Politecnico di Torino
Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering
XXXVI cycle

Fondazione CRT

Supervisors
Prof. Fulvio Corno
Prof. Antonio Lioy

Supporting Developers in the Cybersecurity of IoT Systems

PhD Candidate: *Luca MANNELLA*
Email: luca.mannella@polito.it

1. Context

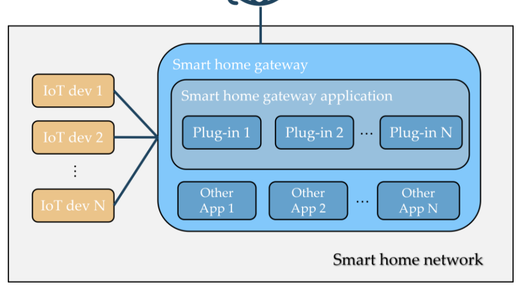
Internet of Things (IoT) systems are very widespread but often not properly protected. If compromised, they can create serious issues and even cyber-physical attacks.

2. Goal

To simplify the development of secure and reliable IoT solutions. Primarily, the focus is on smart homes and developers with limited experience in *cybersecurity* of *IoT* systems.

3. A threat model for extensible Smart Home Gateways

Smart home devices are often affected by vulnerabilities. If IoT objects are managed by a Smart Home Gateway (SHG), there is a potential single point of failure.



Moreover, the risk of a bugged gateway raises if it can be extended by third-parties plug-ins. Hence, we proposed a threat model [2] to help developers during creation (or security analysis) of plug-ins.

Table 1 Proposed threat model.

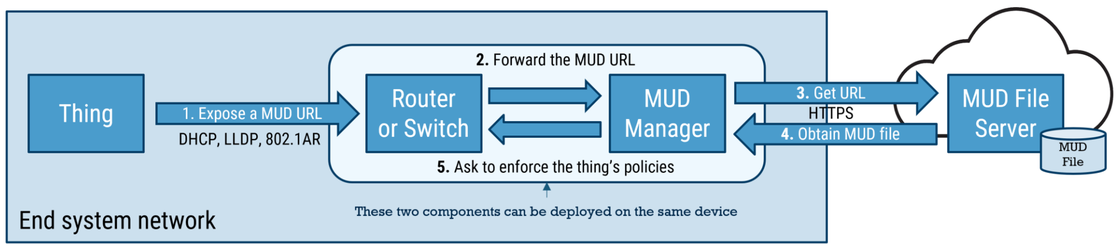
Category	ID	Description
Confidentiality	T1	a plug-in could *access and use* private data of other attack targets (i.e., data outside its scope)
	T2	a plug-in could *access and spread* private data of other attack targets (i.e., data outside its scope)
Integrity	T3	a plug-in could *alter the state* of smart home *devices* outside its scope
	T4	a plug-in could *alter private data* of other *attack targets* outside its scope
Availability	T5	a plug-in could *delay* the regular functionality of an attack target
	T6	a plug-in could *alter* one of the regular functionalities of an attack target
	T7	a plug-in could *alter* the regular functionality of an attack target, preventing the smart home users from using it
	T8	a plug-in could physically *damage* an attack target
Authentication	T9	a plug-in could interact with an attack target, pretending to be a different entity
Authorization	T10	a plug-in could access an authorization level higher than expected
Non-Repudiation	T11	a plug-in could anonymously communicate with an attack target

To demonstrate the feasibility of the threats, we developed a set of proofs of concept [2] for a widespread open-source SHG.

Currently, we are working on demonstrating how programmers can inadvertently introduce these threats into their plug-ins. The study involves two different SHG: Home Assistant and WebThings.

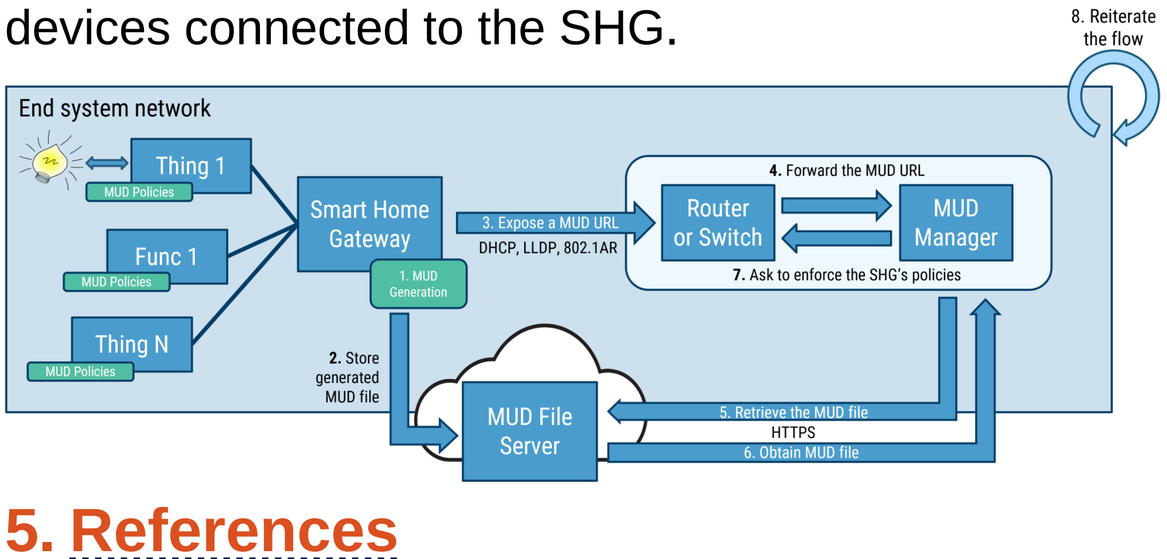
4. Introducing MUD in Smart Home Gateways

Manufacturer Usage Description (MUD) standard (RFC-8520) defines an architecture and a data model to restrict communications to and from IoT devices. To make IoT devices compatible with MUD, manufactures have to write devices' network policies in a dedicated file (the MUD file) stored on their server(s).



Our proposal [3] allows plug-ins developers to leverage MUD for their plug-ins. Specifying plug-ins' network requirements in a MUD-compliant way, developers can indirectly protect non-MUD-enabled IoT devices and every software plug-in.

At run-time these requirements are collected and merged by a dedicated SHG's components in a gateway-level MUD file. This file is retrieved and processed, like in a traditional MUD architecture, in a transparent way for the MUD manager and the devices connected to the SHG.



5. References

1. Corno, F.; De Russis, L.; Mannella, L. "Helping Novice Developers Harness Security Issues in Cloud-IoT Systems", 2022. Journal of Reliable Intelligent Environments 8 (Springer); Issue 3/2022; pp. 261-283; https://doi.org/10.1007/s40860-022-00175-4
2. Corno, F.; Mannella, L. "A Threat Model for Extensible Smart Home Gateways", 2022. SpliTech 2022: 7th International Conference on Smart and Sustainable Technologies (IEEE); Split / Bol, Croatia; July 5-8, 2022; https://doi.org/10.23919/SpliTech55088.2022.9854235
3. Corno, F.; Mannella, L. "A Gateway-based MUD Architecture to Enhance Smart Home Security", 2023. SpliTech 2023: 8th International Conference on Smart and Sustainable Technologies (IEEE); Split / Bol, Croatia; June 20-23, 2023; https://doi.org/10.23919/SpliTech58164.2023.10193747