Ntopng as (cyber-)security enabler in low-critical cyber-physical environments

- Matteo Andolfi
- R&D Project Manager
- m.andolfi@nextworks.it
Low-critical cyber-physical systems and IoT vulnerabilities

Symphony and AN&MONE as Symphony module

AN&MONE architecture overview

Outcomes of using Ntopng

Next steps
Low-critical cyber-physical systems

- **IoT** cyber-physical systems where the impact of cyber attacks is not as high and/or immediate as in mission critical IT systems.

- These systems can be protected with a more relaxed approach, e.g. with a mix of cyber and physical information and analysis, and humans in the loop.
Low-critical cyber-physical systems vulnerabilities (1/2)

Heat remote control

- Attackers can switch on the heaters exploiting a compromised Control plane
  - *This leads to unnecessary energy consumption and a waste of money*

- Detecting strange network patterns might not be effective.

- Reactions can be:
  - *Block the commands’ source*,
  - *Flashing IoT device sw image*
  - *IoT platform reset*

- *Many more example….*
Low-critical cyber-physical managed systems

We need an Enhanced IoT managed Platform
Symphony high level overview

Key Features
- Modular
- Reliable
- Easy to use
- Customizable
AN&MONE as a Symphony module

Core Data Model

- Based on SAREF, SensorThings and other standard and proprietary extensions to cover common IoT devices, automation systems, A/V systems, etc.
- A dynamic resource catalogue maps any object’s interface to REST / gRPC endpoints

Core Services

- Powerful rule-based Event Management system
- Complete Alarm Management system (similar to OPC-UA)
- Multi-backend timeseries database
AN&MONE Architecture & Overview

- **Adaptation Layer:**
  - Retrieves the data from different sources and unifies them

- **Data Management:**
  - Stores and makes available the data to the other components

- **Decision Logic:**
  - Use the data to make decision based on predefined rules
  - Future use of AI model to understand the traffic patterns

- **Actuation Logic:**
  - Makes Reaction/Action to overcomes strange network behaviours
Benefits of using Ntopng (1/3)
Benefits of using Ntopng (2/3)

- **Deep interaction with the Symphony platform**

  - **IoT Stack**
    - **Application**
    - **Service**
    - **Semantics**
    - **Network**
    - **Connectivity**
    - **Physical**

  - **Business logic and human/machine interactions (UIs)**
  - **Understanding of the physical environment**
  - **A network-accessible object is endowed with a “meaning”**
  - **A conventional identity (ID) is assigned to each lower layer object.**
  - **An electric value is someway made accessible to an external component**
  - **Interaction with the physical world,**

---

AN&MONE

Ntop Conf'23
Benefits of using Ntopng (3/3)

Heat remote control / Alarm system
- Controlled by remote user
- Legit at network level
- Strange semantic pattern

Legend:
- IoT Platform
AN&MONE Decision logic
Next Steps (1/2)

- Aggregating the Ntopng data for
  - Data visualization
  - AI/ML training

- Continuous enhancement decision and actuation logic
  - New rules
  - Looking to AI/ML

- Use the AN&MONE platform both in the product side and in EU projects.
Robust-6G EU project – Smart Agriculture

- Compromise of the sensors to provide wrong values
- Discovery of compromised sensors using network patterns and other source of data
- Reaction
  - IoT device fresh and secure sw image
  - IoT Platform reset
  - New IoT Platform deployment
Questions?

Matteo Andolfi
R&D Project Manager
m.andolfi@nextworks.it

NEXTWORKS
HEADING THE FUTURE

info@nextworks.it
www.nextworks.it
HQ: via Livornese, 1027-29, 56122 Pisa (Italy)
Tel: +39-050-3871600
Fax: +39-050-3871601