"Supervising Smart Home Device Interactions: A Profile-Based Firewall Approach"

De Keersmaeker, François ; Sadre, Ramin ; Pelsser, Cristel

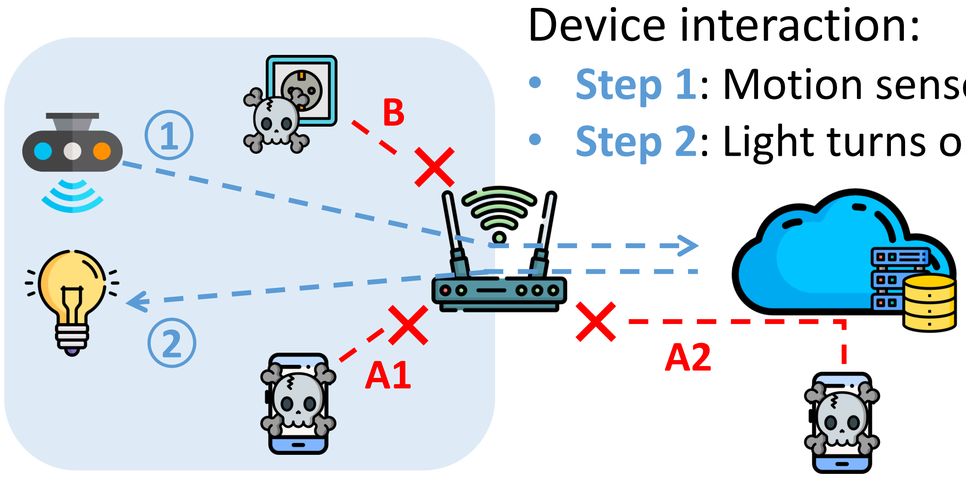
Supervising Smart Home Device Interactions: A Profile-Based Firewall Approach

François De Keersmaeker, Ramin Sadre, Cristel Pelsser

MOTIVATION

❖ **1. Observation:**
IoT devices are an easy target for attackers

❖ **2. Hypothesis:**
IoT devices have predictable network traffic patterns
➔ Express those patterns in the form of a **profile**
➔ **Allow-list** for network traffic



Device interaction:
- **Step 1**: Motion sensor activates
- **Step 2**: Light turns on

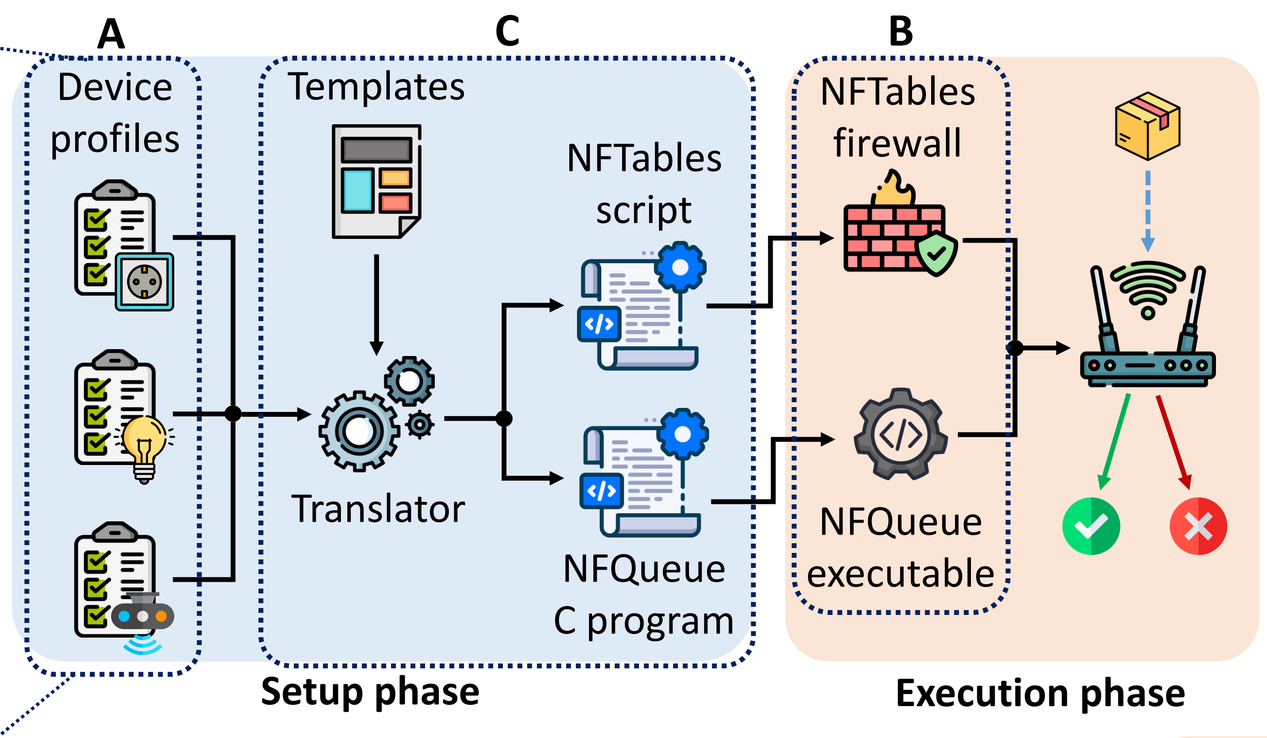
❖ **3. State-of-the-Art:**
IETF's MUD standard (RFC 8520 [1])
- MAC addresses, IP addresses, ports
- Other (application layer) protocols
  - (m)DNS, HTTP, IGMP, CoAP, etc.
- Traffic statistics
  - Duration, packet count, packet rate, etc.
- **Device interactions**
  - Core of home automation systems

❖ **4. Potential attacks complying with MUD profile**
✓ **A.** Spurious command, breaking the interaction patterns
A1. from LAN; **A2.** from WAN
✓ **B.** Compromised device communicating over DNS with attacker's server

A PROFILE-BASED & INTERACTION-AWARE SMART HOME FIREWALL

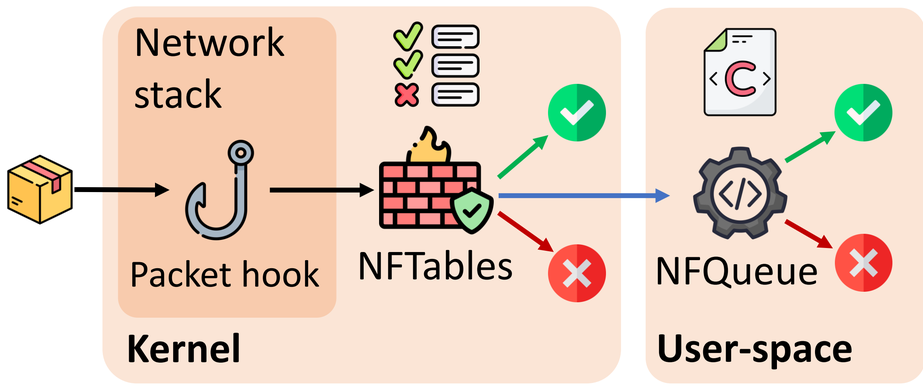
```
device-info:
  name: my-device
  mac: 00:11:22:33:44:55
  ipv4: 192.168.1.100

patterns:
  dns-p:
    protocols:
      dns:
        qtype: A
        domain-name: my.server.com
      udp:
        dst-port: 53
      ipv4:
        src: self
        dst: gateway
    bidirectional: true
    stats:
      packet-count: 4

interactions:
  dns-https-server:
    dns-server: !include patterns.dns-p
    https-server:
      protocols:
        tcp:
          dst-port: 443
        ipv4:
          src: self
          dst: my.server.com
      bidirectional: true
      stats:
        rate: 50/second
```

❖ **A.** Device profiles
➢ YAML format
➢ Addresses MUD shortcomings



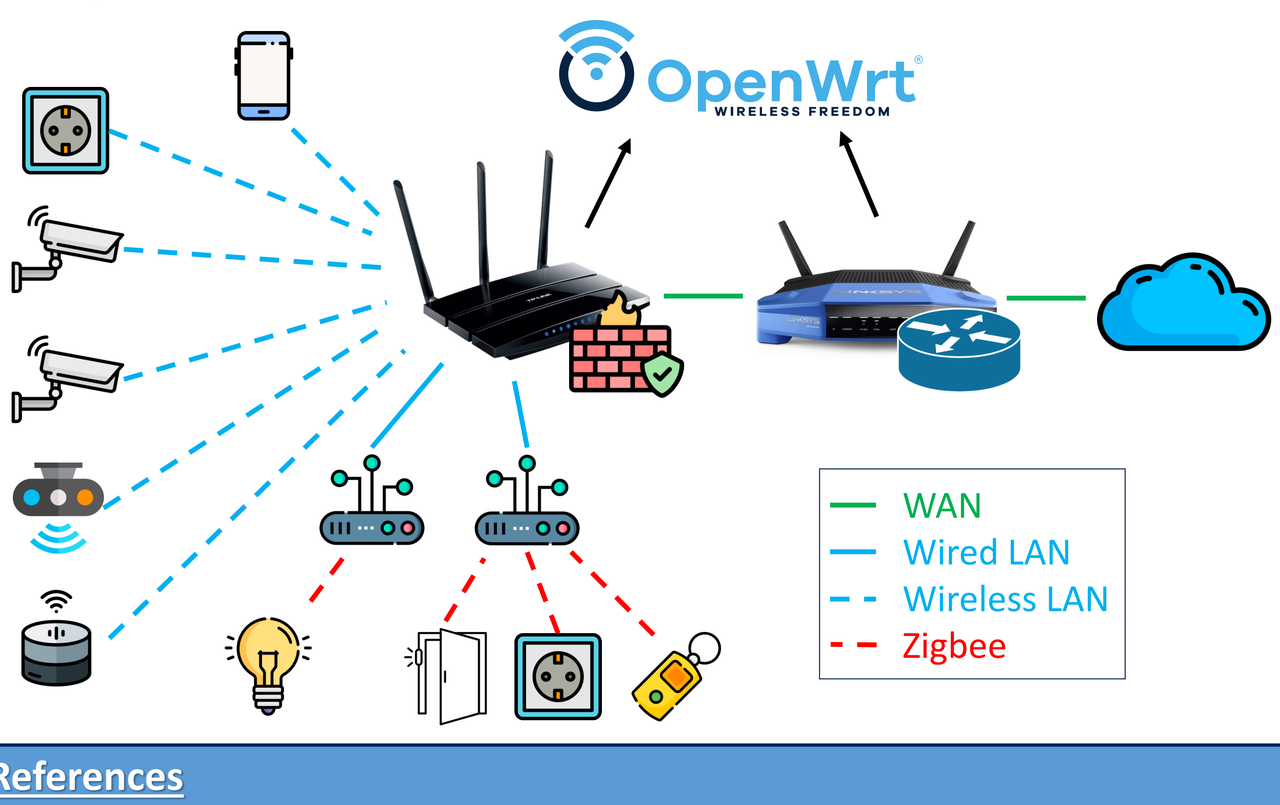
❖ **B.** Implemented with NFTables & NFQueue
➢ Novel Linux base firewall
✓ Lightweight & portable
➢ Inspects live traffic
➢ Offload packets to a user-space program for further processing
➢ Finite State Machine to support interactions

❖ **C.** Profile translator
➢ Input: device profiles and file templates
➢ Output: NFTables & NFQueue files

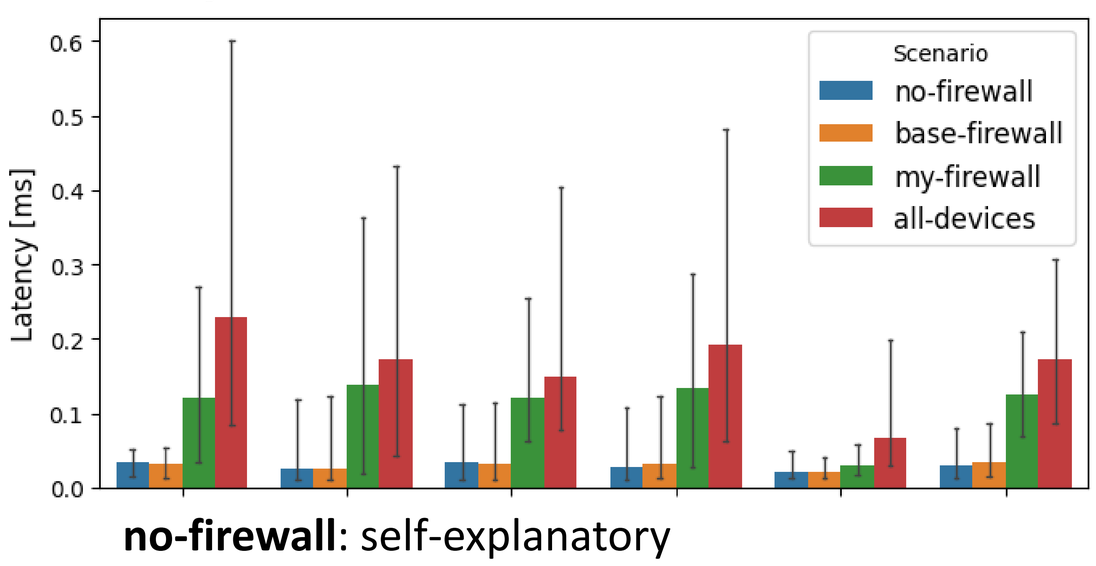


EVALUATION

❖ **Experimental network**



❖ **Latency in attack-free scenarios**



no-firewall: self-explanatory
base-firewall: default firewall
my-firewall: our firewall configured for **one** device
all-devices: our firewall configured for **all** 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