Adaptive Anomaly-Based Firewall for Smart Homes





Journée des Chercheurs CyberExcellence

François De Keersmaeker

2023-04-06

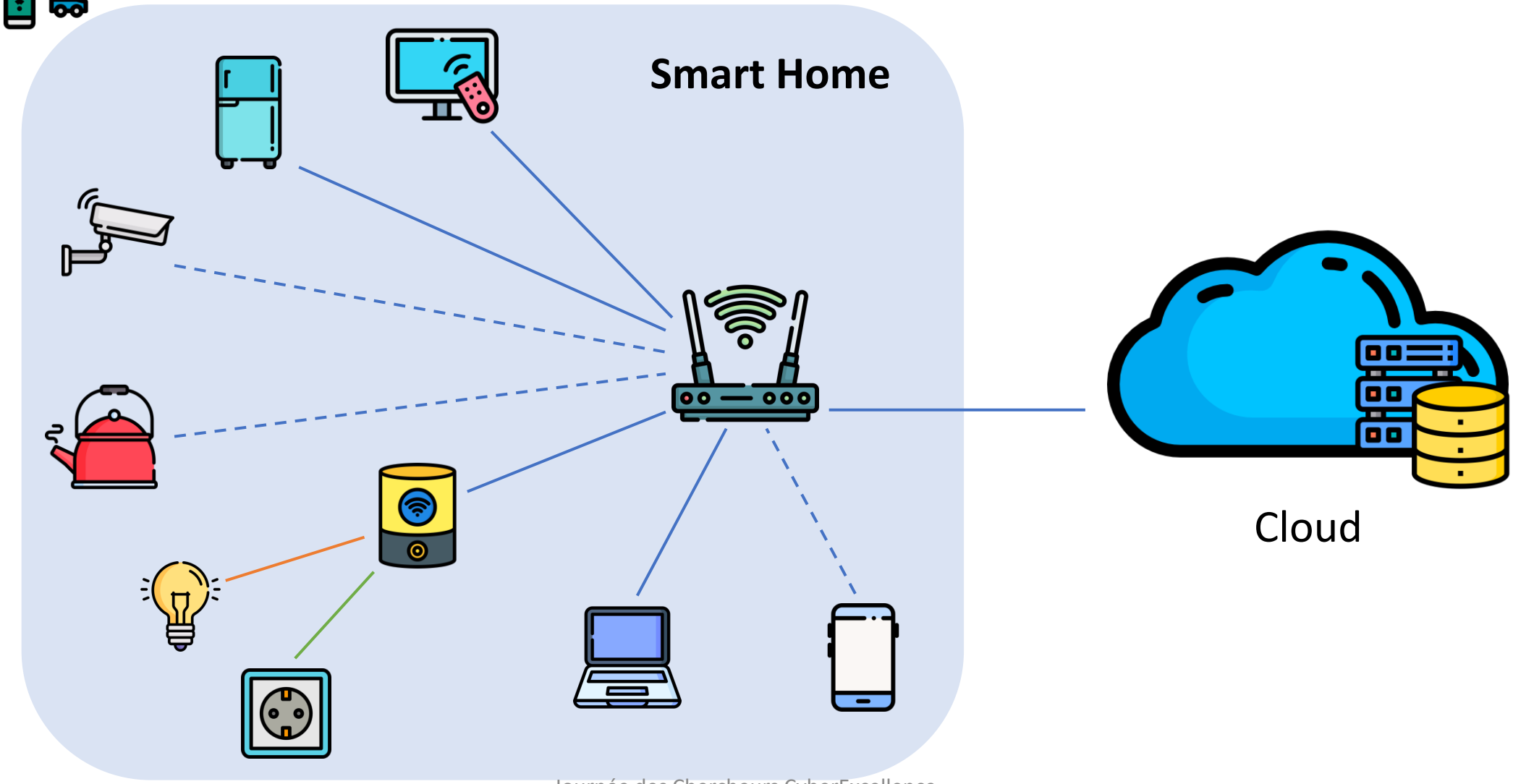
UCLouvain

fnrs
LA LIBERTÉ DE CHERCHER

Outline of the presentation

- Background
  - IoT / Smart Home networks
  - Smart Home device interactions
  - Smart Home security / privacy
  - MUD standard
- Solution system
- Evaluation

IoT / Smart Home networks



Smart Home device interactions

Smart Home

Turn on lamp !

Voice recognition

Cloud

Smart Home device interactions

Smart Home

Turn on lamp !

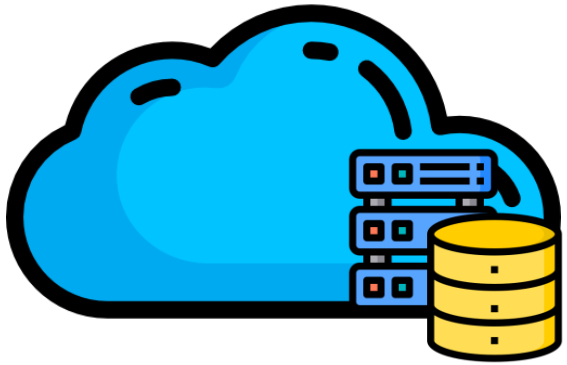
Issue command

Cloud

Smart Home device interactions

Smart Home

Turn on lamp !



Cloud

Issue command

Smart Home security

- IoT / Smart Home market is growing exponentially [1]
  - 2021: **99.89** billion $
  - 2028: **380.52** billion $

- Security is critical…
  - Present in user's home
  - Can represent a **safety** concern
- … but unsatisfactory
  - Easier to compromise than general purpose devices

- Attack example
  - Mirai (2016): 600,000 devices – 600 Gbps

[1] 'Smart Home Market Size, Share, Growth | Analysis Report, 2028'. https://www.fortunebusinessinsights.com/industry-reports/smart-home-market-101900 (accessed Apr. 04, 2023).

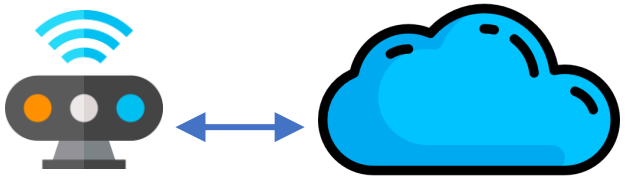
Smart Home security

Why is a smart home **vulnerable** ?

Users not aware

Login: admin
Password: admin

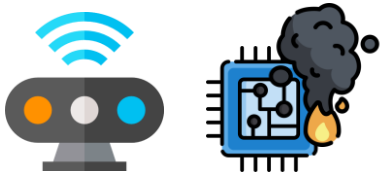
Devices always networked



Install & forget

Why is a smart home **difficult to protect** ?

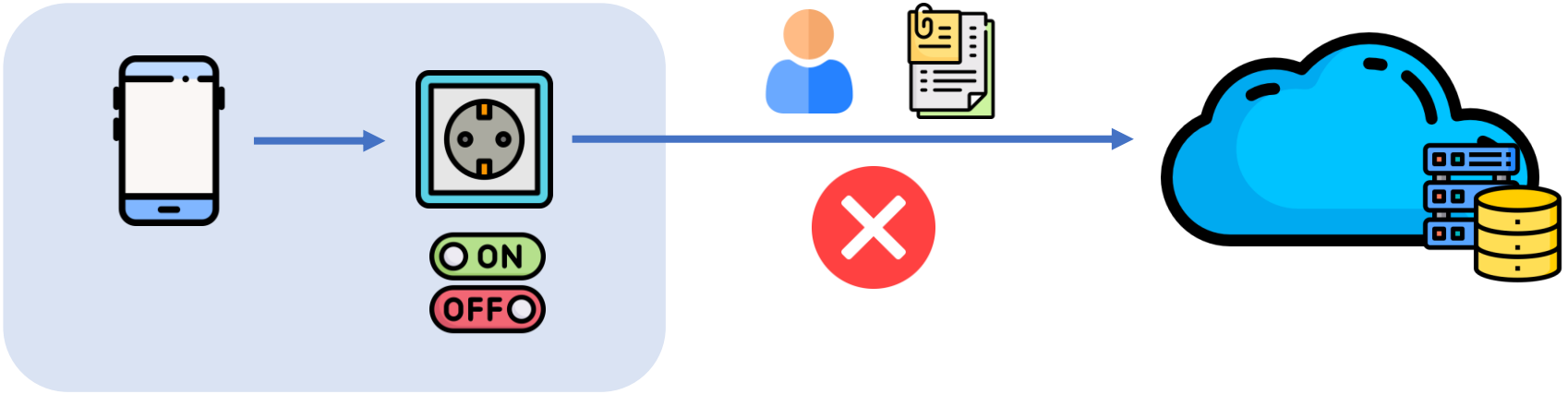
Limited computational resources



No direct user interface

Smart Home privacy

- User privacy is also a big concern
- Most devices disclose user data to manufacturer or third parties
- Unnecessary connections towards cloud
- Not required for operation



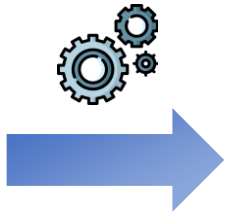
MUD Standard

IETF RFC 8520 [2]

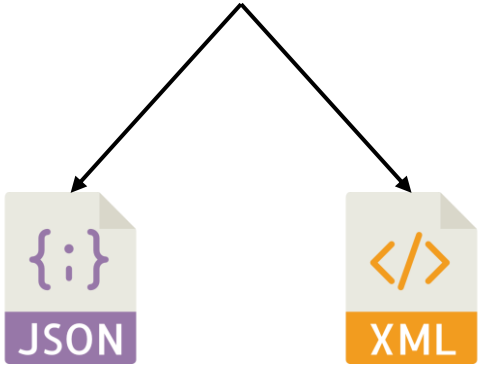
Manufacturer **U**sage **D**escription

Objectives:

- Exhaustively describe the behaviour of IoT devices
- Provide access control



Device profile



Shortcomings

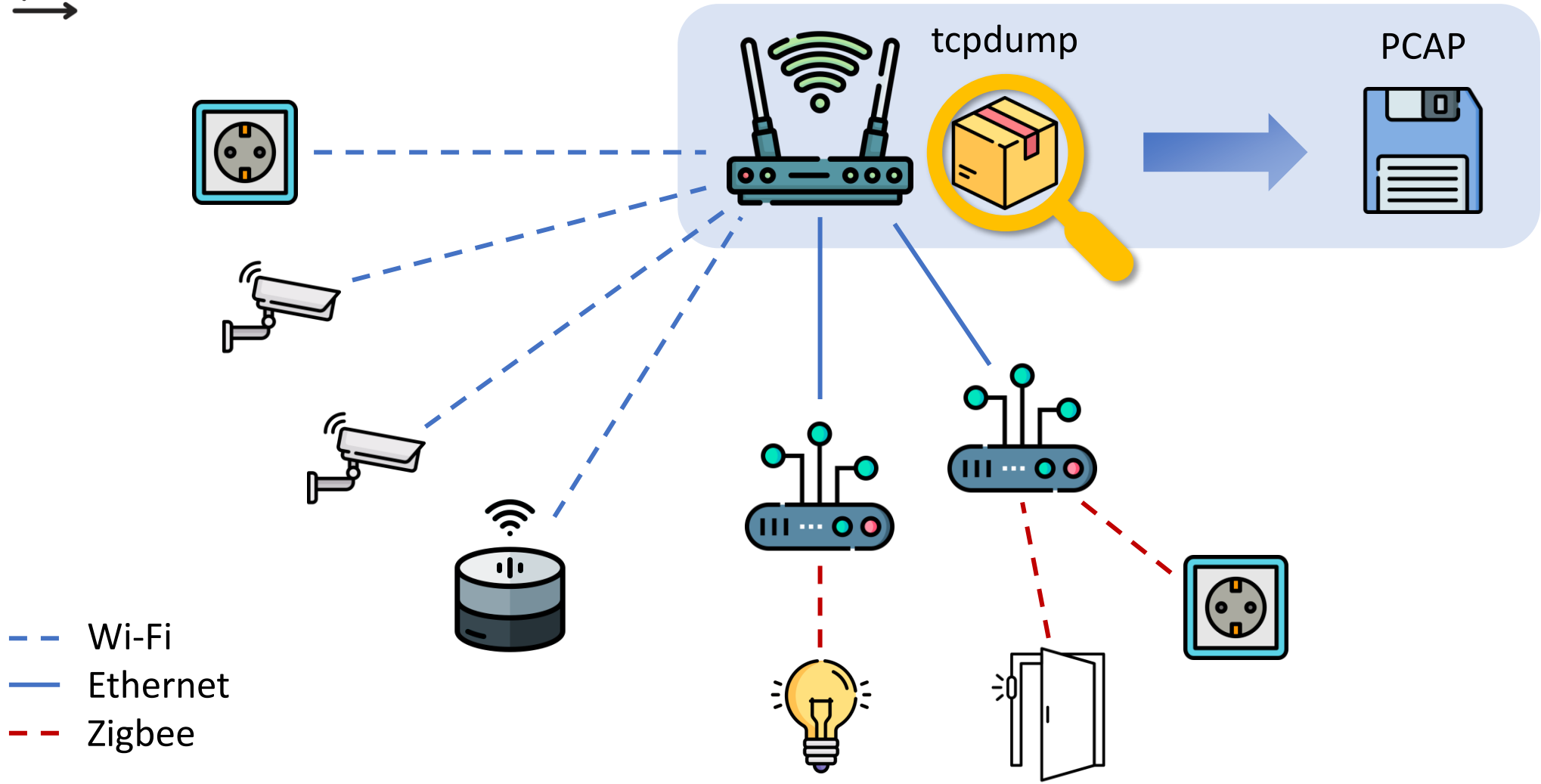
- Incomplete protocol support (e.g. no application layer, no IGMP)
- No traffic statistics (packet count/size/rate, duration)
- No support for interaction patterns

[2] E. Lear, R. Droms, and D. Romascanu, 'Manufacturer Usage Description Specification', RFC Editor, RFC8520, Mar. 2019. doi: 10.17487/RFC8520

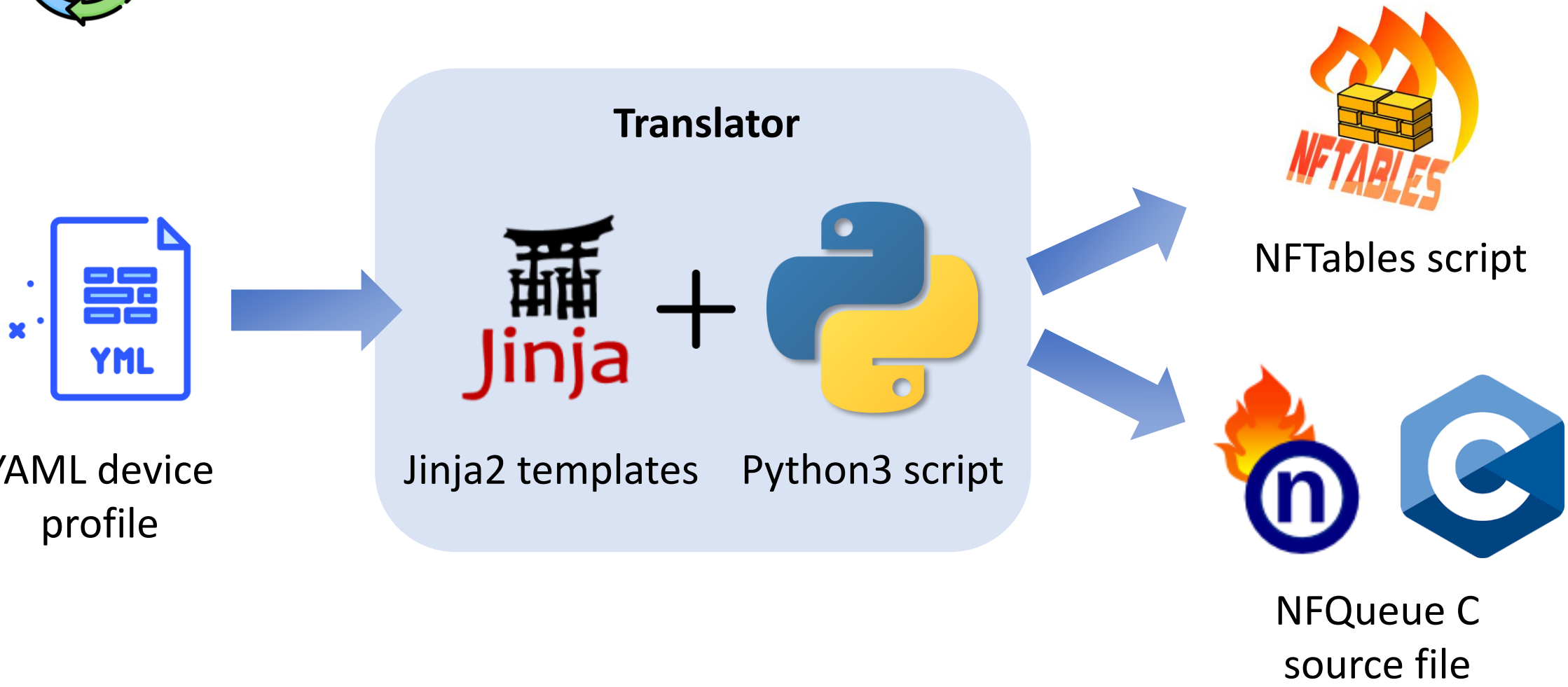
Outline of the presentation

- Background
- Solution system
  - Traffic collection
  - YAML device profiles
  - Smart Home firewall
  - Profile translator
- Evaluation

Traffic collection



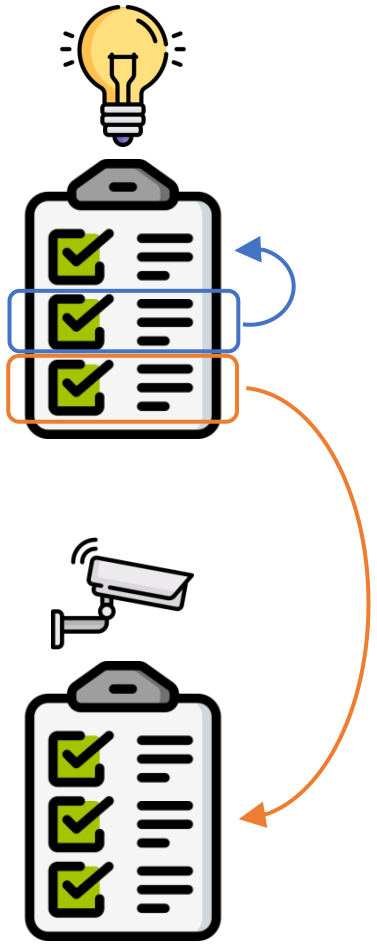
Full system workflow



YAML device profiles

Advantages

- Simpler syntax than JSON or XML
- Support for references to other fields
  - Same file
  - Other file



New features

- New protocols
  - Application layer (HTTP, DNS, CoAP, SSDP, etc.)
- Traffic statistics
  - Packet size
  - Packet count
  - Packet rate
  - Pattern duration
- Support for complex interaction patterns
  - Device A can communicate only if device B communicated before

YAML device profiles


```yaml
# Opening SmartThings app in local network
open-smartthings-app-local:

  open-app: !include ../smartthings-hub/profile.yaml#interaction-policies.open-app-local

  ssdp-response-hue:
    protocols:
      ssdp:
        response: true
      udp:
        src-port: 1900
      ipv4:
        src: self
        dst: local  # Mobile phone running the app
```

```yaml
# Open SmartThings app on mobile phone in local network
open-app-local:

  igmp-join-coap:
    protocols:
      igmp:
        version: 3
        type: membership report
        group: coap  # 224.0.1.187
      ipv4:
        src: local
        dst: igmpv3  # 224.0.0.22

  coap-multicast-ipv6:
    protocols:
      coap:
        type: NON
        method: GET
        uri: /oic/res?rt=x.com.samsung.provisioninginfo
      udp:
        dst-port: 5683
      ipv6:
        src: local
        dst: coap
```

```yaml
coap-multicast-ipv4:
  protocols:
    coap:
      type: NON
      method: GET
      uri: /oic/res?rt=x.com.samsung.provisioninginfo
    udp:
      dst-port: 5683
    ipv4:
      src: local
      dst: coap

igmp-join-ssdp:
  protocols:
    igmp:
      type: membership report
      group: ssdp  # 239.255.255.250
    ipv4:
      src: local   # Phone running app
      dst: igmpv3  # 224.0.0.22

ssdp-msearch:
  protocols:
    ssdp:
      method: M-SEARCH
    udp:
      dst-port: 1900
    ipv4:
      src: local  # Phone running app
      dst: ssdp   # 239.255.255.250
```

Full system workflow

YAML device profile

Translator

Jinja2 templates

Python3 script

NFTables script

NFQueue C source file

Smart Home firewall

NFTables

- New generation of Linux kernel packet filter
- Lightweight & portable
- Supersedes the well-known **IPTables**

<

Features

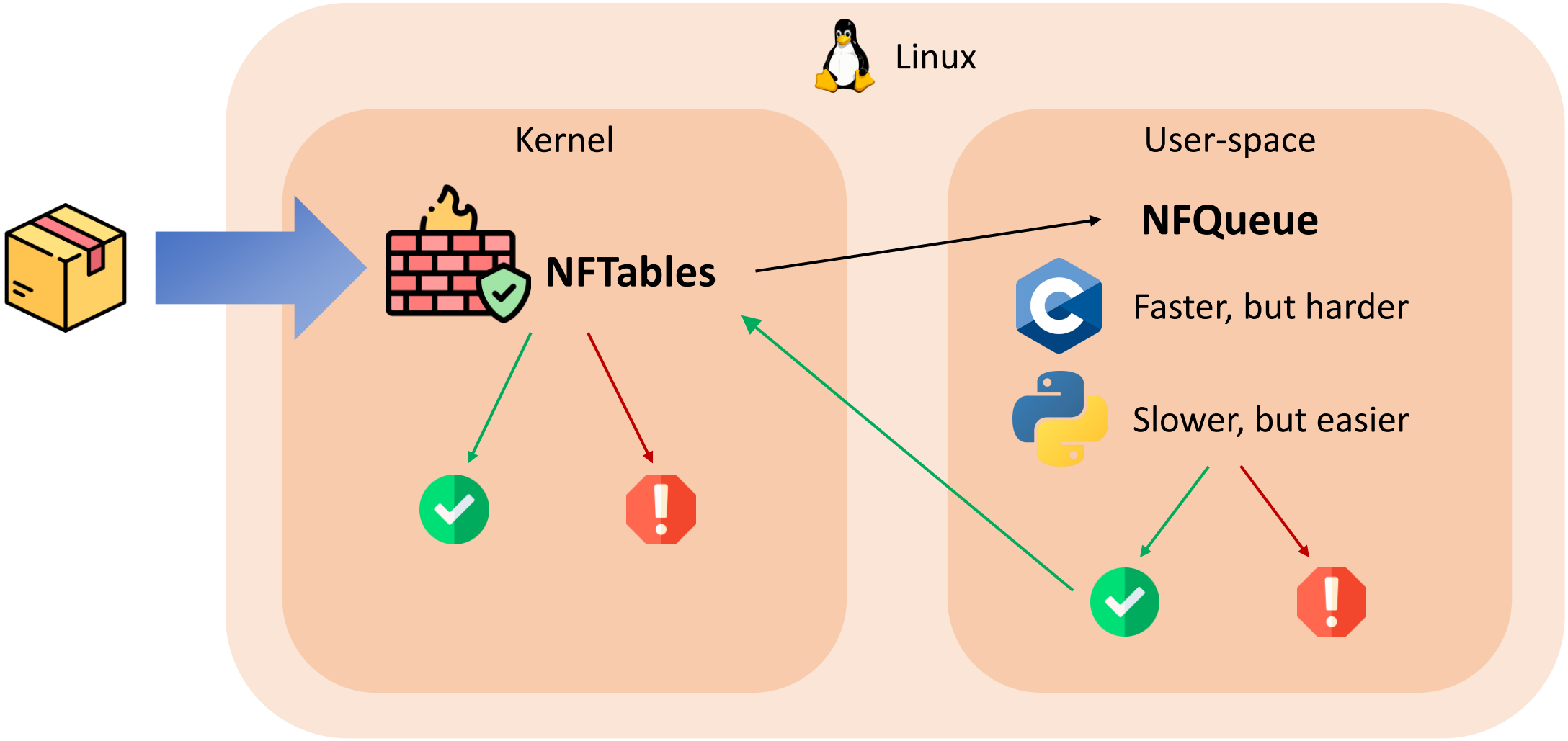
- Match packets in multiple places in the stack
- Connection tracking
- Traffic statistics
  - Packet rate
  - Packet size
- Send packets to a user-space program for further analysis with **NFQueue**

Others

Better suited for signature-based detection

Very versatile, but better suited for dealing with flows

NFQueue


Linux
Kernel
User-space
NFTables
NFQueue
Faster, but harder
Slower, but easier

YAML profile translator

YAML device profile

```yaml
# Opening SmartThings app in local network
open-smartthings-app-local:

  open-app: !include ../smartthings-hub/profile.
  yaml#interaction-policies.open-app-local

ssdp-response-hue:
  protocols:
    ssdp:
      response: true
    udp:
      src-port: 1900
    ipv4:
      src: self
      dst: local  # Mobile phone running the app
```

NFQueue C source file

```c
// Policy open-smartthings-app-local-ssdp-response-hue
pthread_mutex_lock(&(interactions_data[15].mutex));
if (
    (interactions_data[15].current_state == 4)
    && (!ssdp_message.is_request)
) {
    // Policy is one-off, increment state
    #ifdef DEBUG
    printf("open-smartthings-app-local-ssdp-response-hue: State %hhu
    -> State 0\n", interactions_data[15].current_state);
    #endif
    interactions_data[15].current_state = 0;

    if (verdict != NF_STOP) {
        verdict = NF_STOP;
        accepted_packets++;
    }
    #ifdef DEBUG
    printf("Accept: policy
    open-smartthings-app-local-ssdp-response-hue, state = %hhu\n",
    interactions_data[15].current_state);
    printf("Accepted packets: %hu\n", accepted_packets);
    #endif

}
pthread_mutex_unlock(&(interactions_data[15].mutex));
```

Full system workflow

YAML device profile

Translator

Jinja2 templates

Python3 script

NFTables script

NFQueue C source file

Outline of the presentation

- Background
- Solution system
- Evaluation
  - RTT vs Data Rate
  - Next steps

Evaluation: RTT vs Data Rate

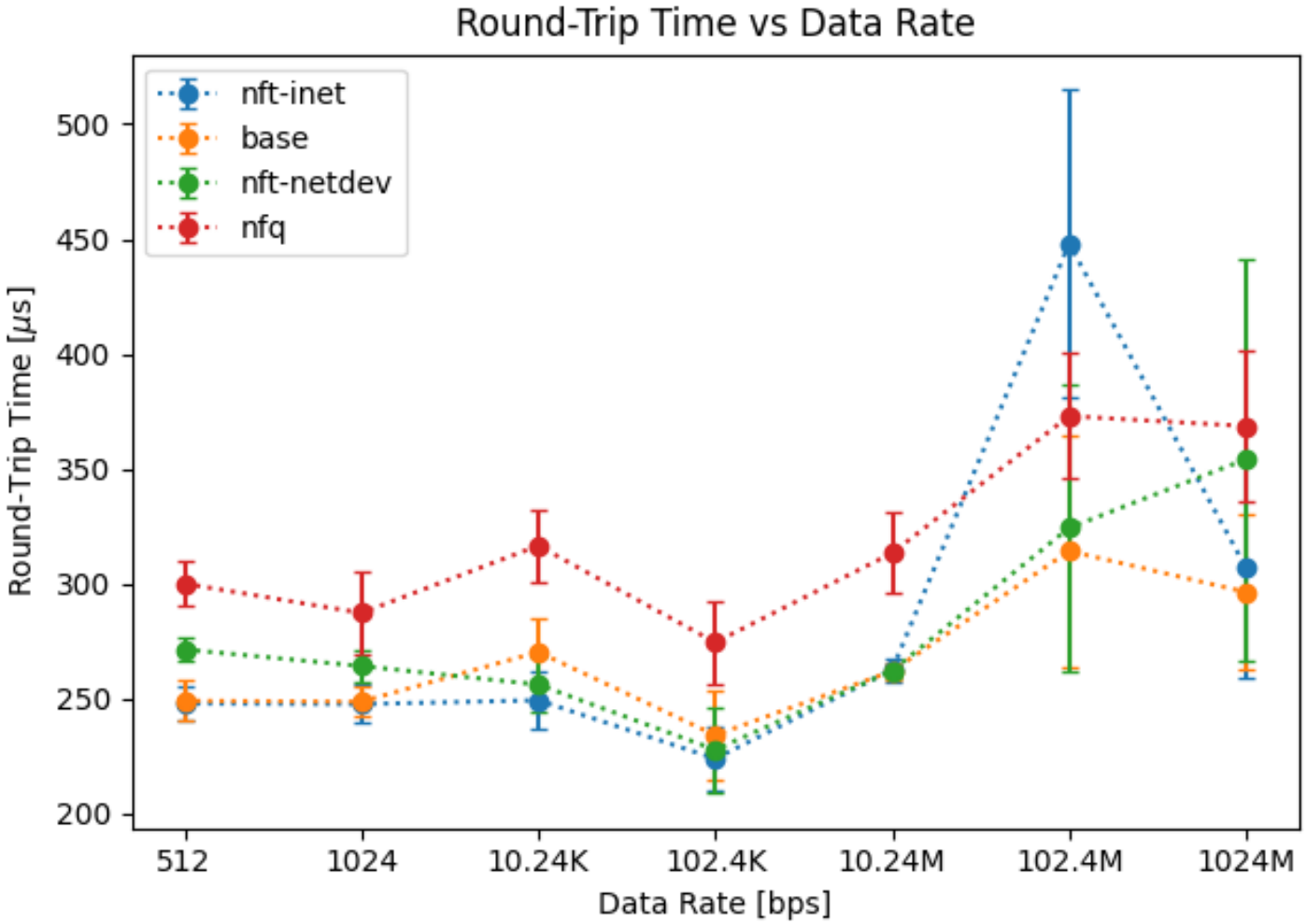
- Objective: measure latency
  - Without firewall
  - With firewall, nftables only (no user-space processing)
  - With firewall, nfqueue (with user-space processing)

iperf3 client

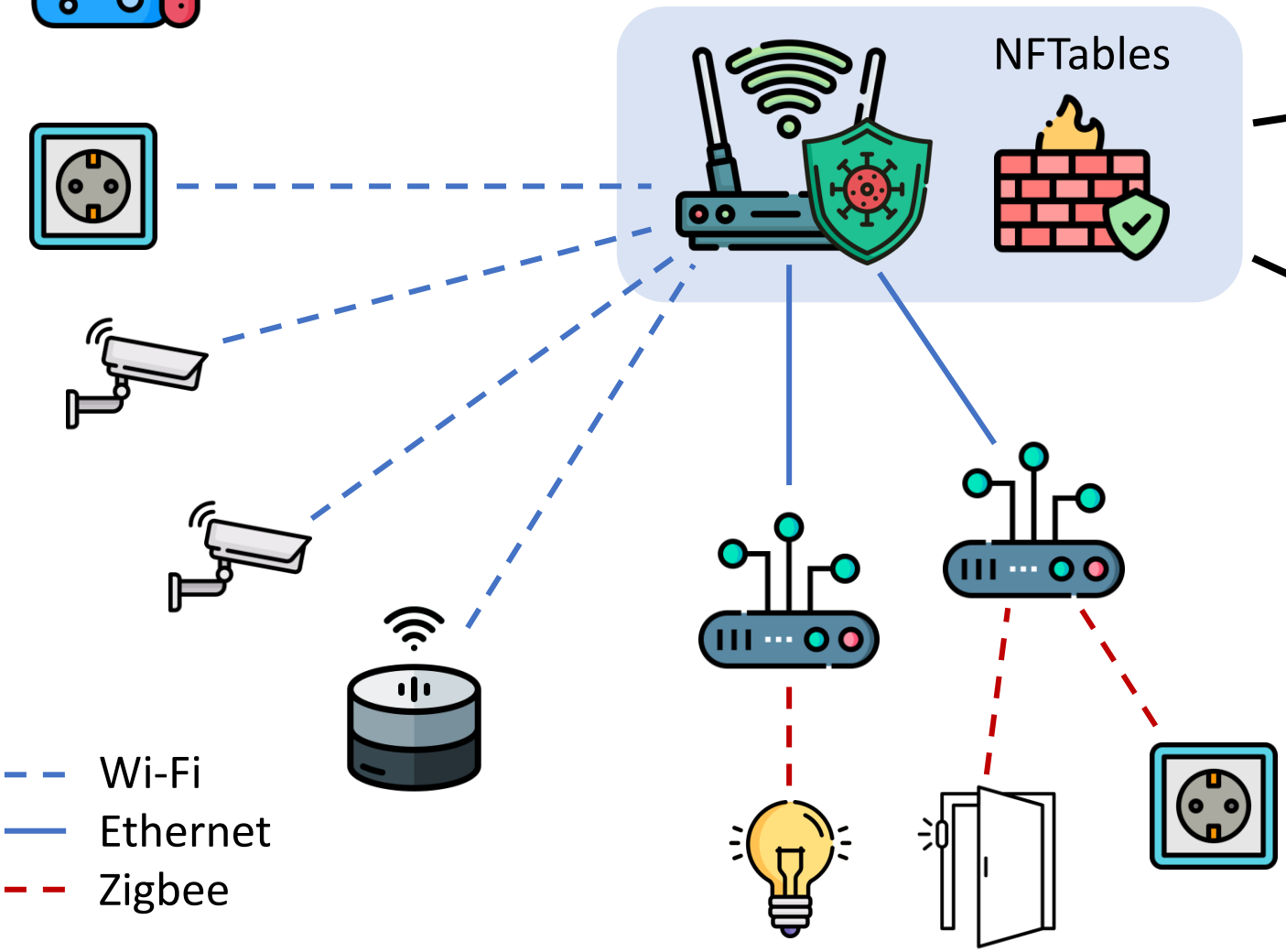
interface — interface

iperf3 server
- No firewall
- nft, inet
- nft, netdev
- nft + nfqueue

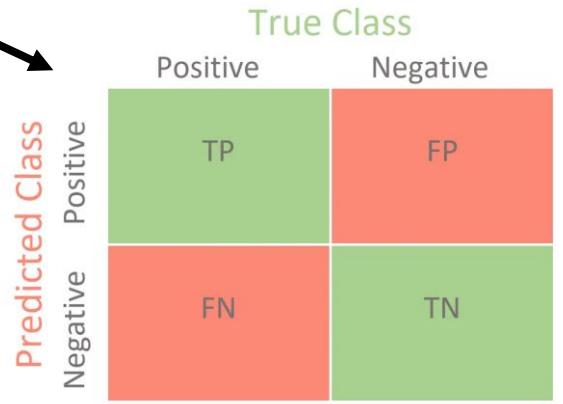
Evaluation: RTT vs Data Rate



Evaluation: Next steps



Measure RTT
in real setting



Confusion matrix

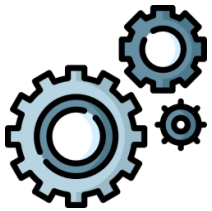
Adaptive Anomaly-Based Firewall for Smart Homes





Icons from flaticon.com

YAML profile translator



Jinja2 templates

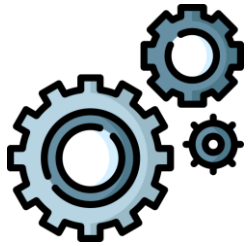
+

Python3 script

YAML profile

yaml_loader

jinja2



Translator

NFTables script

NFQueue C source file

header.c.j2

callback.c.j2

main.c.j2

firewall.nft.j2

Policy.py

NFQueue.py

Protocol.py

ip

tcp

dns

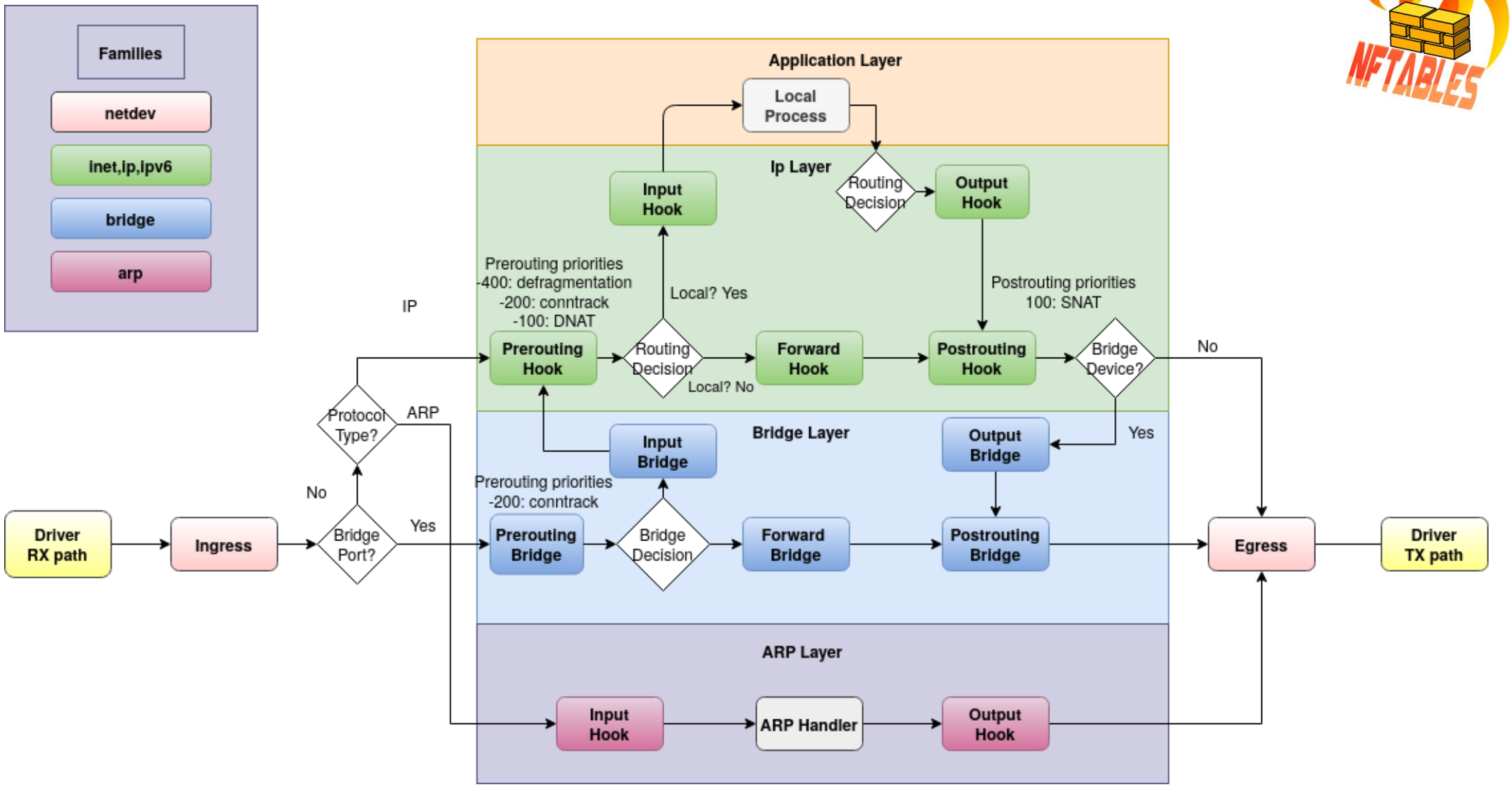
MUD Standard

Existing extensions

- Bandwidth profiling (packet / bitrate) / QoS [3]
- TLS parameters [4]
- Application-layer resource [5]
- Well-known malicious traffic signatures [6]
- Privacy, resource authorization, channel protection (using MSPL) [7]

[3] E. Lear and O. Friel, 'Bandwidth Profiling Extensions for MUD', Internet Engineering Task Force, Internet-Draft draft-lear-opsawg-mud-bw-profile-01, Jul. 2019. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-lear-opsawg-mud-bw-profile-01
[4] T. Reddy.K, D. Wing, and B. Anderson, 'MUD (D)TLS profiles for IoT devices', Internet Engineering Task Force, Internet-Draft draft-reddy-opsawg-mud-tls-05, Aug. 2020. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-reddy-opsawg-mud-tls-05
[5] S. N. Matheu, J. L. Hernández-Ramos, S. Pérez, and A. F. Skarmeta, 'Extending MUD Profiles Through an Automated IoT Security Testing Methodology', IEEE Access, vol. 7, pp. 149444–149463, 2019, doi: 10.1109/ACCESS.2019.2947157.
[6] S. Morais and C. Farias, 'INXU - A Security Extension for RFC 8520 to Give Fast Response to New Vulnerabilities on Domestic IoT Networks', in Proceedings of the 7th Workshop Pré-IETF, Porto Alegre, RS, Brasil: SBC, 2020, pp. 1–14. doi: 10.5753/wpietf.2020.13792.
[7] S. N. Matheu et al., 'Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems', Sensors, vol. 20, no. 7, Art. no. 7, Jan. 2020, doi: 10.3390/s20071882.

NFTables hooks



https://wiki.nftables.org/wiki-nftables/index.php/Netfilter_hooks