e-Lite

PitchD: May 24, 2023

Securing the Connected Home: Extending the MUD Architecture for Smart Home Gateways

Luca Mannella

Ph.D. student in Computer and Control Engineering

XXXVI cycle

e-Lite research group

Department of Control and Computer Engineering

Politecnico di Torino, Turin, Italy

Politecnico di Torino

Politecnico di Torino

e-Lite

Outline

- My research topic
- A bit of context about Internet of Things (IoT)
- The Manufacturer Usage Description (MUD) standard
- Beyond MUD (extending the MUD standard)
- Current and future work

Politecnico di Torino

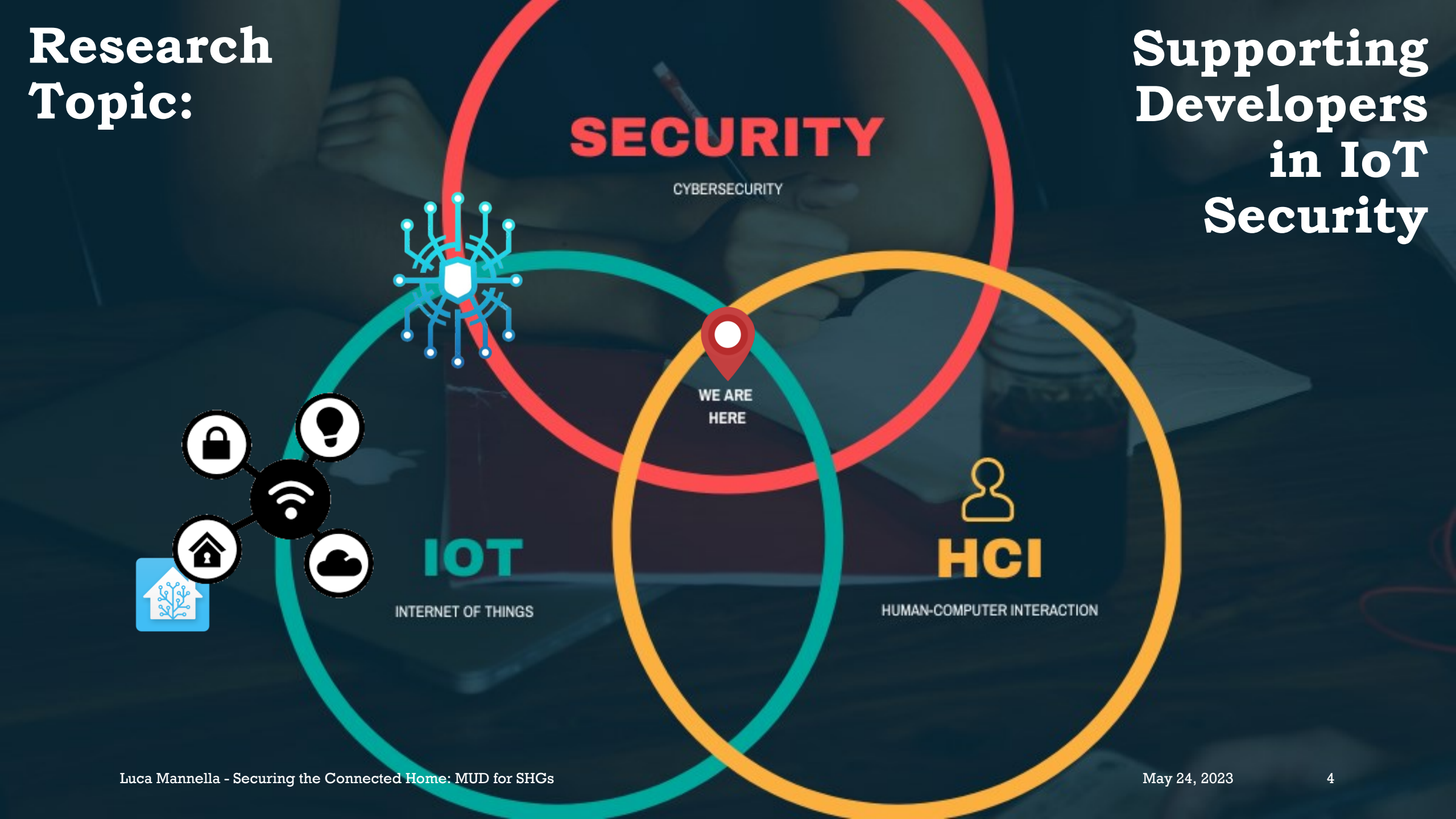
e-Lite

The Goal of my Ph.D.

- Simplify the development of more secure IoT systems
  - Understanding how security is perceived by IoT developers
    - and (try to) improve security awareness
  - Provide developers guidelines and best practices
  - Creating (or expanding) tools and supporting software for programming more secure and reliable IoT applications
- With a specific focus on novice developers
  - (or developers with limited experience in *IoT* or *security* fields)

Research Topic:

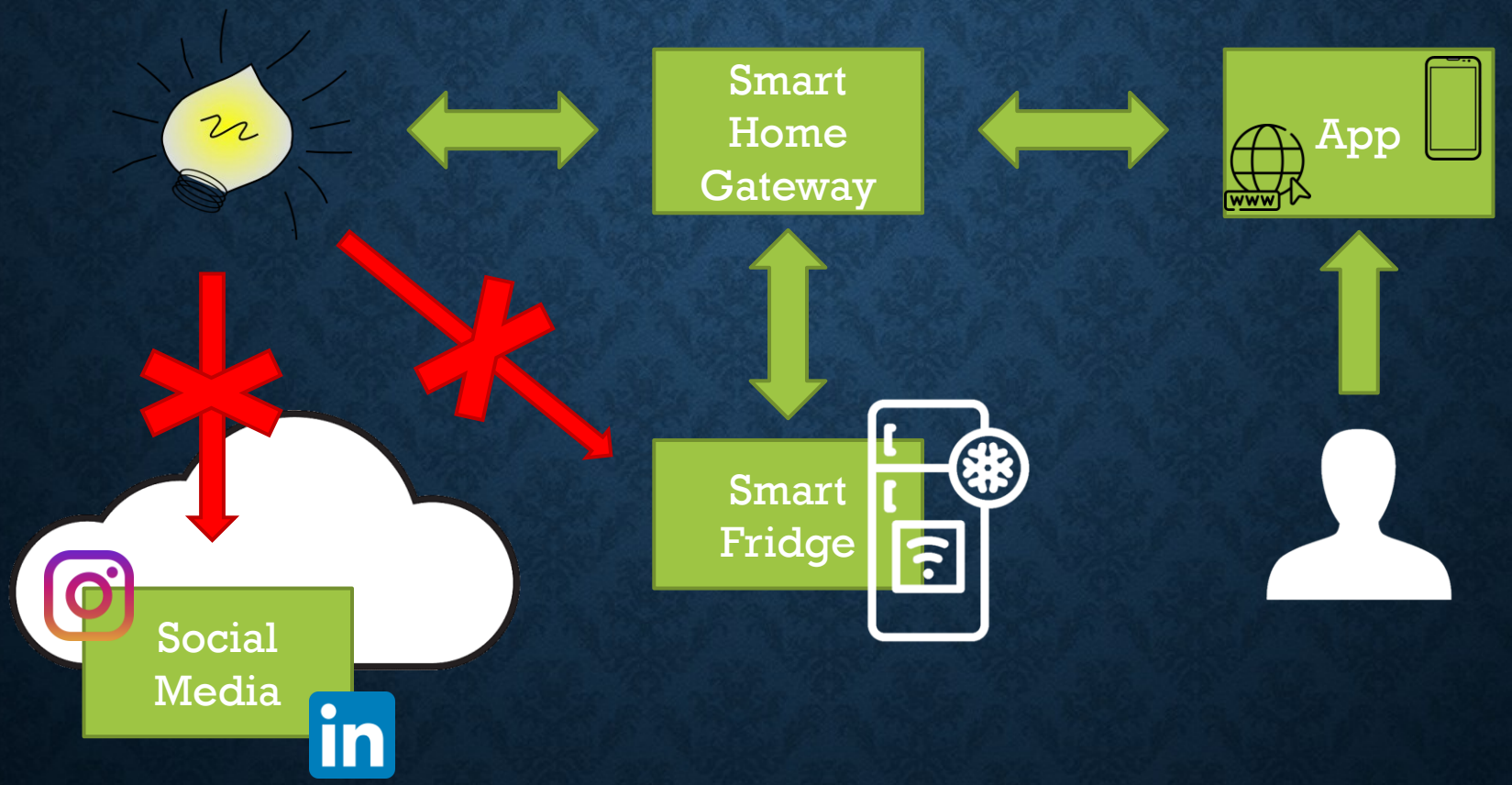
Supporting Developers in IoT Security



IoT Systems are still in a Critical Situation

- Very widespread (12.2 billion active endpoints)
- Sometimes they are not adequately protected
- Compromised devices could create serious issues
  - IoT devices are infected to carry on DDoS attacks (Mirai Botnet)
  - Affecting other devices in the same network
- Developing secure systems is challenging for programmers
  - Especially for Novice Programmers
  - Particularly in a **distributed** and **diversified** environment like IoT
  - Some vulnerabilities are caused by insecure (or misconfigured) applications

Example: a Light in a Smart Home



Manufacturer Usage Description (MUD)

Manufacturer Usage Description (MUD)

- IETF Standard: RFC-8520 (originally proposed by CISCO)
- **Main goal**: reducing unexpected communications to/from an IoT device
  - Defining a proper *architecture* and *data model*
- **How?** With a white-listing approach
  - The manufacturer specifies the authorized connections (policy) in a dedicated "MUD file"
  - Other connections are forbidden

Politecnico di Torino

e-Lite

Intents of MUD

- Reduce the device's **threat surface**
  - to those communications intended by the manufacturer
- To scale network policies
- To address at least some vulnerabilities
  - faster than the time it might take to update systems
- Adding a security mechanism keeping its cost to the bare minimum for the device
- To easily express device capabilities or requirements

Politecnico di Torino

e-Lite

MUD Files and MUD Policies Enforcement

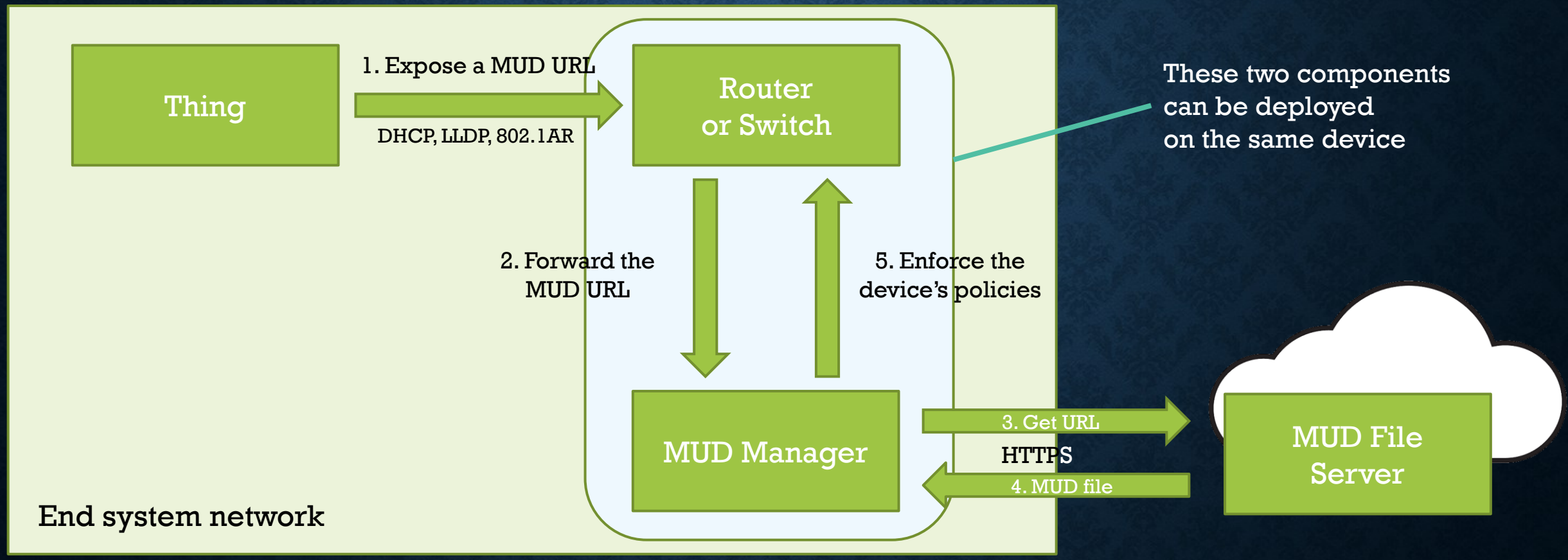
- Each class of device produced by a Manufacturer must have a dedicated MUD file
  - E.g., a MUD file for Amazon Echo Dot, a MUD file for the Philips Hue, etc…
- The MUD file is composed by a set of policy
  - Each policy defines the endpoints of the allowed communications
  - Policies are **JSON** objects defined using **YANG** standard
    - a data modeling language used to model configuration data, state data, Remote Procedure Calls, and notifications for network management protocols
- These policies are enforced by the network where the device is deployed
  - A "MUD Manager" must be in the local network
  - The enforcement is partially left to the local network administration

A MUD File example

```
1  "ietf-mud:mud":{
2    "mud-version":1,
3    "mud-url":"https://lighting.example.com/light
4    "last-update":"2022-07-22T11:20:51+02:00",
5    "cache-validity":48,
6    "is-supported":true,
7    "systeminfo":"An Example Light Bulb",
8    "from-device-policy":{
9      "access-lists":{
10       "access-list":[ {"name":"mud-76100-v6fr"}
11     }
12   },
13   "to-device-policy":{
14     "access-lists":{
15       "access-list":[ {"name":"mud-76100-v6to"}
16     }
17   }
18 },
```

```
{
  "name":"mud-76100-v6fr",
  "type":"ipv6-acl-type",
  "aces":{
    "ace":[
      {
        "name":"cl0-frdev",
        "matches":{
          "ipv6":{
            "ietf-acldns:dst-dnsname":"test.example.com",
            "protocol":6
          },
          "tcp":{
            "ietf-mud:direction-initiated":"from-device",
            "destination-port":{
              "operator":"eq",
              "port":443
            }
          }
        },
        "actions":{
          "forwarding":"accept"
        }
      }
    ]
  }
}
```

How MUD Works



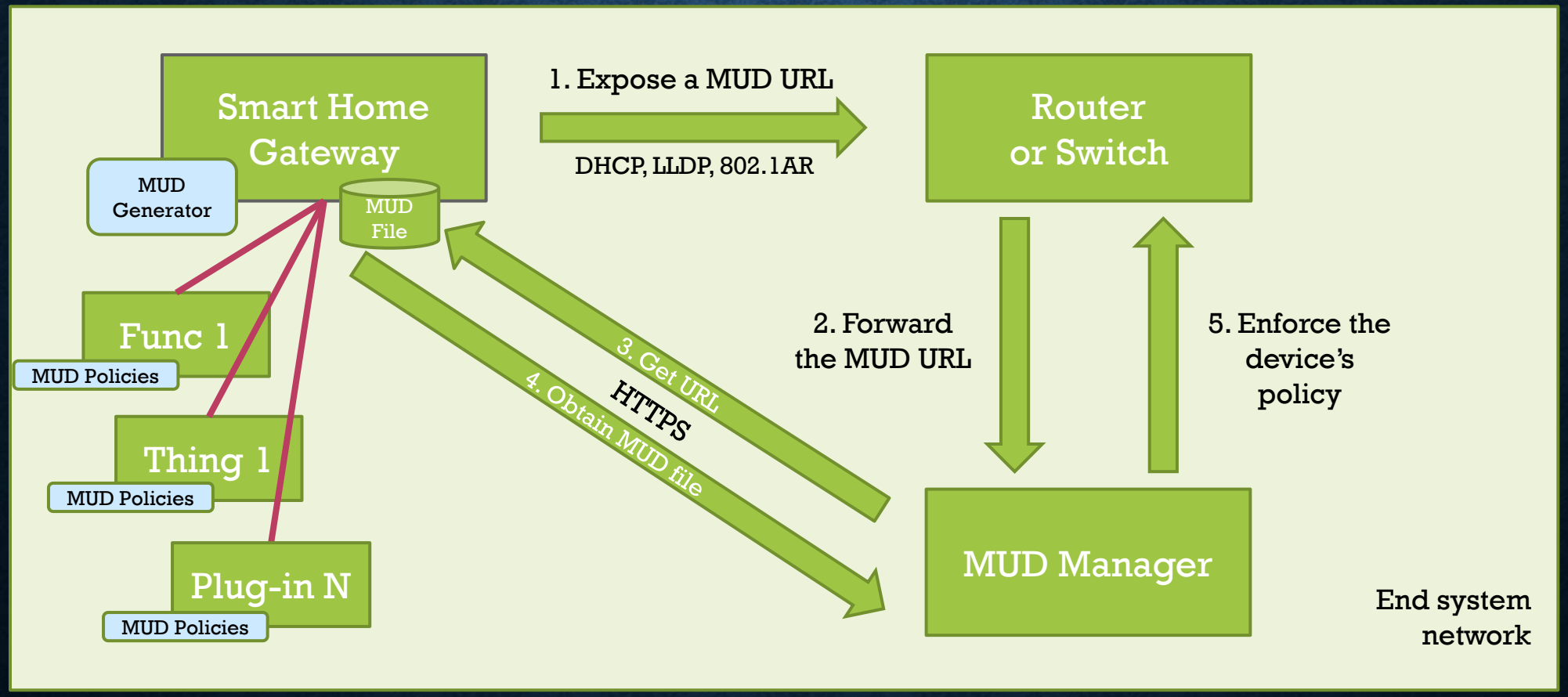
Extending MUD Architecture

Extending MUD Architecture

- Promising, but MUD is not yet very deployed
  - Manufacturers are not creating (and deploying) MUD files
- A possible solution *(already faced in literature)* can be
  - a third party could create the MUD file **instead** of the manufacturer
- Proposed approach
  - A suitable third-party could be a smart home gateway
    - Device able to coordinate many IoT devices
    - Often extensible through plug-ins
  - Developers and tinkerers could help in creating these MUD files
    - even if they have limited experience with the technology (and no dedicated server)
    - Specifying plug-ins' endpoints

Link to the Paper

Extended MUD Architecture



Politecnico di Torino

e-Lite

Main Contributions

- Extend the MUD concept in a transparent way
  - A SHG can manage many devices in its smart home
  - The devices and the MUD manager are not aware of this change
- Protect devices not natively MUD-enabled
  - Thanks to developers' contributions
- Protect SHGs and their plug-ins with the MUD standard
  - Protecting every kind of plug-in (regardless of the functionality offered)
- Testing this proposed approach
  - Through a dedicated plug-in for Home Assistant

Link to the Paper

Current and Next Steps

- MUD snippets' authentication
  - only **trusted** developers must be able to add their MUD snippets
  - MUD snippets must be associated to the proper plug-in
- Refine MUD policies enforcement at plug-in level
- MUD policies issue
  - Policy Errors: detecting if a policy is wrong-written
  - Policy Conflicts: detecting if two policies contradict each other
  - Policy Sub-Optimizations: detecting if policies are overlapping

Other Research Activities

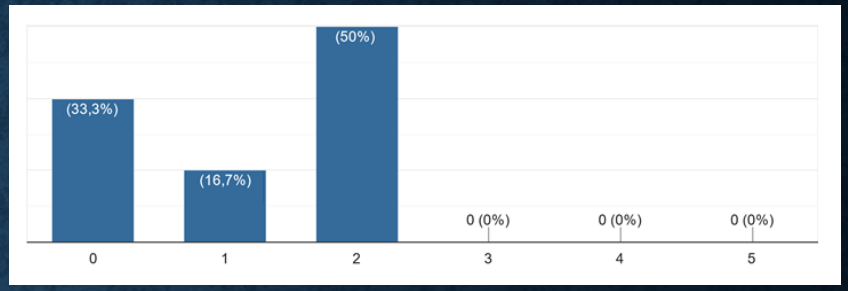
Help Devs to Create More Secure Cloud-IoT Applications

- Analyze the security perception of Novice Cloud-IoT Programmers
  - (developers new to cloud development and IoT domain)
  - Through a survey
  - Starting from a concrete use case: *the assignment of a professional course*
- Analyze the security features of IoT-related components
  - offered by major Cloud-IoT platforms (AWS and Azure)

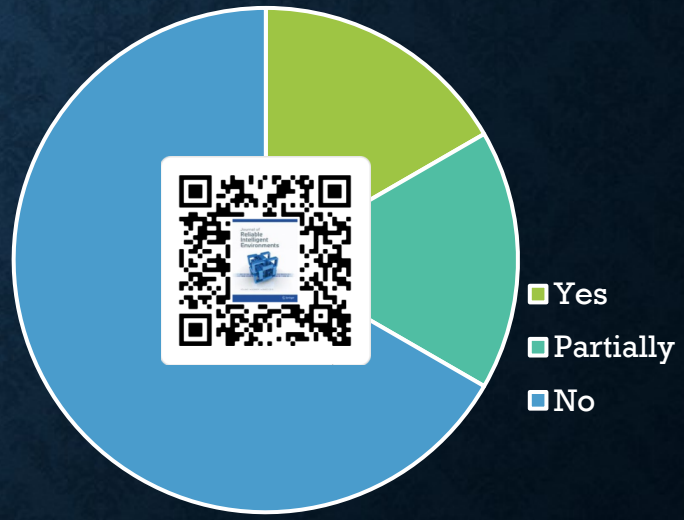
Link to the Paper

A bit of Research Results

- Developers do not think too much about security
  - At least when they are novice to Cloud-IoT domain
- Cloud platforms (like AWS and Azure) are quite able to compensate the developers' shortcomings
  - But sometimes they must be correctly configured
- Proposed a set of 14 guidelines that developer can follow to produce more secure cloud-IoT solution since the very beginning



How many points did you considered as "*potentially attackable*" during the development?

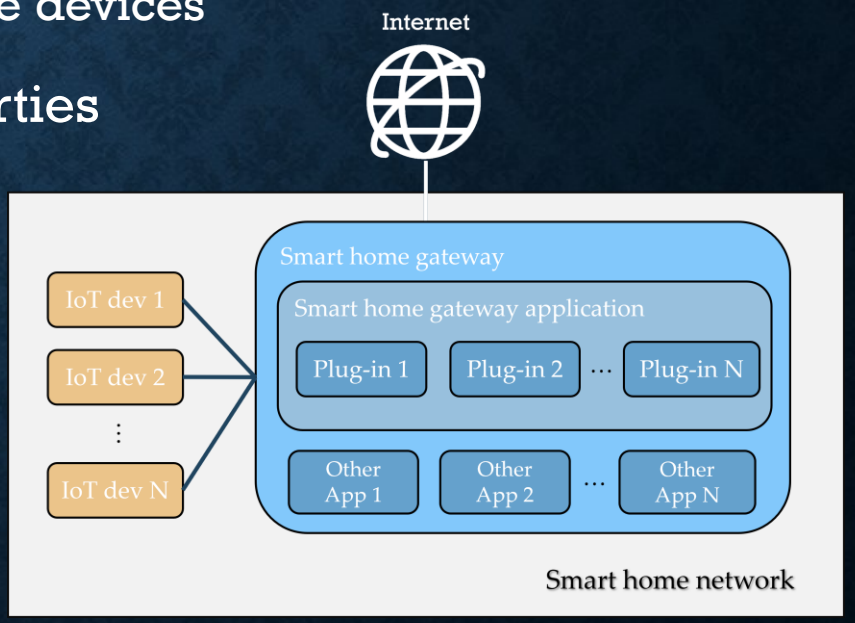


Did you verify if connections to and from AWS are encrypted?

A Threat Model for Extensible Smart Home Gateway

Link to the Paper

- To manage smart homes, smart home gateways (SHG) are often involved
  - Such solutions are often extensible (Home Assistant, OpenHAB, WebThings, etc.)
    - Extending something developed by a third-party is never an easy task
  - A compromised IoT gateway can affect several smart home devices
- 11 threats divided according to the main security properties
  - That could be created by a malicious or defective plug-in
- Work in progress on this topic
  - Further validating the model on more extensible SHGs
  - Demonstrating that developers could even erroneously develop malicious behaviors



Thanks For Your Kind Attention!

Any questions?

Luca Mannella
Ph.D. student
e-Lite research group
Department of Control and Computer Engineering
Politecnico di Torino, Italy

luca.mannella@polito.it

Stay Connected

Publications

References

1. K. Lasse Lueth, et al., "State of IoT—spring 2022," IoT Analytics, Tech. Rep., May 2022. [Online]. Available: https://iot-analytics.com/product/state-of-iot-spring-2022/
2. C. Kolias, et al., "*DDoS in the IoT: Mirai and other botnets*," Computer, vol. 50, no. 7, pp. 80–84, 2017.
3. K. Kafle, et al., "*Security in Centralized Data Store-based Home Automation Platforms: A Systematic Analysis of Nest and Hue*," ACM Trans. on Cyber-Phys. Syst., vol. 5, no. 1, Jan 2021.
4. D. Kumar, et al., "*All Things Considered: An Analysis of IoT Devices on Home Networks*," in 28th USENIX Security Symposium (USENIX Security 19), pp. 1169–1185, 2019.
5. J. L. Hernández-Ramos et al., "*Defining the Behavior of IoT Devices Through the MUD Standard: Review, Challenges, and Research Directions*," in IEEE Access, vol. 9, pp. 126265-126285, 2021.
6. Home Assistant Website, https://www.home-assistant.io/
7. F. Corno, and L. Mannella, "*A Gateway-based MUD Architecture to Enhance Smart Home Security.*" – *To be published*.
8. F. Corno, et al., "*Helping novice developers harness security issues in cloud-IoT systems*," J. Reliab. Intell. Environ. **2022**, 8, 261–283.
9. F. Corno, and L. Mannella, "*A Threat Model for Extensible Smart Home Gateways*," in 2022 7th International Conference on Smart and Sustainable Technologies (SpliTech). IEEE, July 2022, pp. 1–6.