University
of Molise

Security Analysis of Access Control Policies for Smart Homes

Roberta Cimorelli Belfiore, Anna Lisa Ferrara
University of Molise,
Italy

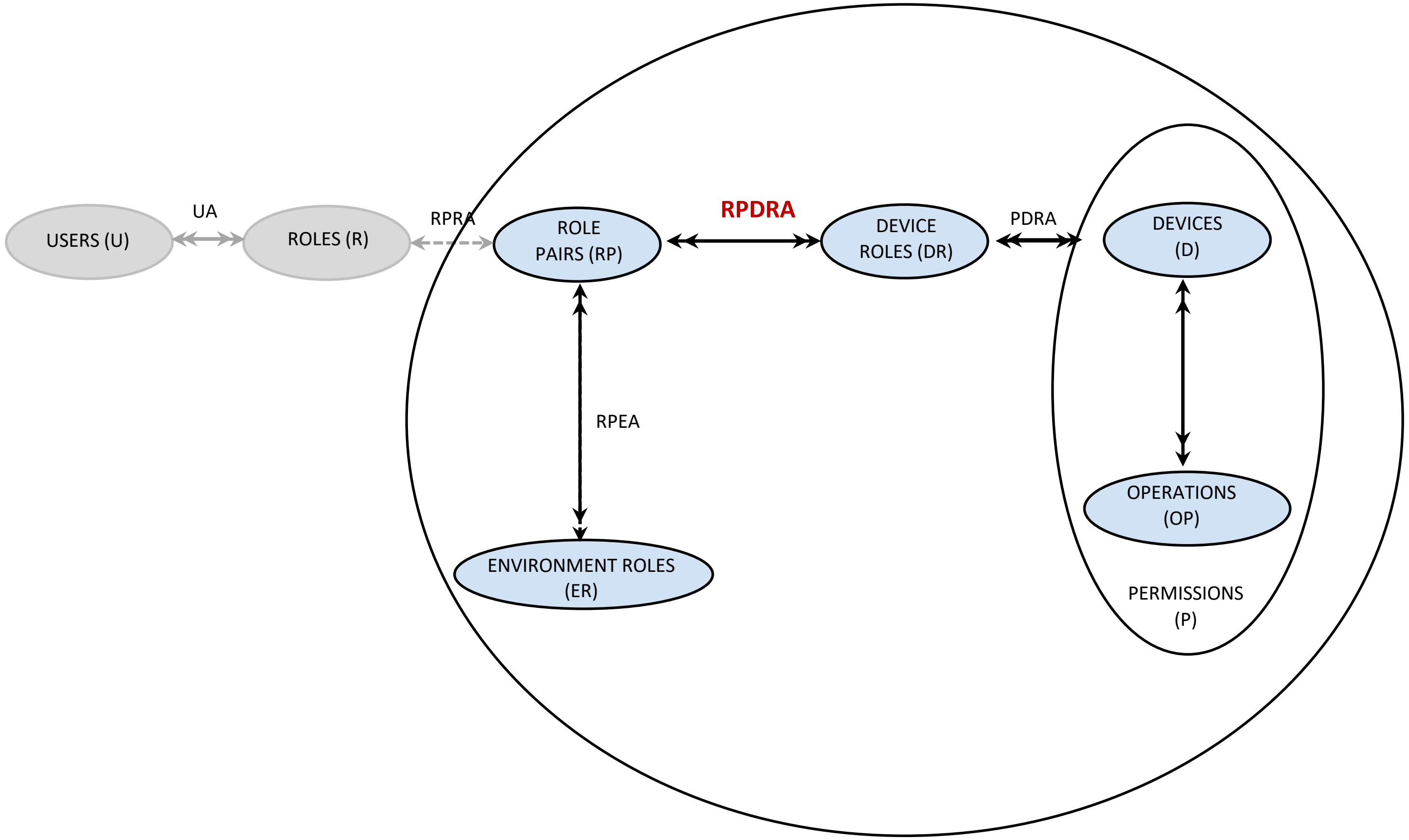
SACMAT2023

Introduction

Smart houses are becoming increasingly common due to the IoT, but protecting privacy and resources is a concern.

To address this issue, sophisticated access control specifications and enforcement models are needed.

State of the art: EGRBAC



Examples:

Role Pairs RP

$Parent(Any\_Time)$
$Maid(At\_Home)$
$Kid(Entertainment\_Time)$

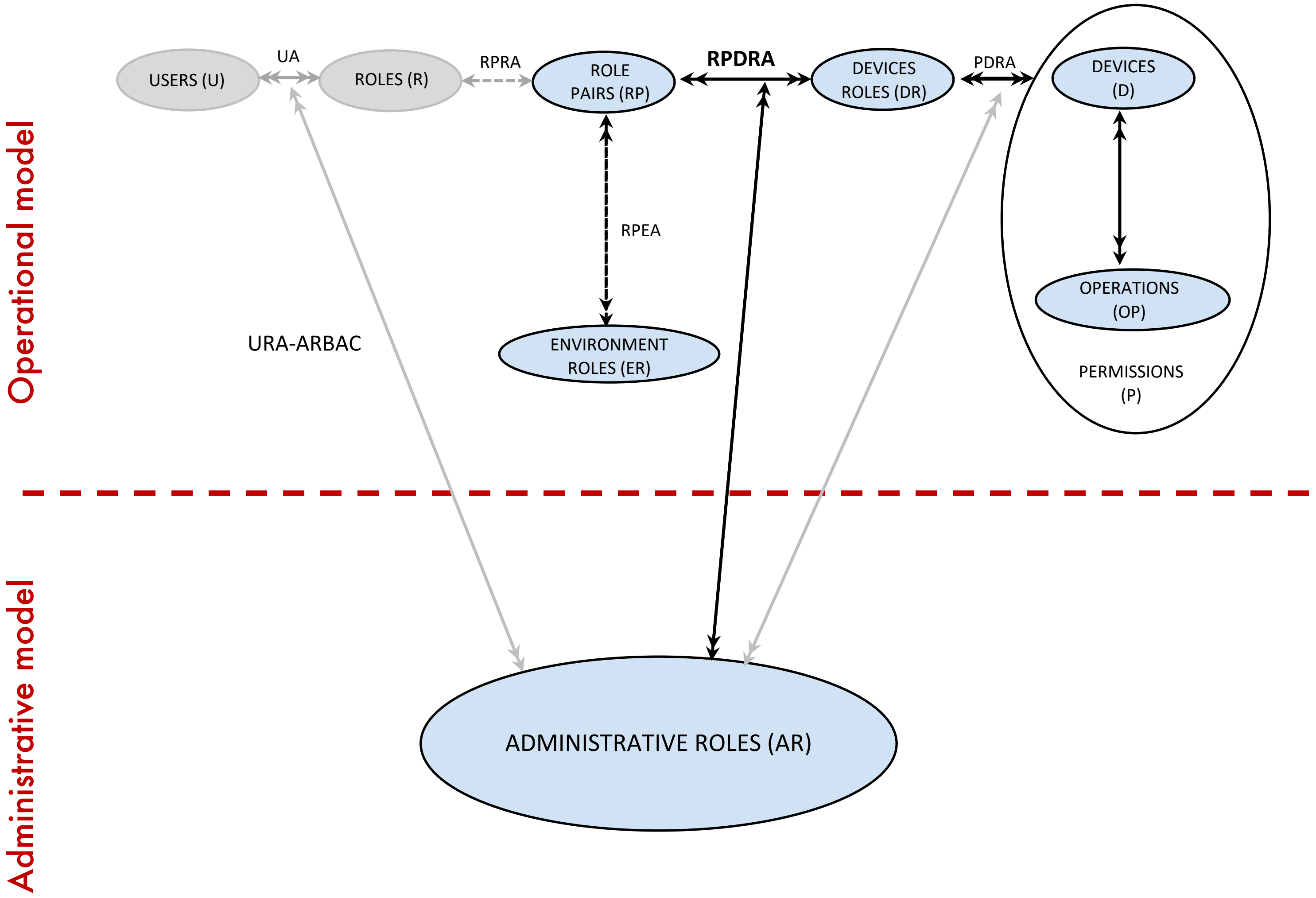
Device Roles DR

$Dangerous\_Devices$
$Cleaning\_Devices$
$Entertainment\_Devices$

RPDRA
Maid(At_Home),Cleaning_Devices

S. Ameer, J. Benson and R. Sandhu, "The EGRBAC Model for Smart Home IoT," 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), 2020, pp. 457-462.

State of the art: Administrative EGRBAC



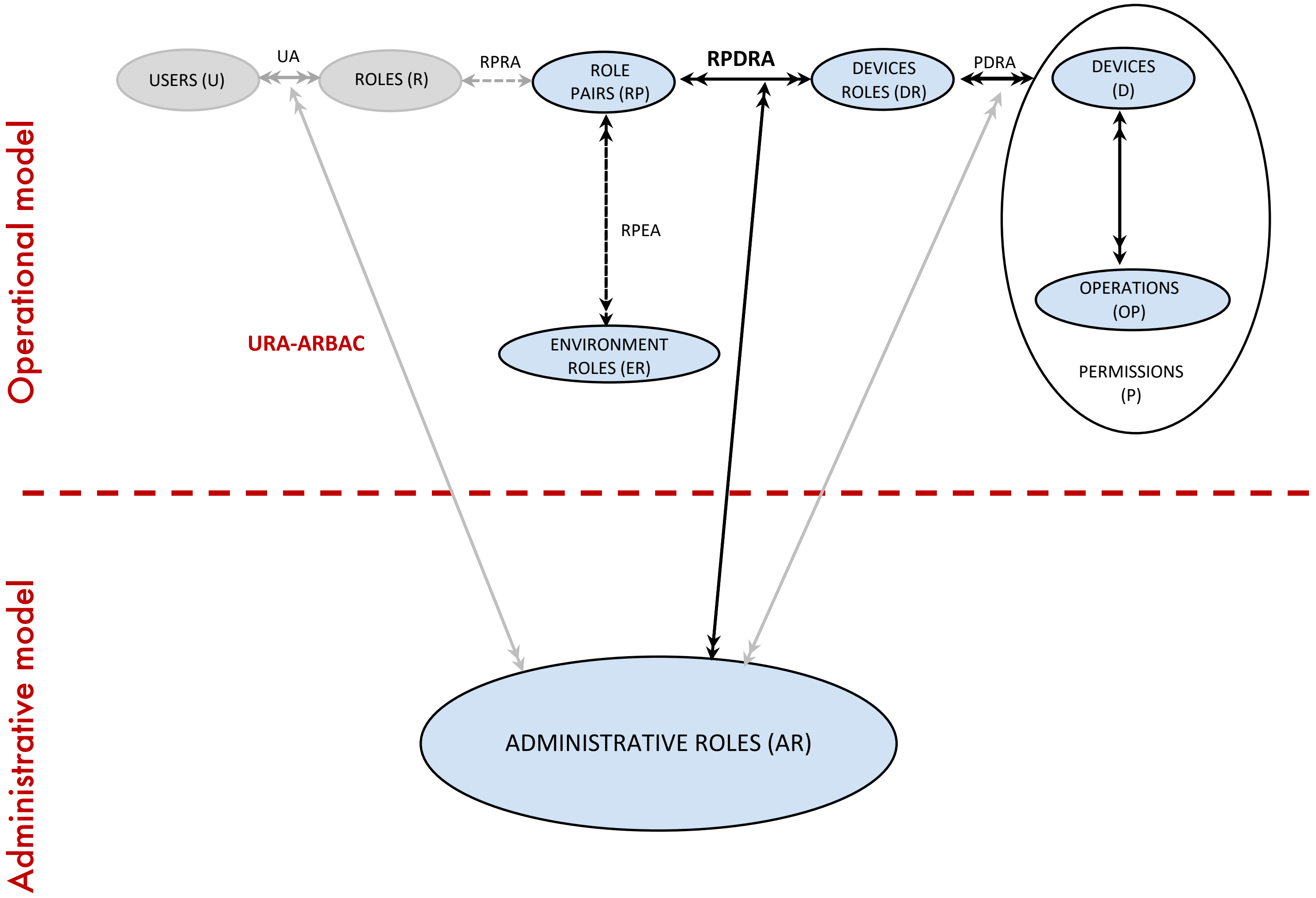
Authorization Functions:

AssignRPDR

RevokeRPDR

Shakarami Mehrnoosh, and Ravi Sandhu. "Role-based administration of role-based smart home IoT." Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. 2021.

State of the art: Administrative EGRBAC



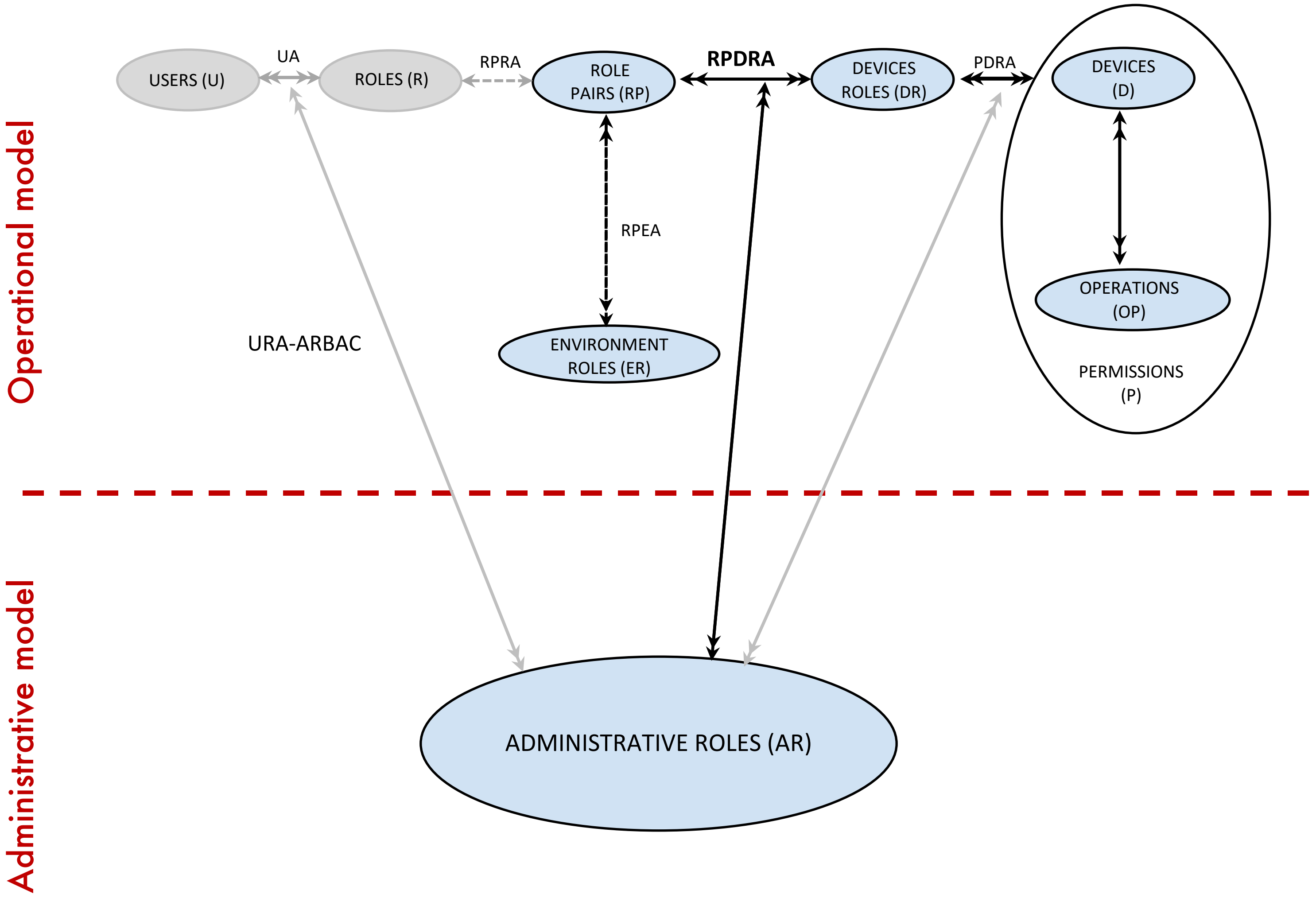
Authorization Functions:

AssignRPDR

RevokeRPDR

Shakarami Mehrnoosh, and Ravi Sandhu. "Role-based administration of role-based smart home IoT." Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. 2021.

State of the art: Administrative EGRBAC



Authorization Functions:

AssignRPDR

RevokeRPDR

Shakarami Mehrnoosh, and Ravi Sandhu. "Role-based administration of role-based smart home IoT." Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. 2021.

Importance of Automated Security Analysis

Mistakes are common and may result in security breaches.

- Verification is essential
- Policies are difficult to inspect by hand

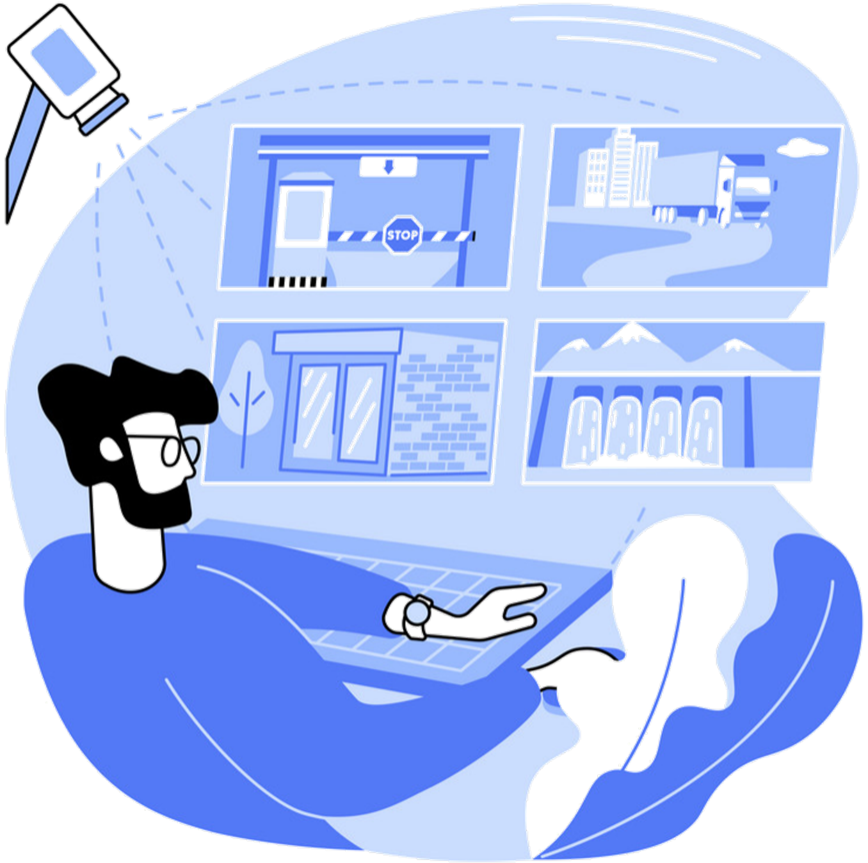
An important aspect of security analysis is undoubtedly the ability to automate it.

ASASP

{P} mohawk

✓AC

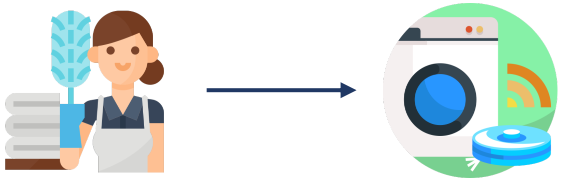
Goal



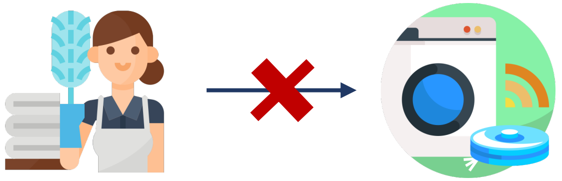
- Automated security analysis in Administrative EGRBAC
- Realistic case study

Authorization functions

AssignRPDR(AUser, AR, RP, DR)

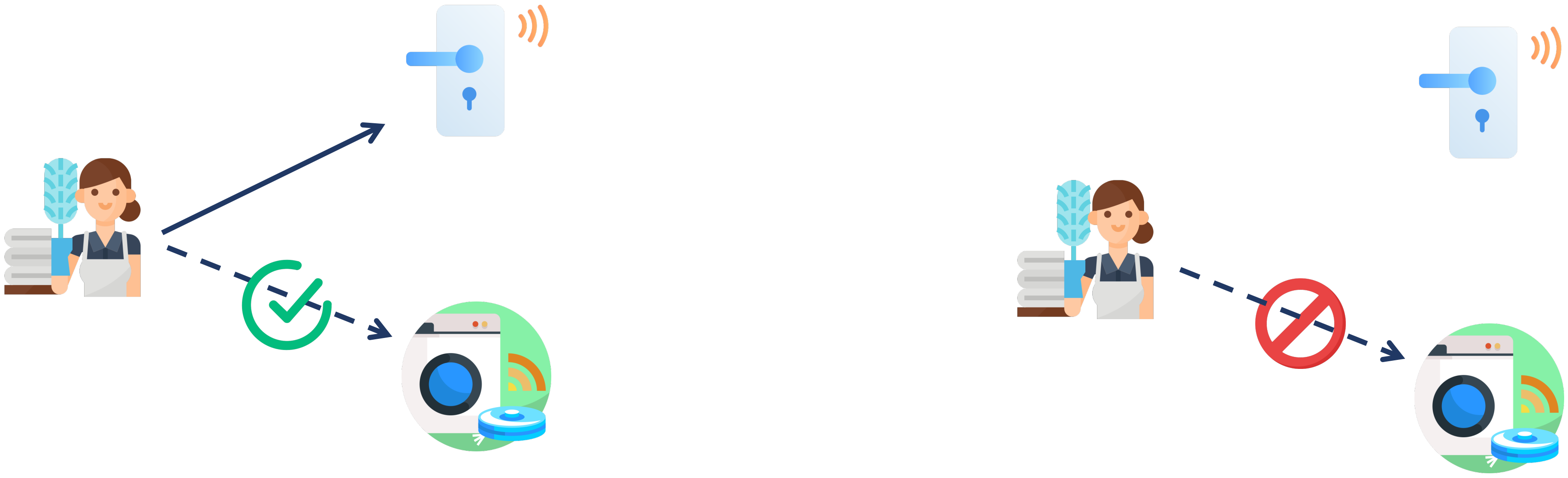


RevokeRPDR(AUser, AR, RP, DR)



Conditioned Assignment function

Sometimes homeowners need to establish policies that enable the assignment of role pairs to device roles based on their association with other device roles



Conditioned Assignment function

We include preconditions for assignment actions, following ARBAC97's paradigm

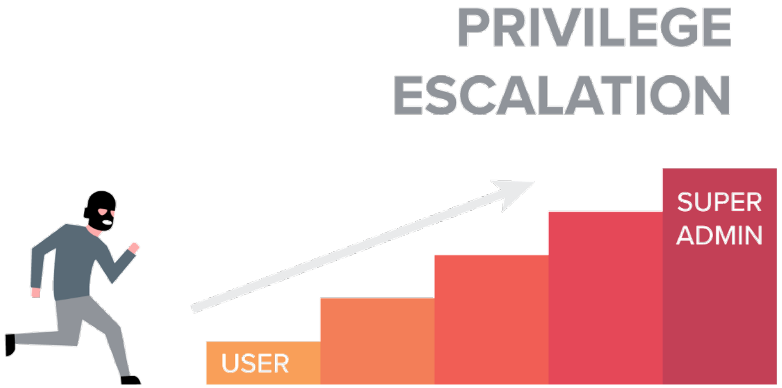
AssignRPDR(AUser, AR, RP, *precondition*, DR)

AssignRPDR(Roberta, Home_Owner, maid_AtHome, *Door_Device*, Cleaning_Devices)

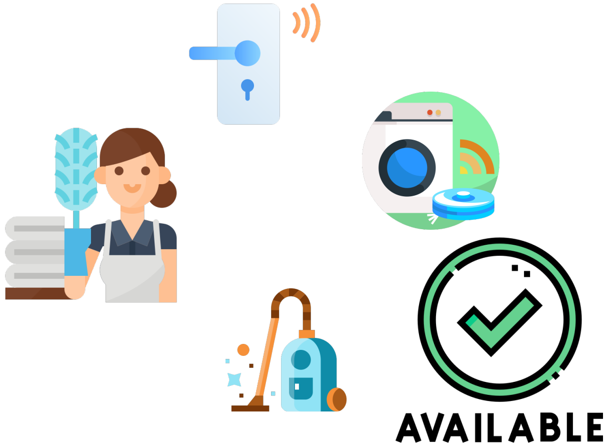
Security Requirements

Homeowners design administrative policies to achieve specific security goals:

- Privilege escalation: ensuring that no role pair has unauthorized access to devices



- Availability: ensuring that a role pair has the necessary devices



DR - reachability problem

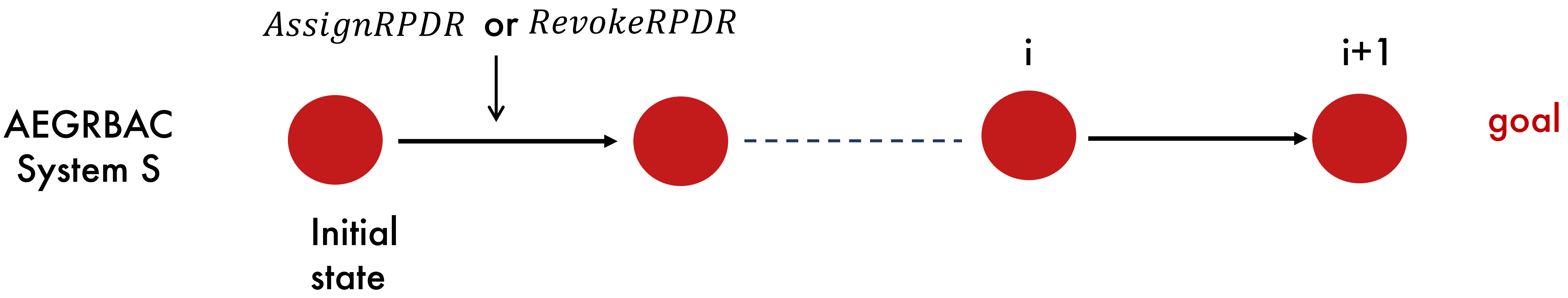
- availability
- escalation of privileges
- ...

↓ each reduces to

DR-reachability Problem

Can any role pair gain access to a given device-role goal using the AEGRBAC rules?

DR - reachability problem



Our approach

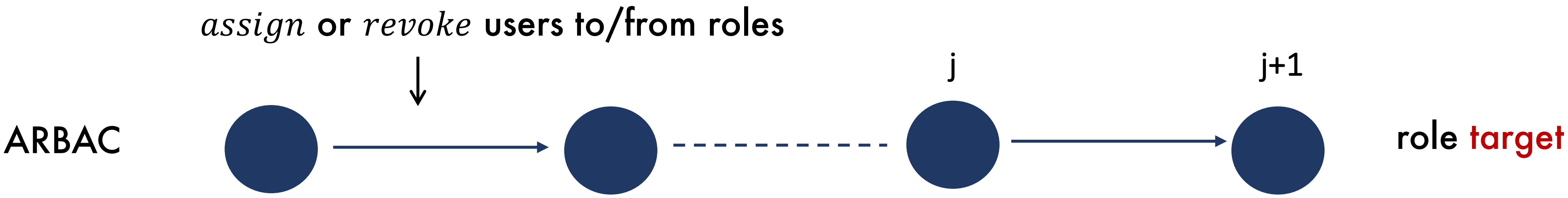
Step 1:
Reduction to role reachability problem in ARBAC

Step 2:
Automatic analysis using existing tools

Our approach

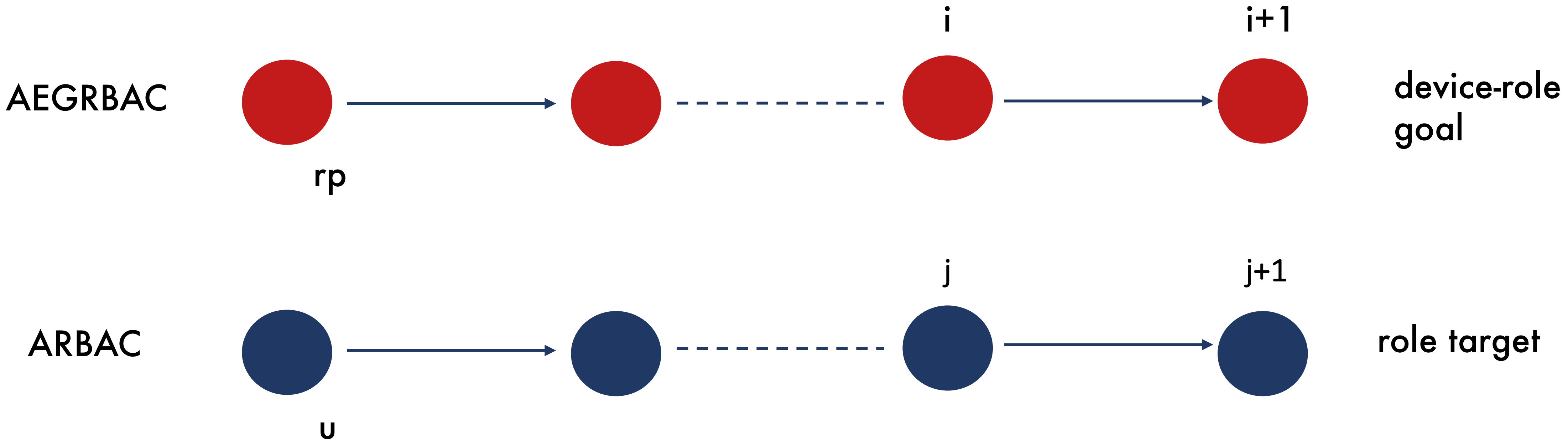
Step 1:

We reduce the DR-reachability problem to the role-reachability problem in URA-ARBAC



Theorem

There is a run in AEGRBAC iff there is a run in ARBAC



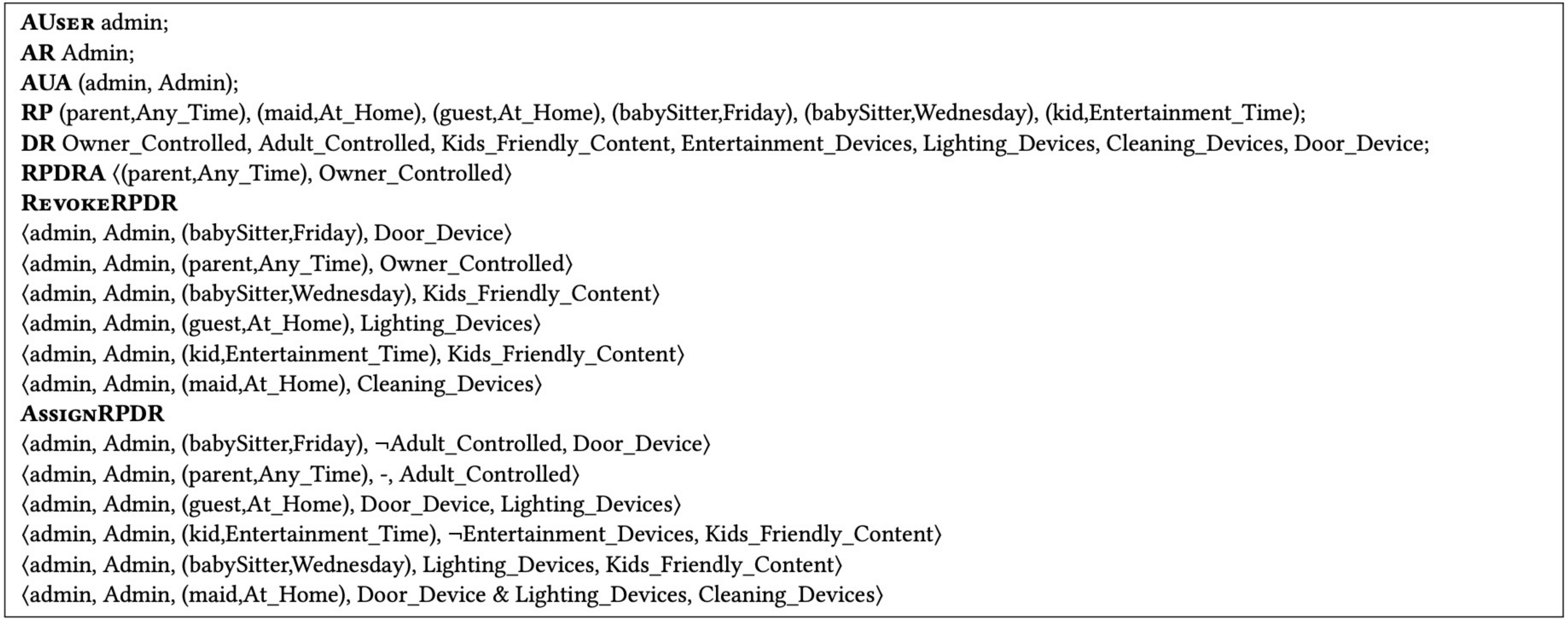
Our approach

Step 2:
Automatic Analysis

We continue the analysis leveraging existing tools in ARBAC

✓ERIFIER OF ACCESS CONTROL

Experiments

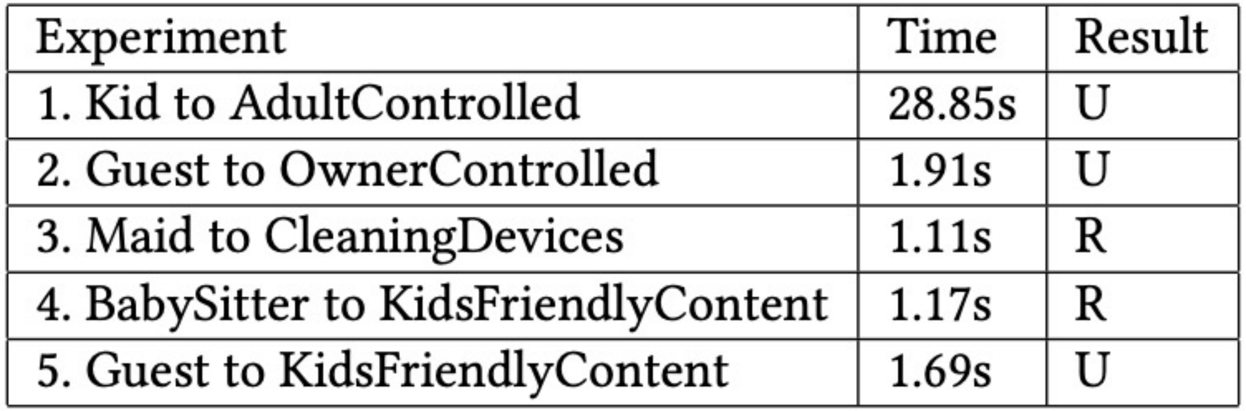


AUser admin;
AR Admin;
AUA (admin, Admin);
RP (parent,Any_Time), (maid,At_Home), (guest,At_Home), (babySitter,Friday), (babySitter,Wednesday), (kid,Entertainment_Time);
DR Owner_Controlled, Adult_Controlled, Kids_Friendly_Content, Entertainment_Devices, Lighting_Devices, Cleaning_Devices, Door_Device;
RPDRA ⟨(parent,Any_Time), Owner_Controlled⟩
RevokeRPDR
⟨admin, Admin, (babySitter,Friday), Door_Device⟩
⟨admin, Admin, (parent,Any_Time), Owner_Controlled⟩
⟨admin, Admin, (babySitter,Wednesday), Kids_Friendly_Content⟩
⟨admin, Admin, (guest,At_Home), Lighting_Devices⟩
⟨admin, Admin, (kid,Entertainment_Time), Kids_Friendly_Content⟩
⟨admin, Admin, (maid,At_Home), Cleaning_Devices⟩
AssignRPDR
⟨admin, Admin, (babySitter,Friday), ¬Adult_Controlled, Door_Device⟩
⟨admin, Admin, (parent,Any_Time), -, Adult_Controlled⟩
⟨admin, Admin, (guest,At_Home), Door_Device, Lighting_Devices⟩
⟨admin, Admin, (kid,Entertainment_Time), ¬Entertainment_Devices, Kids_Friendly_Content⟩
⟨admin, Admin, (babySitter,Wednesday), Lighting_Devices, Kids_Friendly_Content⟩
⟨admin, Admin, (maid,At_Home), Door_Device & Lighting_Devices, Cleaning_Devices⟩

Our full policy has 12 users, 11 roles, 15 role pairs RP, 19 device roles DR and 236 authorization functions

Experiments

We tested the policy against 21 queries using the tool VAC, the analysis terminated in a few seconds, regardless of whether the target pair was reachable or not



Experiment	Time	Result
1. Kid to AdultControlled	28.85s	U
2. Guest to OwnerControlled	1.91s	U
3. Maid to CleaningDevices	1.11s	R
4. BabySitter to KidsFriendlyContent	1.17s	R
5. Guest to KidsFriendlyContent	1.69s	U

Table 1: Experimental results

Future developments

Consider case studies in large-scale scenarios:
e.g., *smart building*

Consider different underlying tools for the analysis and compare their output/performance

Thanks for your attention

Roberta Cimorelli Belfiore
r.cimorellibelfio@studenti.unimol.it

Anna Lisa Ferrara
annalisa.ferrara@unimol.it

acm SIGSAC

SACMAT2023