Dynamic monitoring and protection of heterogeneous IoT applications

UCLouvain

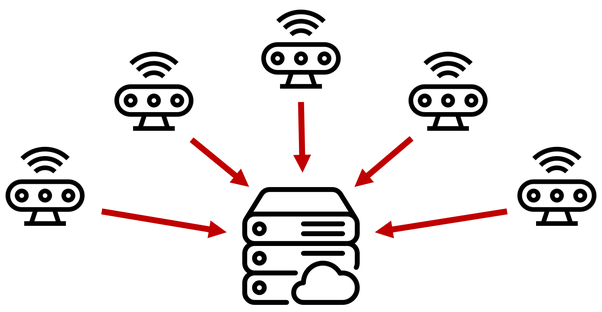
François De Keersmaeker, supervisor Ramin Sadre

fnrs

MOTIVATION

- **IoT devices are an easy target for attackers**
  - Limited computational resources
  - Always networked
  - Lack of updates (install & forget)
  - Users do not know security practices (default credentials, etc.)

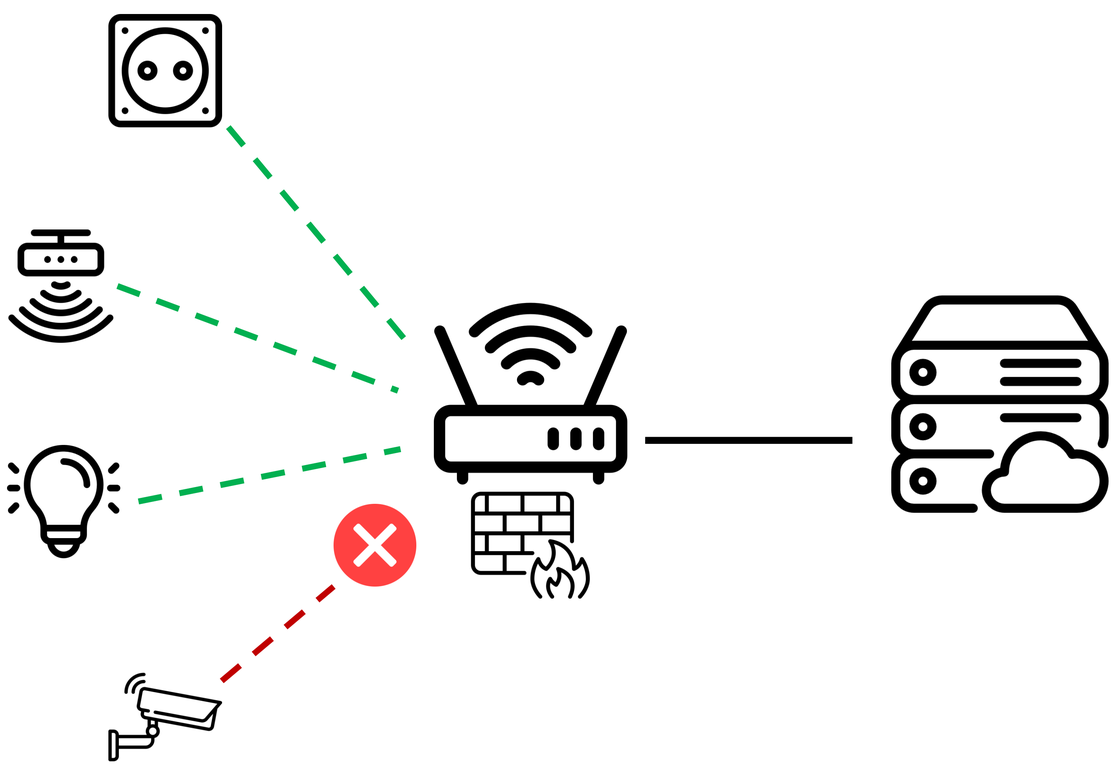
- Used in large-scale attacks
  - Famous example: the Mirai botnet
  - Peak at 600,000 devices and 600 Gbps traffic



- Difficult to protect
  - Cannot run protection system
  - No direct user interface

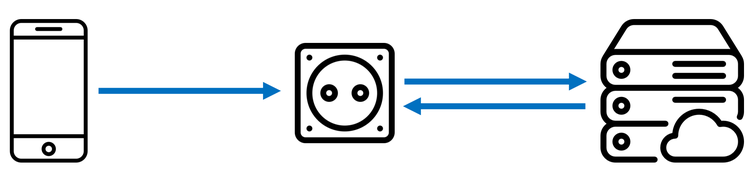
EVALUATION (Work in progress)

- Testbed of Smart Home IoT devices
- Install firewall on router
- Generate benign and malicious traffic



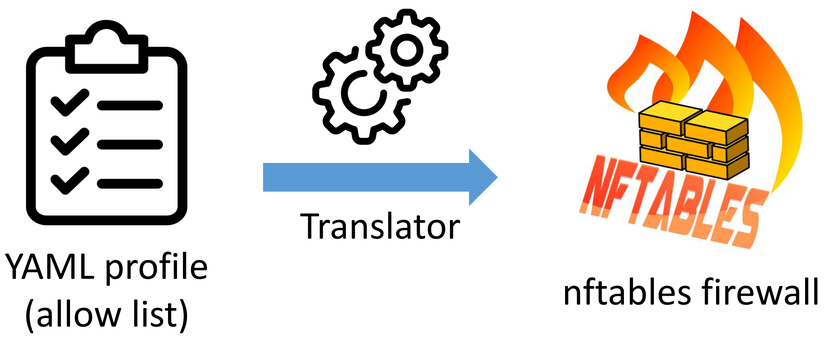
MAIN IDEA

- IoT behaviour is easily predictable



➔ Express this behaviour in the form of an **allow list**

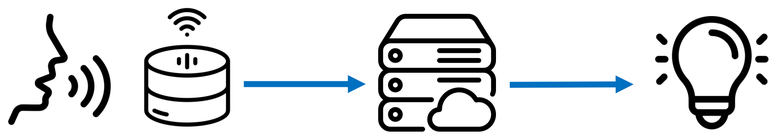
- Profile that specifies the authorized network traffic from/to the device (similar to MUD [1])
  - Allow only specified traffic
  - Block anything else
  - Concretely: translated to a **nftables firewall**



How to prevent unwanted traffic in IoT networks ?

NEW !

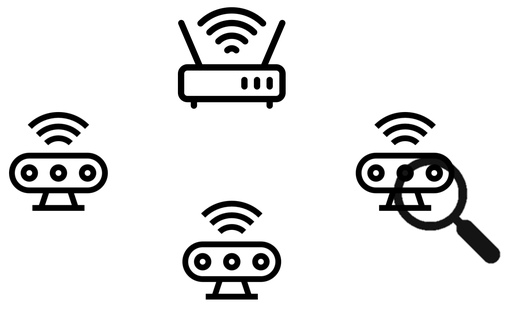
- Also based on **traffic statistics** (duration, packet count/rate, etc.)
- Support **complex patterns** resulting from **device interaction**



PERSPECTIVES

- Support non-IP, IoT-specific protocols

- Dynamic resource allocation in response to attacks
  - In the **Edge**, closer to the devices
  - In the **Cloud**, with a global view
- Automatic identification of IoT devices



References

[1] E. Lear, R. Droms, and D. Romascanu, “Manufacturer Usage Description Specification,” Internet Requests for Comments, RFC Editor, RFC 8520, Mar. 2019.

Icons from flaticon.com