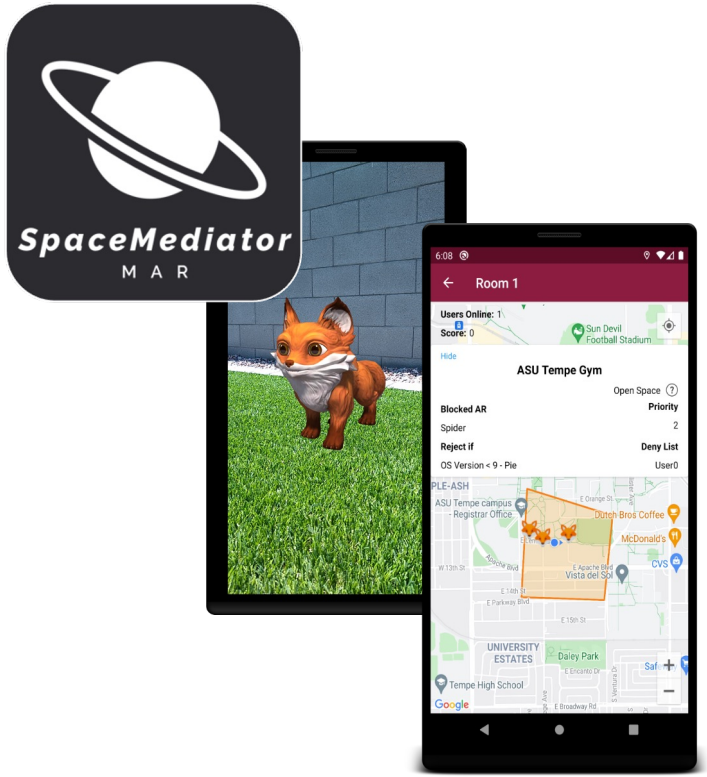
SpaceMediator:
Leveraging Authorization Policies to Prevent Spatial and Privacy Attacks in Mobile Augmented Reality



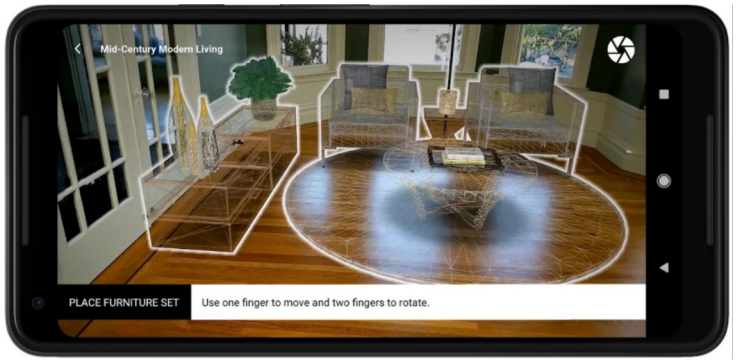
Luis M. Claramunt [ASU], **Carlos Rubio-Medrano** [TAMUCC], Jaejong Baek [ASU], Gail-Joon Ahn [ASU]

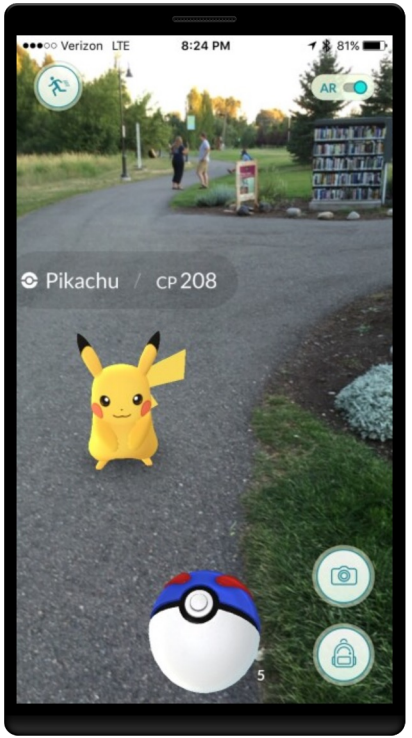
Arizona State University, Texas A&M University – Corpus Christi

The 28th ACM Symposium on Access Control Models and Technologies, Trento, Italy, June 2023

Motivation

- *Mobile Augmented Reality* (MAR) is trending:
  - Shopping – (e.g., eBay, Wayfair),
  - Entertainment – (e.g., Snapchat, MARK),
  - Productivity – (e.g., GeoGebra, Measure),
  - Games – (e.g., Pokémon GO, Jurassic World Live).





The Problem

Recorded Incidents

- *MAR-Apps* have been used in places it was considered disrespectful,[1]
- Many users having access to the same content has led to crowds,[2]
- Criminals have used content to target their victims for robberies,[3]
- According to police: [4]
    - Breaking into private property,
    - Injuries for being distracted,
    - Car accidents.

[1] M. Chan. (2016) Pokémon go players anger 9/11 memorial visitors: 'it's a hallowed place'. [Online]. Available: https://time.com/4403516/pokemon-go-911-memorial-holocaust-museum/
[2] (2016) Pokemon go away: Troublesome sydney pokestop shut down. [Online]. Available: https://www.bbc.com/news/technology-36948331
[3] T. Mullen. (2016) Hundreds of pokémon go incidents logged by police. [Online]. Available: https://www.bbc.com/news/uk-england-37183161
[4] L. Gornstein. (2016). Terrible things happening to pokémon go players. [Online]. Available: https://www.cbsnews.com/pictures/terrible-things-happening-to-pokemon-go-players/6/

The Problem with MAR

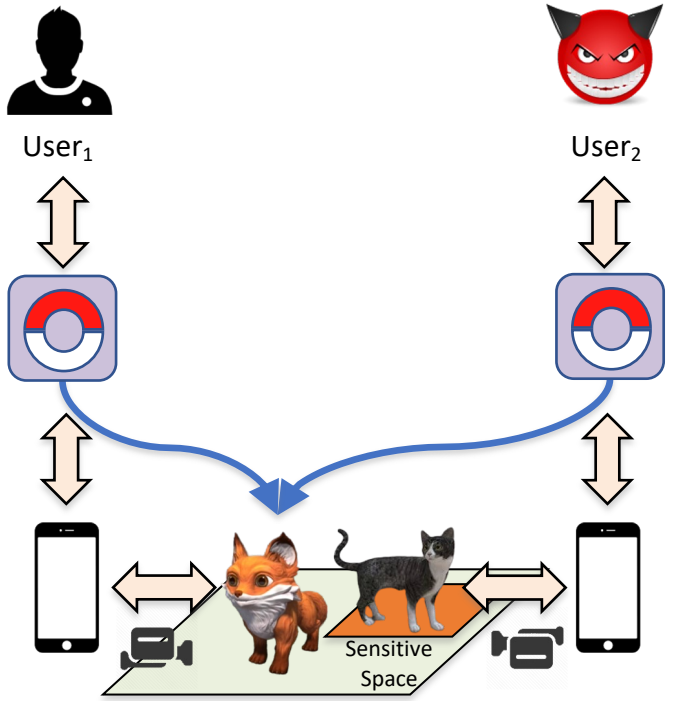
- Despite benefits and popularity, some security issues exist:
  - Privacy Leak:
    - Users' data *unwillingly* shared with other users or third-parties,
    - Largely explored in the literature (tons of papers),
  - Space Affectation:
    - MAR content placed in physical spaces *degrades* user experience,
    - Users meeting with malicious third parties via MAR content,
    - Recently recognized as a problem by the cybersecurity community[5],
  - Space Invasion:
    - *Intrusive* MAR content in *sensitive* spaces (hospitals, memorials, etc.),
    - Adds a new spatial dimension to issues already in literature[6],

[5] K. Lebeck, K. Ruth, T. Kohno and F. Roesner, "Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users," *2018 IEEE Sym. on Security and Privacy (S&P)*, 2018.

[6] C. E. Rubio-Medrano, S. Jogani, M.Leitner, Z. Zhao, and G-J. Ahn. 2019. "Effectively Enforcing Authorization Constraints for Emerging Space-Sensitive Technologies", *ACM Sym. on Access Control Models and Technologies* (SACMAT '19), 2019.

Case Study on MAR-Apps

- 15 MAR-Apps available in Google Play,
- Used two devices representing a benign and malicious user,
- Space Invasion:
  - MAR in sensitive space,
- Space Affectation:
  - Interaction between User1 and User2,
  - Degrading MAR content,
- Privacy Leak:
  - Sensitive information made public.



Space with same MAR Objects

Results of Case Study

It is common for MAR-Apps to:

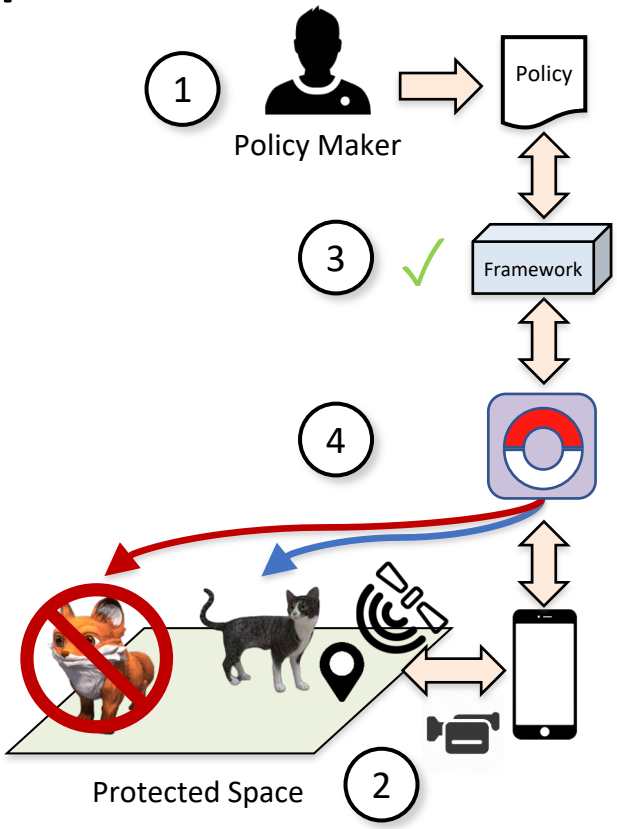
- Lack regulation over where the MAR content can be placed,
- Give access to the same MAR objects to all users,
- Mishandle gathered information.

Application	Space Invasion	Space Affectation	Privacy Leak	Downloads
Pokémon GO	✓	✓	-	100M
Jurassic World	✓	✓	-	10M
Walking Dead	✓	✓	-	5M
Color Quest	✓	-	-	1M
Snaappy	✓	✓	✓	1M
AR Real Drive	✓	-	-	500K
Just a Line	✓	-	-	500K
Weapon AR	✓	✓	-	100K
vTime XR	✓	✓	✓	100K
WallaMe	✓	✓	✓	100K
RealTag	✓	✓	-	100K
Real Note	✓	✓	✓	50K
My World	✓	✓	✓	10K
Tendar	✓	-	-	5K
MARK	✓	✓	-	1K

Our Solution

Policy-Governed MAR-Apps

1. A policy to protect a space or regulate user interaction is created,
2. App-User activates MAR-App and relevant data to evaluate the policy, i.e., location, is obtained,
3. The MAR-App requests the framework for authorization before providing content,
4. Once a response is received, the MAR-App renders only authorized functionality

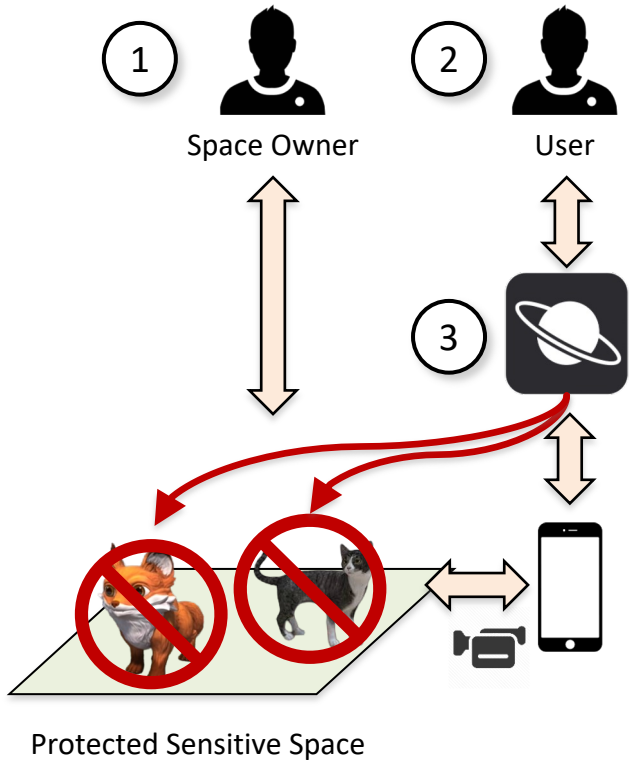


Space Owners Regulate Sensitive Space

1. A *Space Owner* wants to restrict MAR-App functionality in a *protected sensitive space*,

2. A User approaches the protected space using a MAR-App,

3. The functionality provided by the MAR-App must follow the directions specified by the Space Owner,

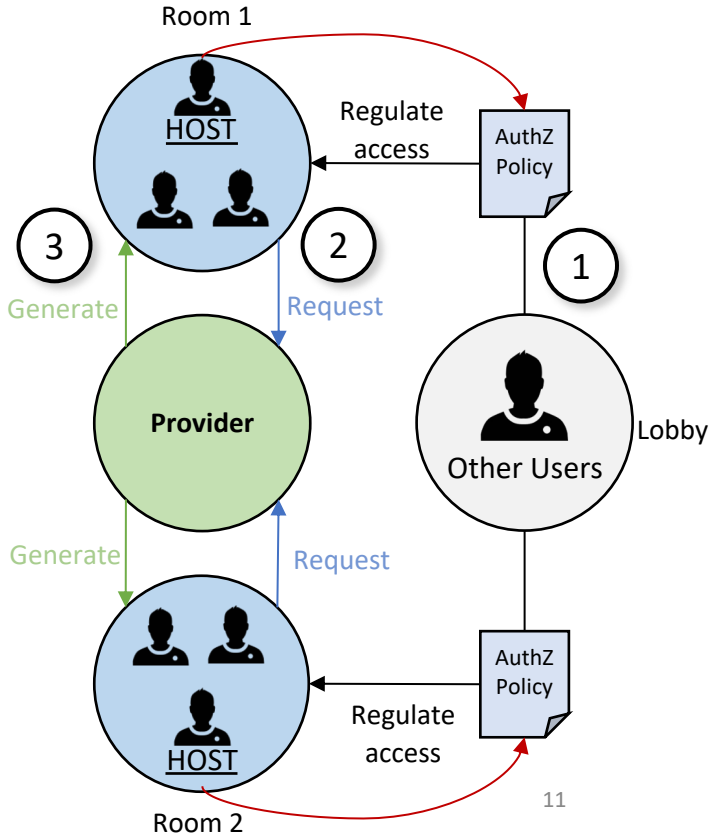


App-Users Regulate User Interaction

1. MAR content is available through rooms that restrict user interaction,
   - *Room*: Isolated and regulated MAR environment other users can join,

2. Users within the same rooms can request for new MAR content,

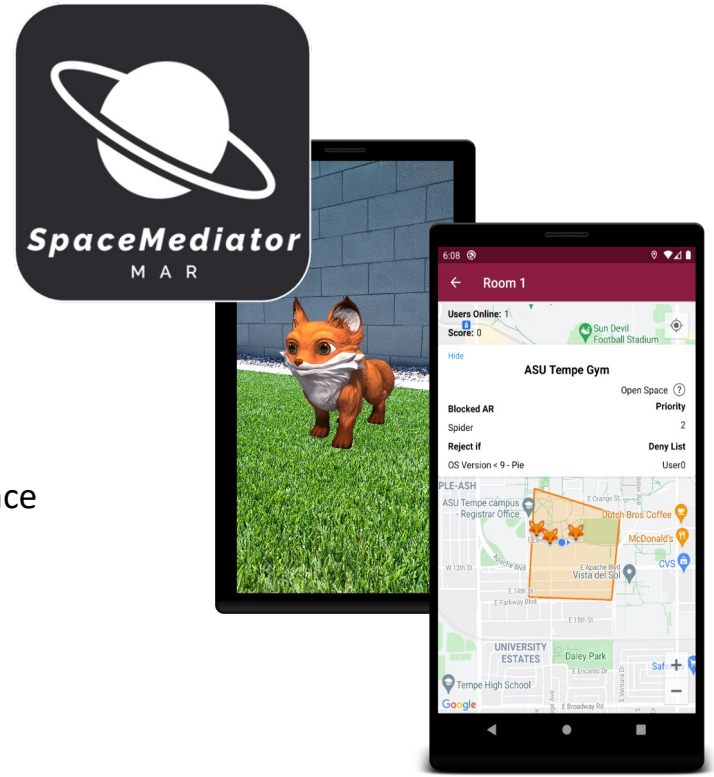
3. Different MAR objects, with distinct locations, will be generated and distributed among rooms,



SpaceMediator

Proof-of-Concept Policy-Governed MAR-App,

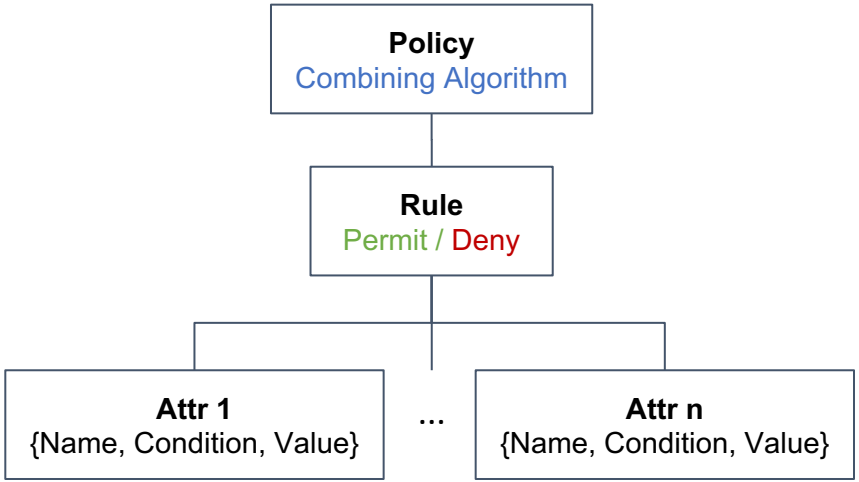
- Imitates Pokémon GO,
- Restricts:
  - Sensitive Space restricts MAR content, by Space Owner,
  - User Interaction, by App-Users
  - Restricts Private Information, by App-Users



Authorization Policies

- Policies are written using attributes from:
  - Users, e.g., username, date of birth,
  - Phones, e.g., OS Version, Manufacturer,
  - Protected Spaces, e.g., home or a park,
  - Others, e.g., Time, MAR content,
- Along with a type (*Open* or *Close)*,
  - Open: By default, grants access,
    - Specify who to reject,
  - Close: By default, denies access,
    - Specify who to accept,
- Implemented as a subset of XACML.

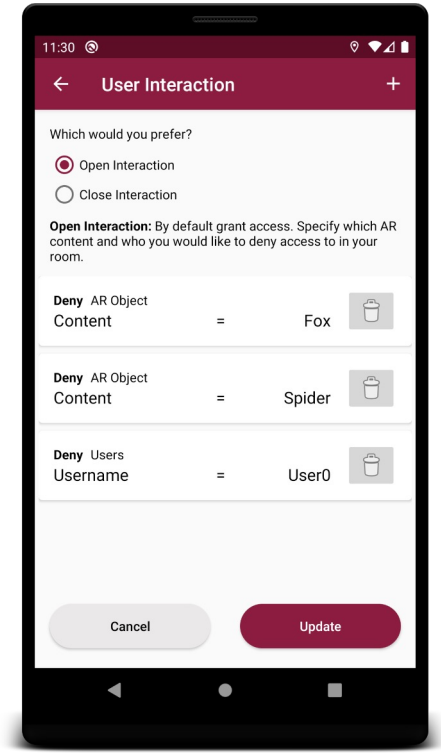
Policy Type	Combining Algorithm	Rules
Open	Permit-Unless-Deny	Deny
Close	Deny-Unless-Permit	Permit



Open Policy

By default, grants access, except to:

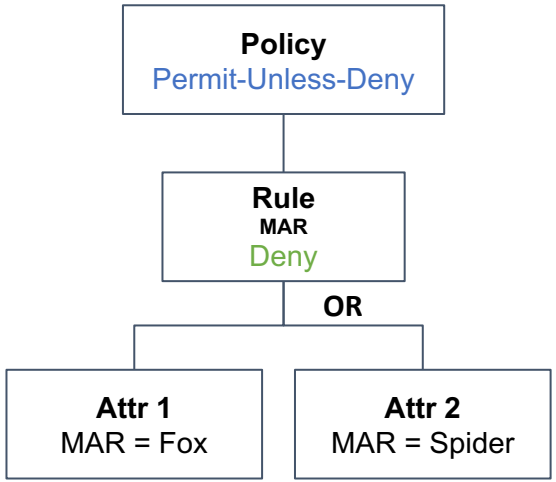
- Defined AR Objects,
- Specified usernames,
- Those who have **any** of the specified attributes



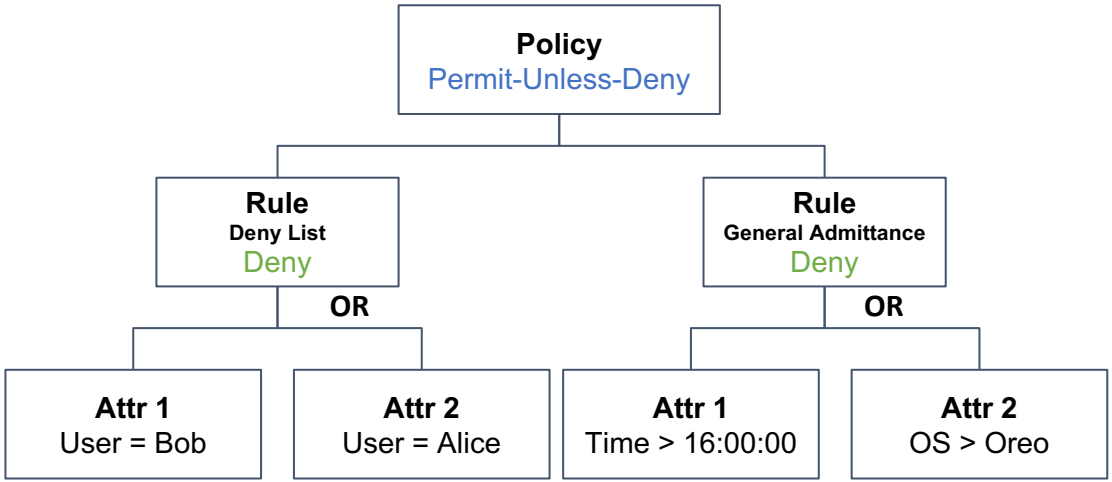
Open Policy

Open Policy

Regulates MAR Distribution



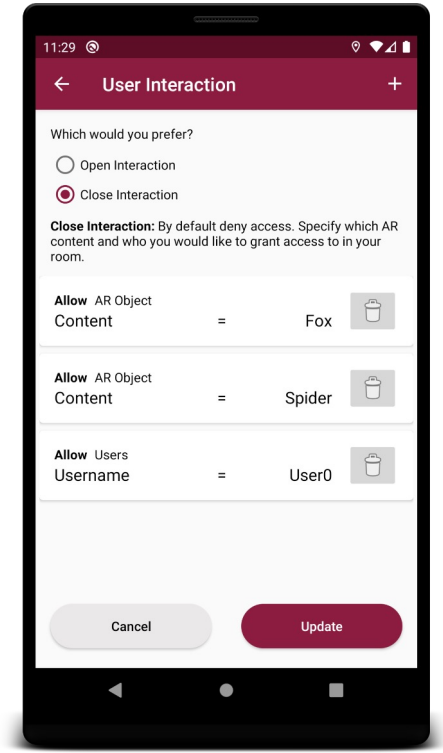
Regulates MAR Interaction



Close Policy

By default, denies access, except to:

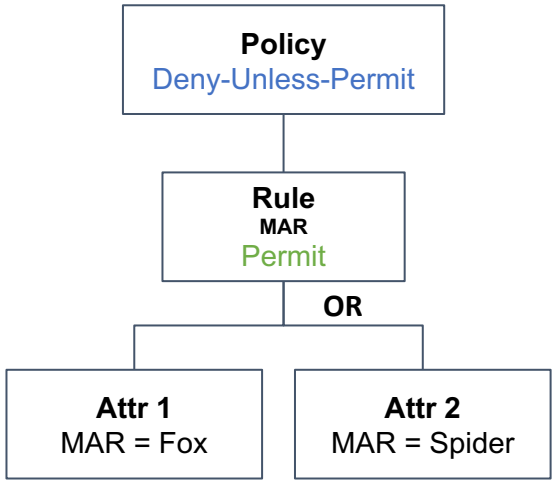
- Defined AR Objects,
- Specified usernames,
- Those who have **all** of the specified attributes



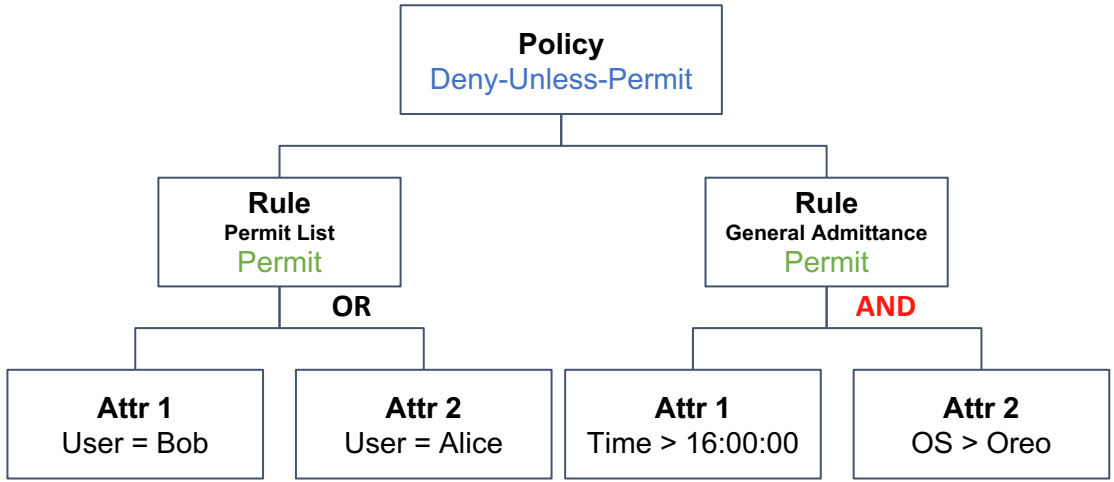
Close Policy

Close Policies

Regulates MAR Distribution



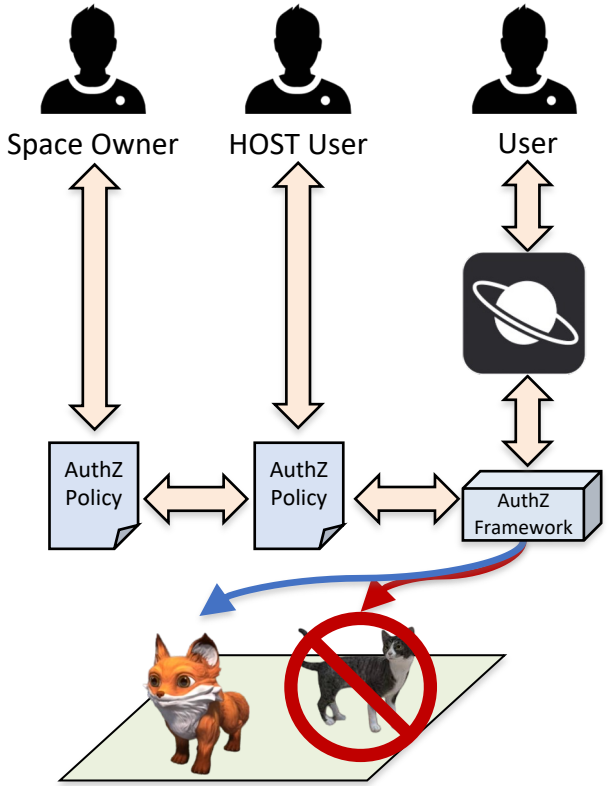
Regulates MAR Interaction



Evaluation

Policy Understanding/Writing

- Space Owners and App-Users need to write policies,
  - Restricting content and accessibility by name, time, age, etc.,
- App-Users need to understand policies,
  - Why is my MAR-App not working when visiting a hospital?



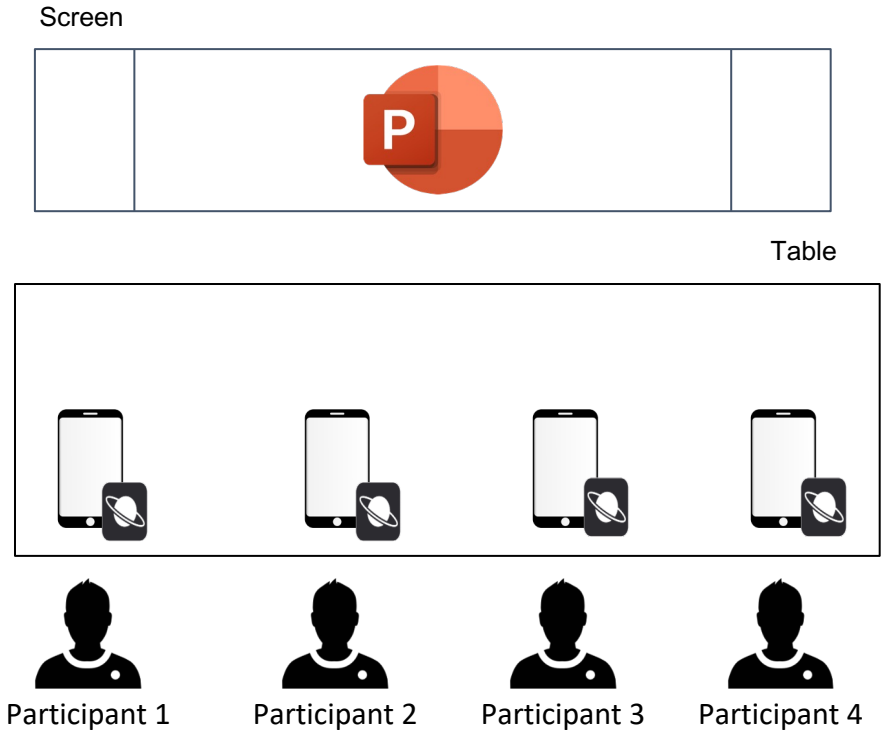
Protected Physical Space

Research Questions

ID	Question	Space Invasion	Space Affectation	Privacy Leak
1	Can participants understand security issues?	✓	✓	✓
2	Can participants identify security issues?	✓	✓	✓
3	Can participants write effective policies?	✓	✓	-
4	Can participants comprehend policies?	✓	✓	-
5	Can participants use our privacy tool properly?	-	-	✓
6	Do participants agree with regulating MAR?	✓	✓	✓

User Study

- Conducted with 40 participants,
- Different education background,
  - CS vs Non-CS,
- Group sessions of 60 min,
- Followed procedure approved by IRB,
  - Introduction,
  - SpaceMediator usage,
  - Questionnaire.



Results

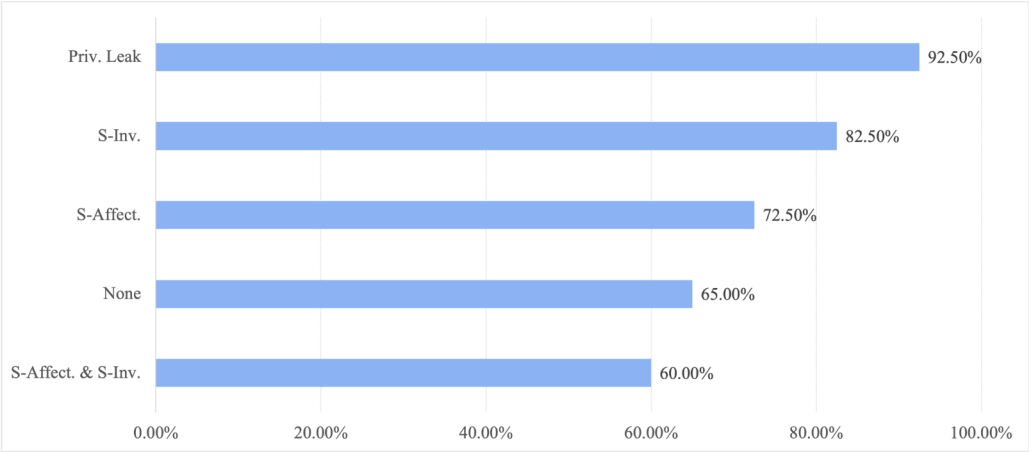
RQ2. Can participants identify security issues?

Example - Space Invasion

“The Communications Director from the Holocaust Museum in Washington, D.C., wants the Museum excluded from Pokémon Go. The game is considered inappropriate for the memorial.”

Compromised Scenarios

- Total of 5 with different attacks,
- Participants recognized them successfully.

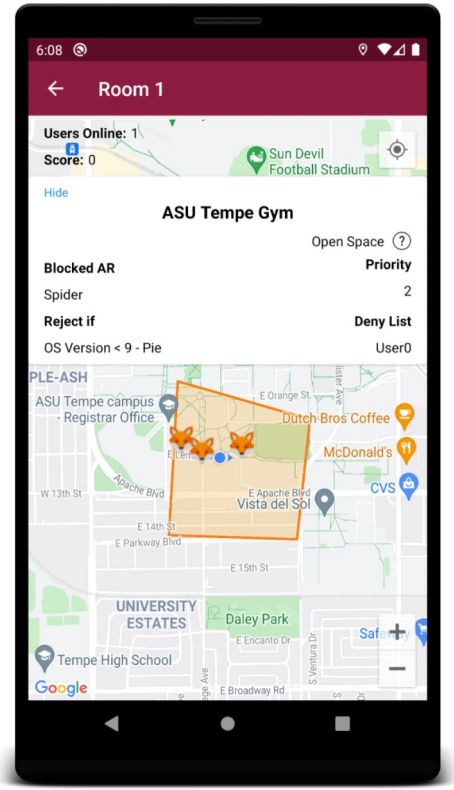


RQ3. Can participants write effective policies?

Exercise 1

"At ASU Tempe campus, ***block*** spiders MAR content, and ***deny*** access to Eve or anyone who has an OS less than Android Pie."

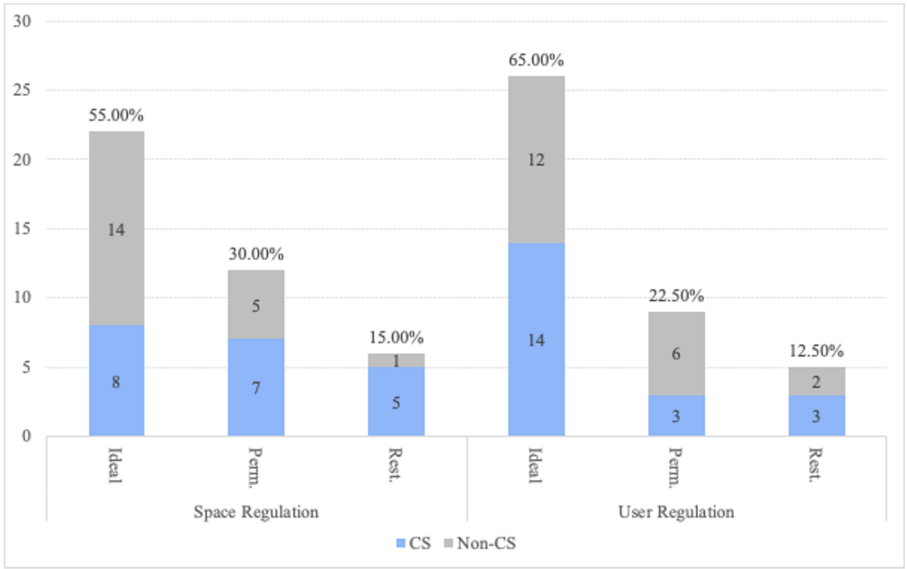
- Total of 4 exercises,
- Different types of policies,
- Distinct attributes per policy.



RQ3. Can participants write effective policies?

Policy Evaluation Results:

- Restrictive,
  - Compromises functionality,
- Permissive,
  - Vulnerable to security problems,
- Ideal,
  - Carries all expected regulations,
- Most were ideal.



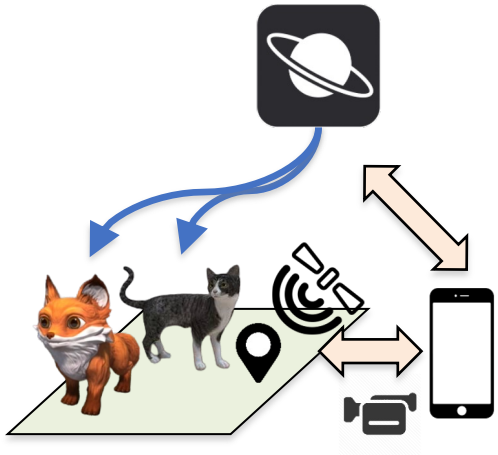
Ending Remarks

Future Work

- Emphasize front-end development to write regulations,
- Proper determination and authentication of space ownership,
- Database processing at scale,
- Further analysis on improper policies' security and usability,
- Future upload to Google Play.

Conclusion

- MAR is in its first development phase, but growing at a tremendous pace,
- Still, some issues exist: privacy, space affectation, and space invasion,
- High understanding and interest in prevention of MAR-Apps security issues.



Protected Space

Thank You!

Any further questions you may contact us:

Carlos Rubio-Medrano

carlos.rubiomedrano@tamucc.edu
https://carlosrubiomedrano.com/