INSPIRE-5Gplus

MUD/Manifest

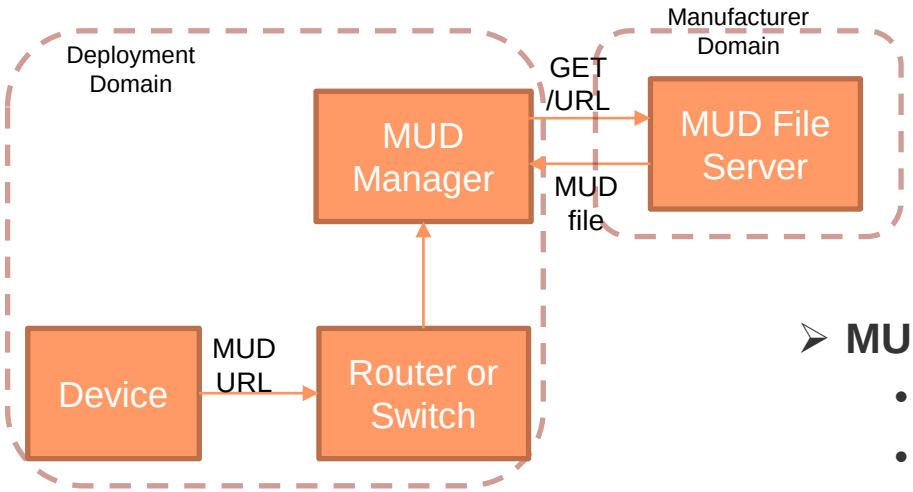
Managing dependencies in the 5G environment through MUD files

WAL5Gplus Workshop

Sara Nieves Matheu Garcia
University of Murcia (UMU)

MUD STANDARD

- **Manufacturer Usage Description (MUD)**
  - IETF standard (2019), well received by the community (e.g., NIST)
  - Manufacturer's responsibility



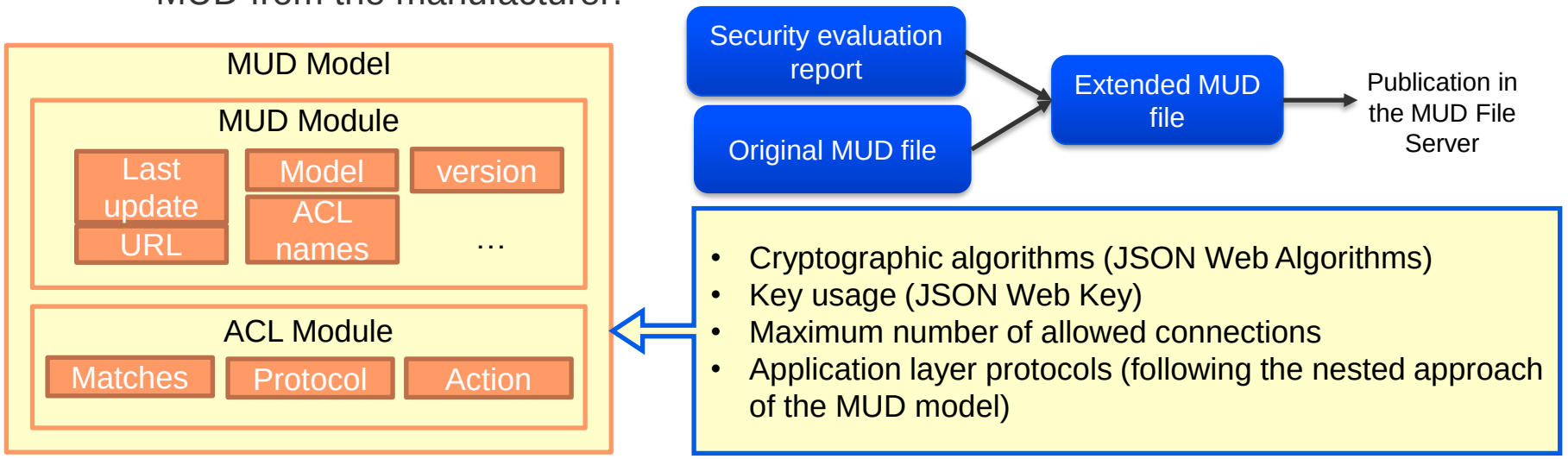
- Standardization
- Scalability
- Flexibility (high level words)
- Extensible (e.g., QoS)

- **Limited to network behavior**
- **Usage limited to give recommendations**

- **MUD Architecture**
  - Device: Sends the MUD URL.
  - Router or switch: Obtains the MUD URL.
  - MUD Manager: Obtains, validates, translates and enforces the MUD policies.
  - MUD File Server: Stores the MUD file.

MUD STANDARD

- **Problem:** MUD expressiveness limited to network behavior.
- **Our proposal (V1):**
  - MUD model extension to integrate additional security aspects beyond network layer.
  - Generation of the extended MUD from the security evaluation and the original MUD from the manufacturer.



INSPIRE-5Gplus

```
module: ietf-access-control-list
  +--rw access-lists
     +--rw acl* [name]
        |  +--rw name
        |  +--rw type?
        |  +--rw aces
        |  +--rw ace* [name]
        |     +--rw name
        |     +--rw matches
        |     |  +--rw mud
        |     |  |  +--rw manufacturer?
        |     |  |  +--rw same-manufacturer?
        |     |  |  +--rw model?
        |     |  |  +--rw local-networks?
        |     |  |  +--rw controller?
        |     |  |  +--rw my-controller?
        |     |  +--rw direction-initiated?
        |     |  +--rw eth?
        |     |  +--rw ipv4?
        |     |  +--rw ipv6?
        |     |  |  +--rw dscp?
        |     |  |  +--rw ecn?
        |     |  |  +--rw length?
        |     |  |  +--rw ttl?
        |     |  |  +--rw protocol?
        |     |  |  +--rw (destination-network)?
        |     |  |  +--rw (source-network)?
        |     |  |  +--rw flow-label?
        |     |  +--rw tcp?
        |     |  +--rw udp?
        |     |  |  +--rw length?
        |     |  |  +--rw source-port
        |     |  |  +--rw destination-port
        |     |  |  +--rw application-protocol?
        |     |  +--rw icmp?
        |     |  +--rw [application-protocol-name]?*
        |     |  |  +--rw application-protocol?
        |     |  |  +--rw num-connections?
        |     |  |     +--rw operator
        |     |  |     +--rw value
        |     |  |  +--rw keys?
        |     |  |     +--rw alg*
        |     |  |     +--rw crv?*
        |     |  |     +--rw key_ops*
        |     |  +--rw egress-interface?
        |     |  +--rw ingress-interface?
        |     +--rw actions
        |     |  +--rw forwarding
        |     |  +--rw logging?
        |     +--ro statistics
        +--rw attachment-points
```

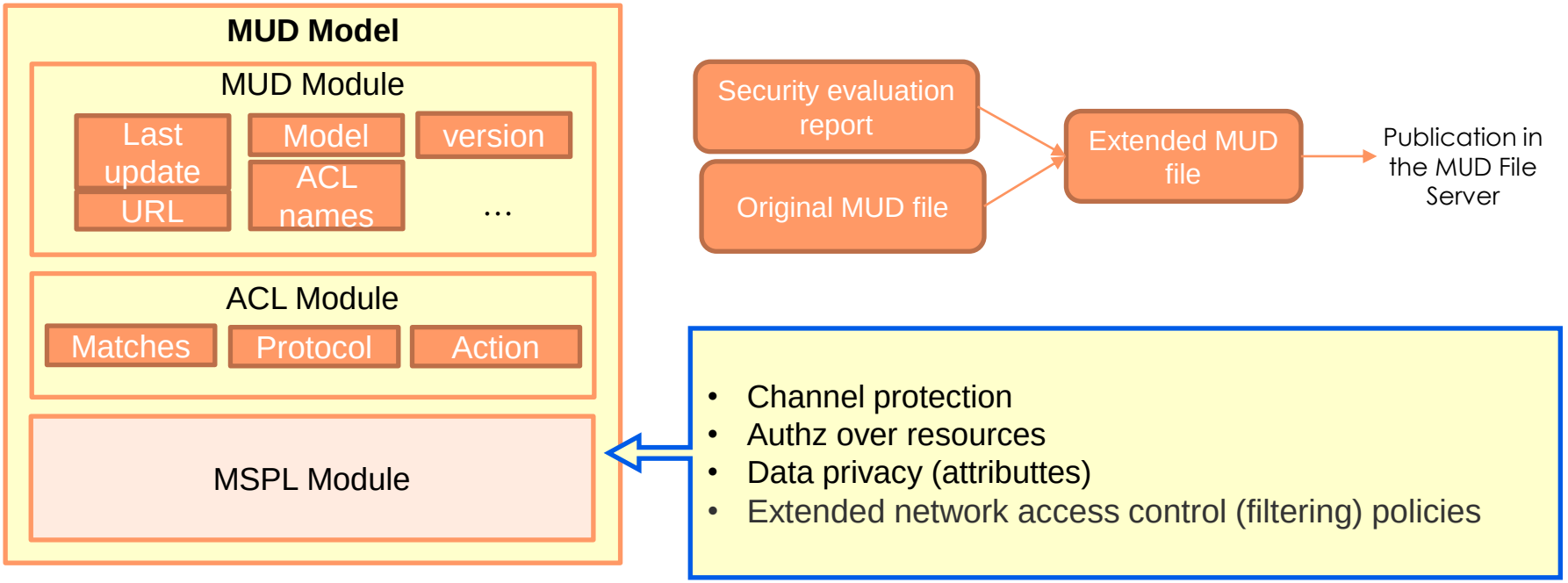
Nested approach

JWK, JWA

We are currently working on a refinement of this approach in BIECO project to include HTTP resources, authZ, CVE/CWE vulnerabilities

MUD STANDARD

- **Our proposal (V2):** https://www.mdpi.com/1424-8220/20/7/1882
  - è MUD model extension based on ANASTACIA internal policy description language MSPL (Medium-level Security Policy Language). A new block after ACL module.



MSPL: https://www.secured-fp7.eu/files/secured_d41_policy_spec_v0100.pdf
MSPL in ANASTACIA:
https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c03f6297&appId=PPGMS

```
rw from-device-policy
    |   rw acls
    |       |   rw access-list* [name]
    |       |       rw name -> /acl:acls/acl/name
    |   rw mspls
    |           rw mspl-list* [name]
    |               rw name -> /mspl:mspls/mspl/name
rw to-device-policy
        rw acls
            |   rw access-list* [name]
            |       rw name -> /acl:acls/acl/name
        rw mspls
                rw mspl-list* [name]
                    rw name -> /mspl:mspls/mspl/name
```

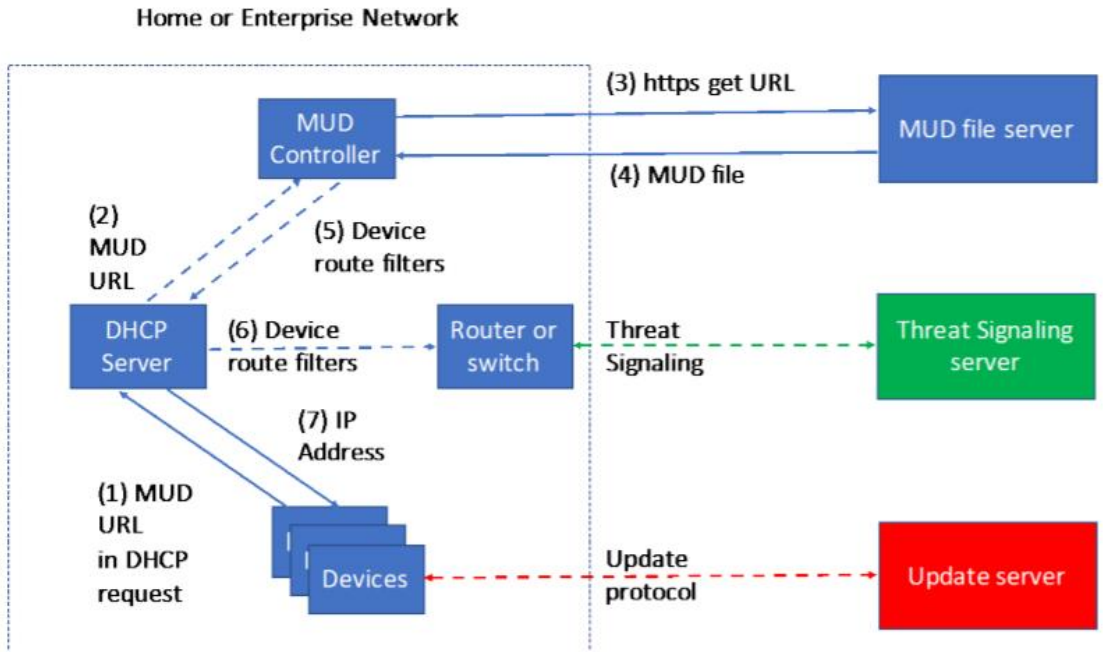
```
module: umu-mspl-list
    |    rw mspls
    |        rw mspl* [name]
    |            rw name    string
    |            rw configuration
    |                capability    string
    |                configuration-rules
    |                    rw configuration-rule* [name]
    |                        |   rw configuration-rule-action
    |                        |   rw configuration-rule-condition
    |                    rw name
    |                    rw priority
end_module
```

MORE INFO: https://www.mdpi.com/1424-8220/20/7/1882

Threat MUD

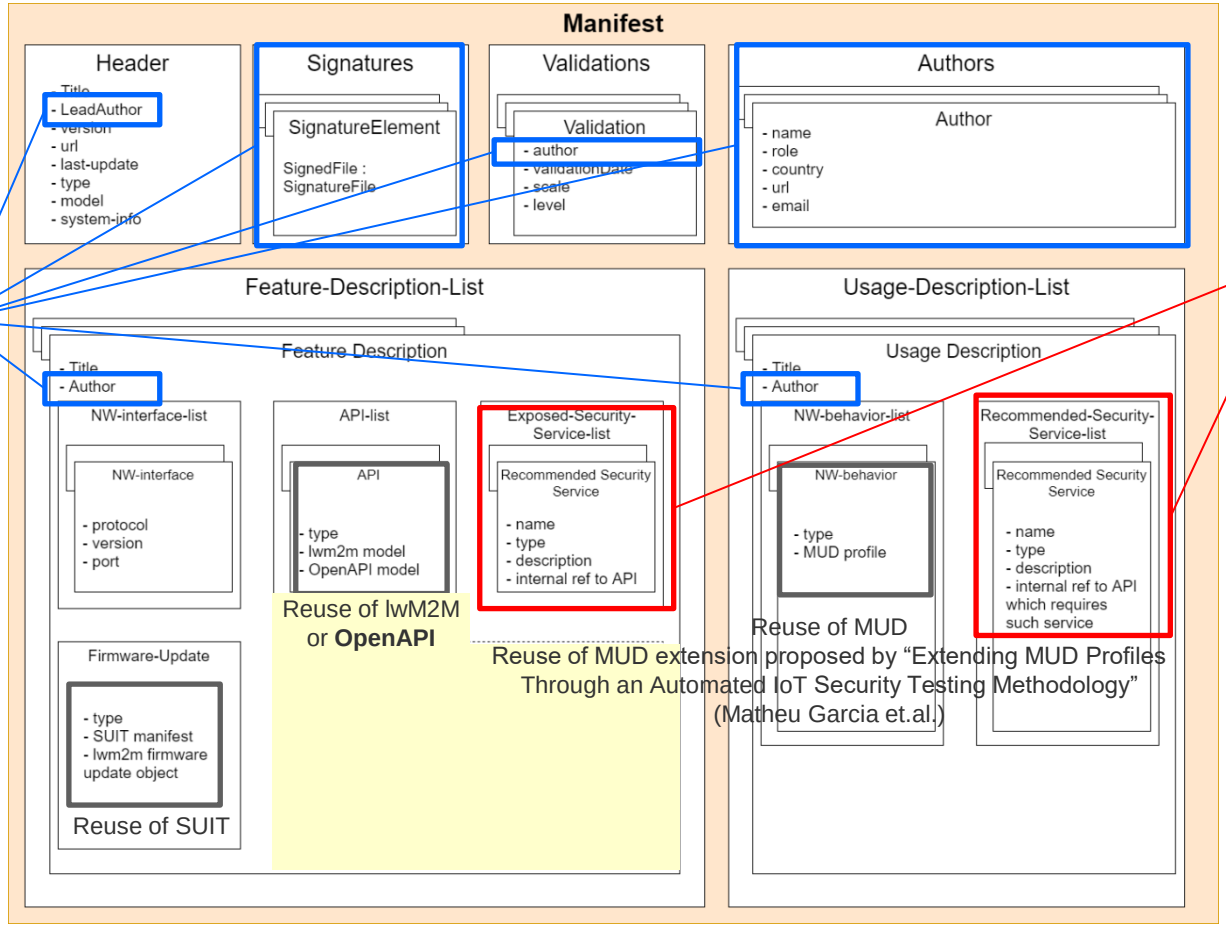
INSPIRE-5Gplus

- The same format as MUD files
- List only external sites to and from which traffic should be prohibited because the sites are associated with a given threat
- The threat MUD file is designed to list all domains and IP addresses that are associated with any given threat that should be blocked.



https://www.nccoe.nist.gov/publication/1800-15/VolB/index.html

Manifest v0.1 – adapted for IoT (ORANGE)



Endorsement of responsibilities, requires PKI infrastructure, managed by an entity such as GP for IoT or another relevant group.

New, can help for SD-IOT VNF orchestration for security function placement

Integration in the Orange's manifest

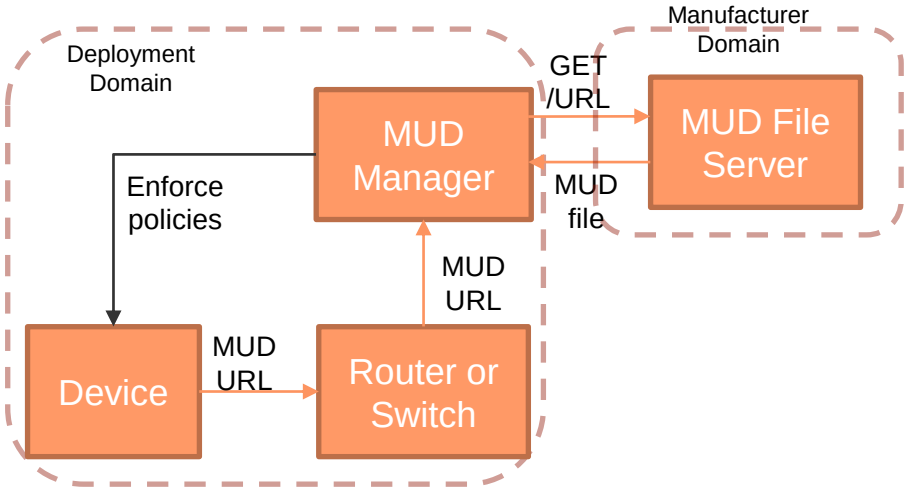
- MUD file as part of the manifest. **Different views:**
  - Manufacturer can certify that under those conditions the system is secure. And beyond that, he is not responsible.
  - Manufacturer can give recommendations to protect the device during runtime
  - MUD file to monitor suspicious behaviours.
  - It is possible also to create a MUD at runtime, from the network behaviour of the device (mudgee tool).
- Policies from the MUD file can be enforced using SDNs.
- The MUD can be more extended if necessary.

Integration in the Orange's manifest

- We can also include the Threat MUD file (proposed by the NIST)
  - MUD associated to a specific threat
  - The MUD specifies the mitigations (Which domains should be avoided because they are compromised)
  - **Dynamic**
  - Fast application of mitigations

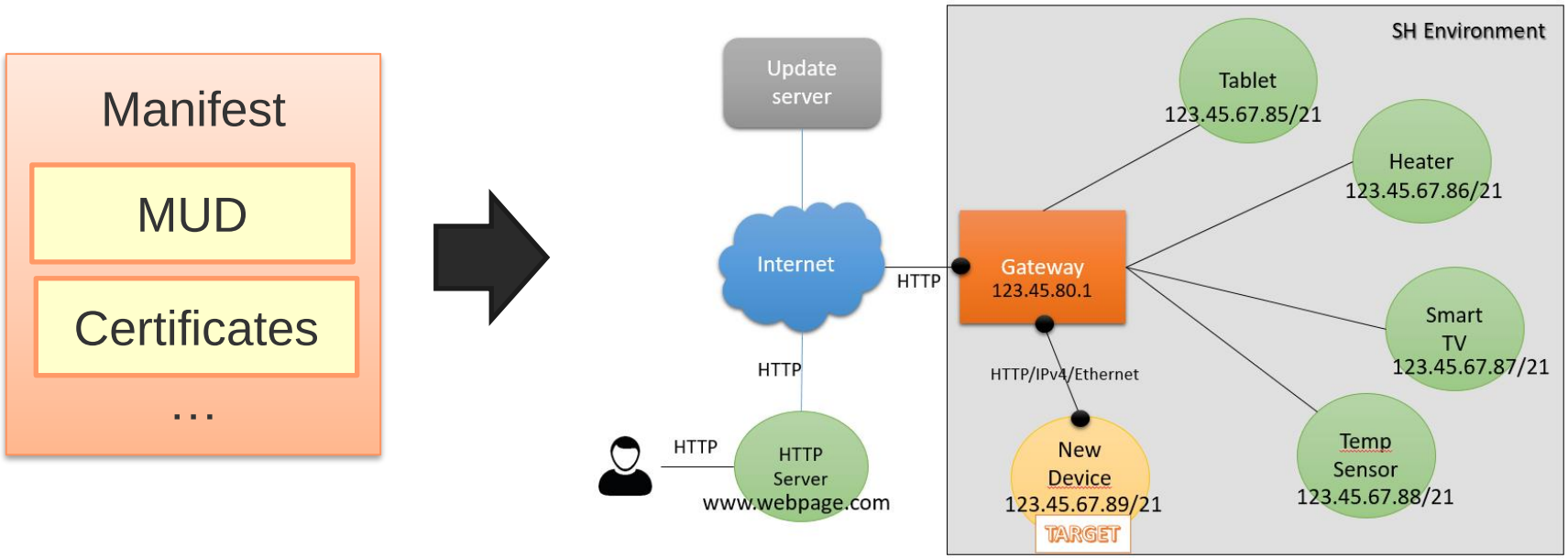
Possible Usage

- **As a way to configure in a secure way the device**
  - Manufacturer indicates security recommendations (policies) inside the MUD
  - MUD obtaining is performed during the bootstrapping (EAP-PSK-AAA)
  - Policies are enforced before the system can access to the network (reduced attack surface).
  - More information: https://www.mdpi.com/2076-3417/9/21/4576



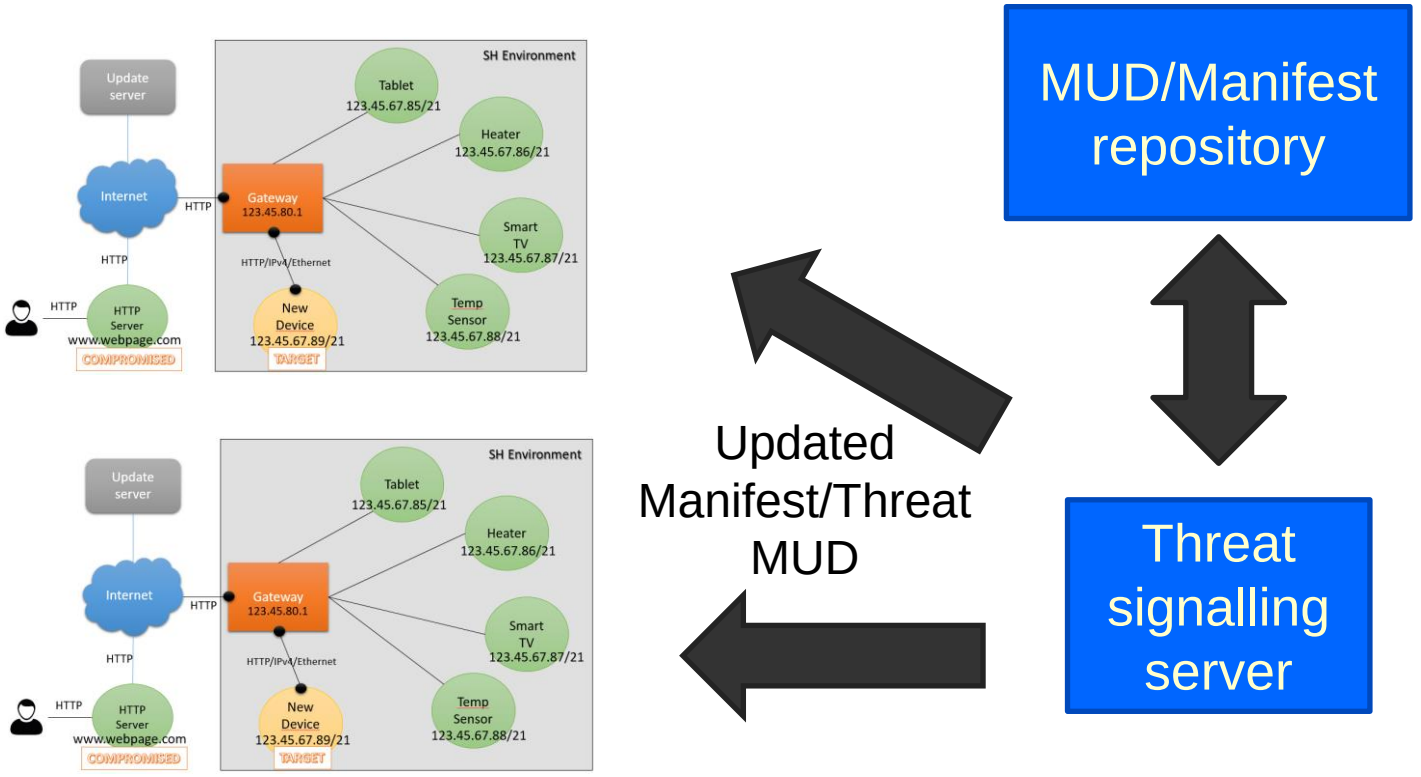
Possible Usage

- **Manage 5G dependencies and send information about mitigations**
  - Manifest and MUD includes information from certificates and network communications → Dependencies with other components and services are known



Possible Usage

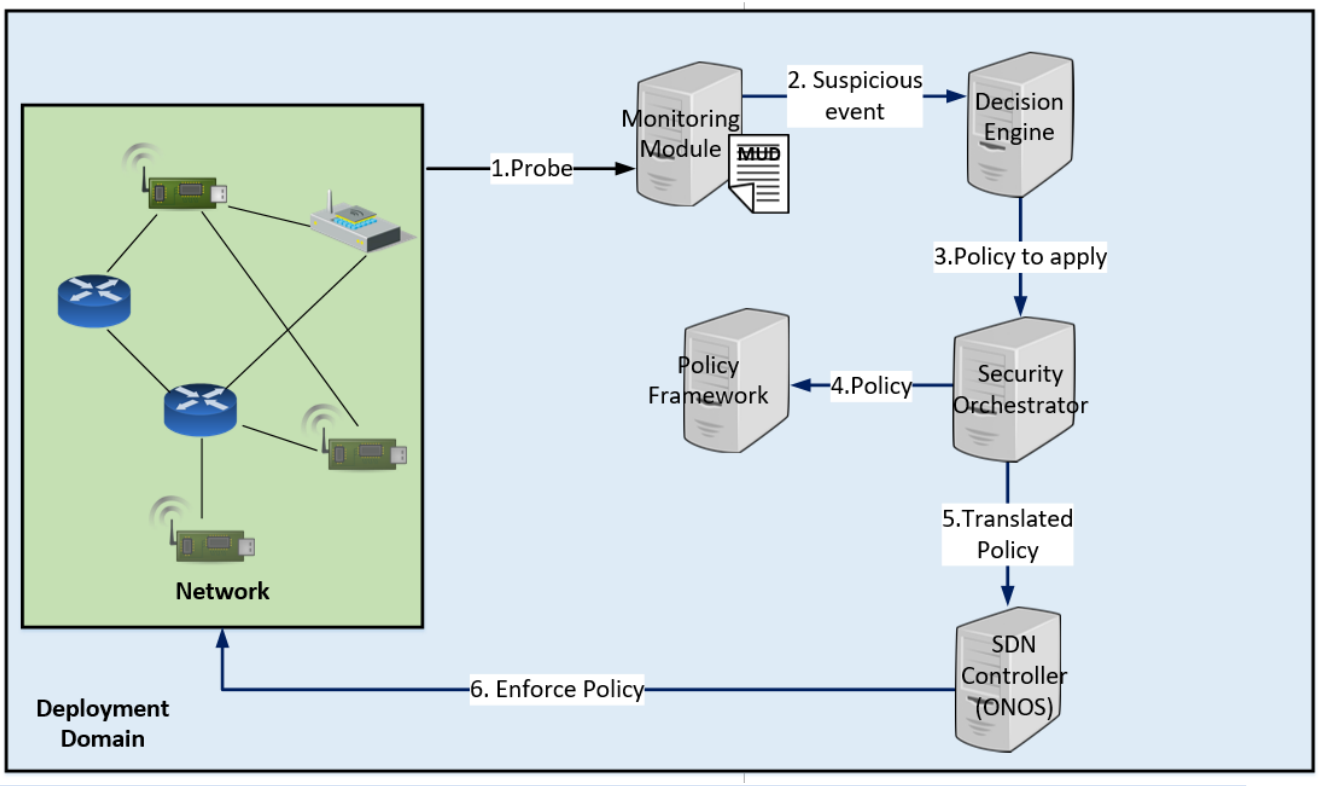
- **Manage 5G dependencies and send information about mitigations**
  - If a certain services is compromised, this information (dependencies) can be used to send an alert to those systems that depends on the compromised one and even to send them a possible mitigation (threat MUD).



Possible Usage

- **Monitoring compliance – Integration with MMT and UMU orchestrator**
  - Detect suspicious behaviours and return the system to a MUD-compliance status.

1. Monitor the system
2. Detect a misbehaviour (non compliance of the MUD policies)
3. Decide which policy apply to solve the misbehaviour and come back to a MUD compliant state.
4. Translate the policy
5. Select an enforcement
6. Enforce the policy



Thank you for your attention!

Find us at www.inspire-5gplus.eu

Twitter: @inspire_5gplus

Acknowledgment:

The research conducted by INSPIRE-5Gplus receives funding from the European Commission H2020 programme under Grant Agreement Nº 871808. The European Commission has no responsibility for the content of this presentation.