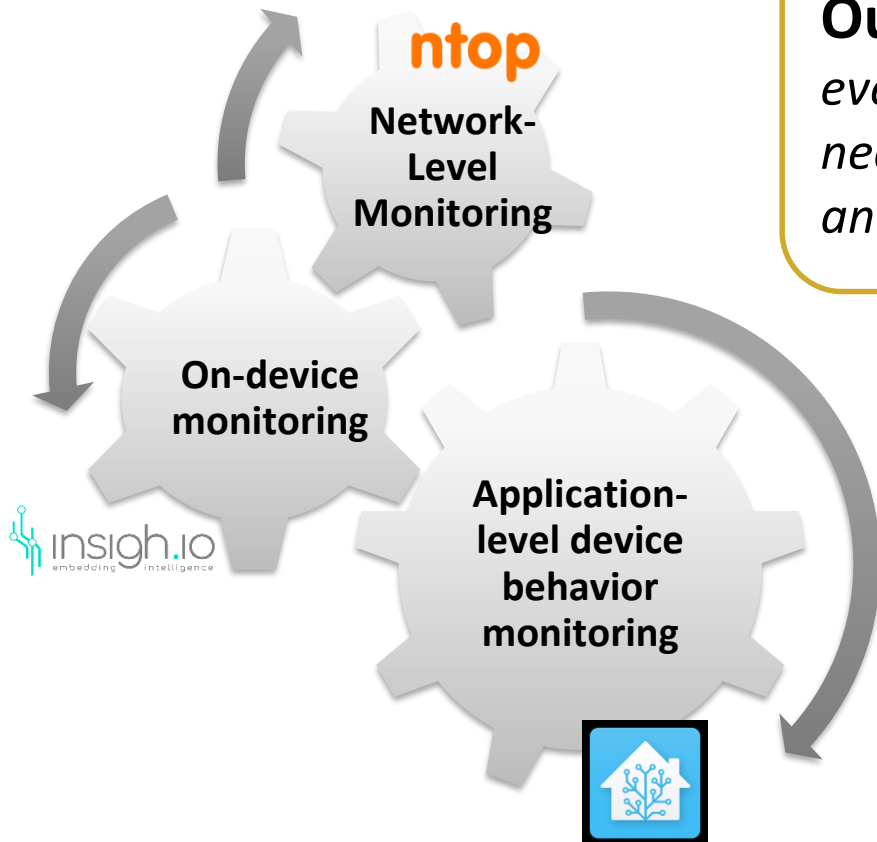


Current Status

- ✓ 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

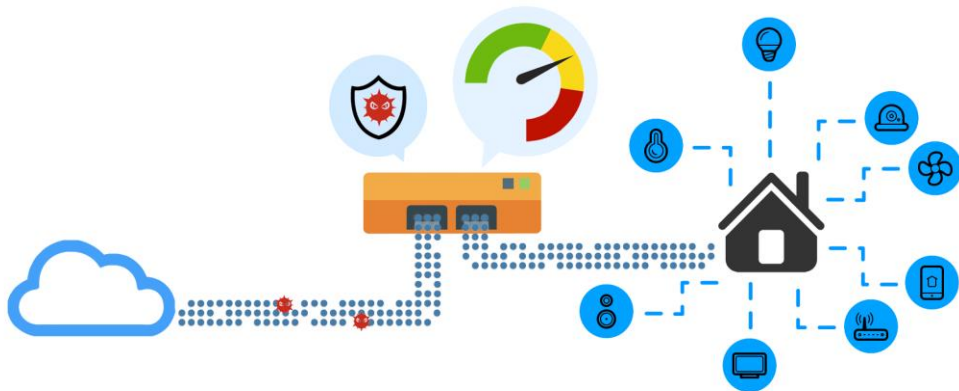


Our Value Proposition: *Simplify, automate and eventually make accessible to non-expert users all the necessary tools required for proper control of end-points and early identification of potential malicious operation.*

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



ntopng

Dashboard

Alerts

Flows

Macs

Interface

Settings

Developer

Help

wlan0

1.50 kbit/s

134.20 bit/s

Upgrade to Pro/Enterprise version 1 Flow 3 Flow 9 Mac 7 Int 8 Device 14 Flow

192.168.10.104:3000/na/mac_stats.lua?devices_mode=source_macs_only

15%

Search

Search

15:16:25 +0000

Uptime: 16 Days, 04:02:10

Mac List

20

Filter Macs

Manufacturer

Device Type

Mac Address	Manufacturer	Device Type	Name	Hosts	ARP	Seen Since	Breakdown	Throughput	Traffic
CC:50:E3:68:66:4A	Espressif Inc.	IoT	ESP_68664A-SonoffS26	1	14,276	16 Days, 04:58:23	<div>Sent</div>	0 bit/s	8.52 MB
94:DE:80:2D:8F:F9	Giga-Byte Technology Co.,Ltd.	Unknown	SHANNON	1	42,174	16 Days, 04:22:53	<div>Recv</div>	432.35 bit/s	2.48 GB
80:9F:9B:3A:83:4D	n/a	Video	E18884697	1	1,337	06:16:30	<div>Sent</div>	582.66 bit/s	429.83 MB
50:EC:50:87:79:72	Beijing Xiaomi Mobile Software Co., Ltd [MITD01SYL]	IoT	yeelink-light-lamp4_mio226	1	104,074	15 Days, 02:03:20	<div>Sent</div> <div>Recv</div>	0 bit/s	40.58 MB
50:C7:BF:01:01:96	Tp-Link Technologies Co.,Ltd.	IoT	HS100	1	30,414	16 Days, 04:58:24	<div>Sent</div> <div>Recv</div>	0 bit/s	70.12 MB
34:02:86:87:D5:ED	Intel Corporate	Laptop	gotis-dell	1	5,572	07:09:16	<div>Sent</div>	494.33 bit/s	3.71 MB
18:D6:C7:64:60:CE	Tp-Link Technologies Co.,Ltd.	Router/Switch	18:D6:C7:64:60:CE	6	164,359	16 Days, 04:58:20	<div>Sent</div> <div>Recv</div>	1.25 kbit/s	446.95 MB
12:A4:F1:BC:43:45	n/a	Router/Switch	rpi4b-3c97	1	782	16 Days, 04:58:26	<div>Sent</div>	0 bit/s	746.78 KB

Showing 1 to 8 of 8 rows. Idle devices not listed.

ntopng Community v4.3.201108

© 1998-20 - ntop.org

15:16:25 +0000 Uptime: 16 Days, 04:02:10

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
- ✓ Inshio back-end
- ✓ Home-Assistant instance
- ✓ Influx Cloud Instance

Sonoff S26 WiFi Smart Socket

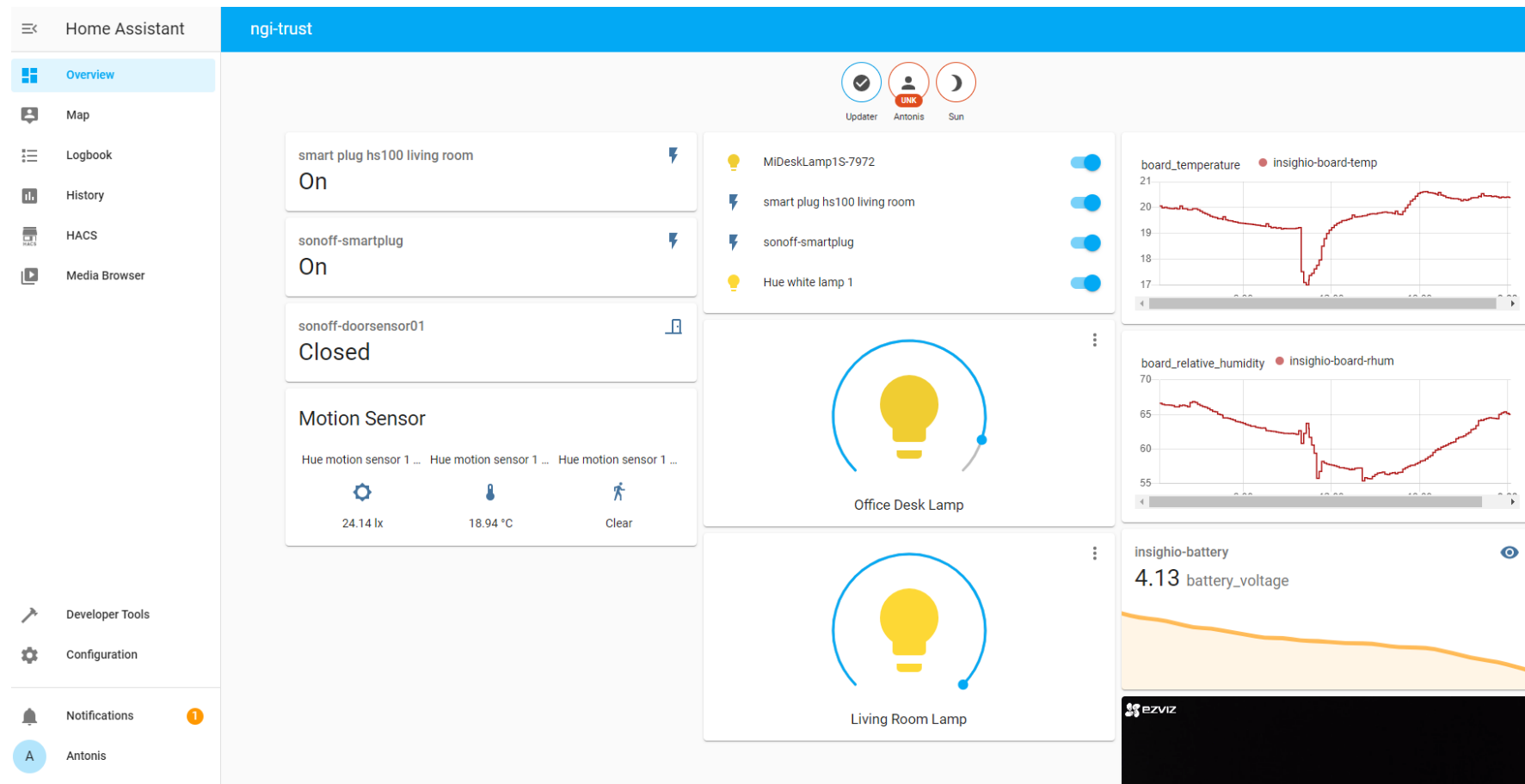


Type of Device	Manufacturer	Model	Control App	Approx. Cost (€)
Smart Plug	TP-Link	HS100	Kasa	15
Smart Plug	Sonoff	S26	eWeLink	20
Door sensor	Sonoff	DW2-WiFi	eWeLink	15
Desk Lamp	Xiaomi	Mi LED 1S	Mi Home	50
Camera with PTZ	Ezviz	C6CN	Ezviz	50
Smart Bulb	Philips	Hue E27	Hue	20
Motion Sensor	Philips	Hue 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**



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

