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

Luis Claramunt
lclaramu@asu.edu
Arizona State University
Tempe, Arizona, USA

Carlos Rubio-Medrano
carlos.rubiomedrano@tamucc.edu
Texas A&M University - Corpus Christi
Corpus Christi, Texas, USA

Jaejong Baek
jaejong@asu.edu
Arizona State University
Tempe, Arizona, USA

Gail-Joon Ahn
gahn@asu.edu
Arizona State University
Tempe, Arizona, USA

ABSTRACT

Mobile Augmented Reality (MAR) is a portable, powerful, and suitable technology that integrates *digital content*, e.g., 3D virtual objects, into the physical world, which not only has been implemented for multiple intents such as shopping, entertainment, gaming, etc., but it is also expected to grow at a tremendous rate in the upcoming years. Unfortunately, the applications that implement MAR, hereby referred to as MAR-Apps, bear security issues, which have been imaged in worldwide incidents such as robberies, which has led authorities to ban MAR-Apps at specific locations. Existing problems with MAR-Apps can be classified into three categories: first, *Space Invasion*, which implies the intrusive modification through MAR of sensitive spaces, e.g., hospitals, memorials, etc. Second, *Space Affectation*, which involves the degradation of users' experience via interaction with undesirable MAR or malicious entities. Finally, MAR-Apps mishandling sensitive data leads to *Privacy Leaks*.

To alleviate these concerns, we present an approach for *Policy-Governed* MAR-Apps, which allows end-users to fully control under what circumstances, e.g., their presence inside a given sensitive space, digital content may be displayed by MAR-Apps. Through `SpaceMediator`, a proof-of-concept MAR-App that imitates the well-known and successful MAR-App Pokémon GO, we evaluated our approach through a user study with 40 participants, who recognized and prevented the issues just described with success rates as high as 92.50%. Furthermore, there is an enriched interest in Policy-Governed MAR-Apps as 87.50% of participants agreed with it, and 82.50% would use it to implement content-based restrictions in MAR-Apps. These promising results encourage the adoption of our solution in future MAR-Apps.

CCS CONCEPTS

• **Security and privacy** → **Access control**; • **Human-centered computing** → **Mobile devices**; **Mixed / augmented reality**.

SACMAT '23, June 7–9, 2023, Trento, Italy

ACM ISBN 979-8-4007-0173-3/23/06…$15.00
https://doi.org/10.1145/3589608.3593839

KEYWORDS

Attributes, Authorization Policies, Mobile Augmented Reality

ACM Reference Format:
Luis Claramunt, Carlos Rubio-Medrano, Jaejong Baek, and Gail-Joon Ahn. 2023. `SpaceMediator`: Leveraging Authorization Policies to Prevent Spatial and Privacy Attacks in Mobile Augmented Reality . In *Proceedings of the 28th ACM Symposium on Access Control Models and Technologies (SACMAT '23), June 7–9, 2023, Trento, Italy.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3589608.3593839

1 INTRODUCTION

Augmented Reality (AR) alters the perception of the physical world by merging natural objects with additional *digital content*, e.g., 3D virtual objects, resulting in distinct users' sights of their surroundings. Noticeably, its popularity has increased recently with the introduction of Mobile Augmented Reality (MAR), which leverages mobile devices with low accessibility costs, high power, and communication infrastructure [24]. Currently, several types of applications implement MAR, hereby referred to as MAR-Apps. For example, there are MAR-Apps used for shopping (e.g., IKEA Place, Wayfair, eBay, etc.), entertainment (e.g., Snapchat, MARK, etc.), productivity (e.g., GeoGebra, Measure, etc.), and gaming (e.g., Jurassic World Live, etc.). Furthermore, the last category involves one of the most successful MAR-Apps: Pokémon GO, which became a worldwide phenomenon since its release in 2016 when it experienced 21 million daily active users [26]. Despite being still in its early development stages [29], MAR has succeeded in value, as users and implementation raised considerably [6]. Likewise, further development on libraries facilitates MAR execution, e.g., ARCore [9], ARKite [2], Vuforia [20], etc. Therefore, it is no surprise that Allied Market Research anticipates the MAR market to reach $184.61 billion by 2030, from $12.61 billion in 2020, with a compound annual growth rate of 31.40% from 2021 to 2030 [21].

Thus, with such tremendous potential and with no standard over how to regulate MAR-Apps, it is crucial to consider their safety as some, i.e., Pokémon GO, have been problematic, depicting three major security issues; based on recorded incidents and possible outbreaks. First, *Space Owners*, the entities who are in charge of *sensitive spaces*, .e.g., memorials, hospitals, etc. must have the opportunity to regulate MAR-Apps operations within such locations, as some MAR content might be unwanted or lead to unwelcome behavior; otherwise, they would suffer from *Space Invasion*. Such

incident has already occurred throughout the world with Pokémon GO as Space Owners dealt with intrusive MAR, e.g., the 9/11 Memorial in New York City [27], Auschwitz WWII Holocaust [1], etc. Second, there is also a possibility for digital graffiti as MAR leaves physically unnoticeable traces, e.g., stickers, drawings, messages, 3D objects, etc. Currently, there are no restrictions on such content, allowing hostile entities to place malicious content easily. Furthermore, such entities have already exploited MAR-Apps compromising users' security to execute robberies, fights, assaults, etc. [3]. Overall, the MAR content experience of users is deprecated via dangerous content and risky multi-user interactions, which lead to *Space Affectation* issues. Third, MAR-Apps also deal with sensitive information, which leads to *Privacy Leak* if gathered without explicit user consent or is unwillingly shared with third parties. This issue, which has been found to occur in other sorts of mobile apps [5], also occurs when MAR-Apps mishandle sensitive information, e.g., device facts, user location, user data, etc. [16].

To alleviate these concerns, we propose regulating the operations of MAR-Apps, e.g., under what circumstances they can display 3D objects on certain physical spaces, by means of user-issued authorization policies. For example, Space Owners may be allowed to adequately restrain the utilization of MAR-Apps within their domains, thus preventing the Space Invasion attack described above. Similarly, the interaction between users of MAR-Apps can be also controlled through *Rooms*: isolated and regulated MAR environments for users to join in which the distribution of MAR content can be regulated. This way, each Room receives unique MAR objects, as well as policies created by users determining regulations for access and acceptable MAR content, thus potentially preventing the Space Affectation attack. Alongside, users are also allowed to know and control the release of all the sensitive information collected from them by MAR-Apps through an *Attribute Wallet*: an abstract container which handles the data gathering and release by means of user-issued authorization policies, thus also resulting in the prevention of the Privacy Leak attack. Overall, the specification, evaluation, and enforcement of such security-related constraints lead to our so-called Policy-Governed MAR-Apps. In this paper, we demonstrate such a concept by means of `SpaceMediator`, a *proof-of-concept* Policy-Governed MAR-App that imitates the popular Pokémon GO, as it represents a multiplayer geolocation-based scheme where multi-user interaction is possible through assigned locations to available MAR objects. Although, it respects protected sensitive spaces, restrains interaction among users, and allows them to manage gathered sensitive information.

In order to evaluate the effectiveness and the usability of our approach, we sampled `SpaceMediator`'s through a user study with 40 participants. Without a requirement of prior computer science knowledge or exposure to MAR, they were introduced to the security issues found in MAR-Apps, prevented them in `SpaceMediator`, and provided feedback reflecting their experience. Exemplary research questions considered in our study included the following:

RQ1 Can participants understand the concepts of space invasion, space affectation, and privacy leak attacks?
RQ3 Can participants write effective Space Protection Policies?.
RQ4 Can participants write effective User Interaction Policies?.
RQ7 Do participants agree with the regulation of MAR-Apps?.

The results were satisfactory as, for example, participants comprehended the attacks with rankings as high as 4.65 on a scale from 1 to 5; also, 87.50% of them agreed on Policy-Governed MAR-Apps over sensitive spaces, and 82.50% would implement user regulations. Likewise, they wrote policies to regulate the operations of `SpaceMediator`, which assisted us in testing the feasibility of leaving the regulation responsibilities to ordinary users.

Overall, this paper provides the following contributions:

(1) We explore the potential occurrence in practice of the Spatial Invasion, Spatial Affectation, and Privacy Leak attacks in a series of MAR-Apps collected from Google Play.
(2) We provide `SpaceMediator`, an Open-Source Policy-Governed MAR-Apps that alleviates the aforementioned attacks by giving Space Owners and Users full control over their interaction with MAR content.
(3) We provide the results of a user study featuring `SpaceMediator`, which shows that Policy-Governed MAR-Apps can be understood and practiced by users with a high degree of efficiency and overall satisfability.

2 BACKGROUND AND RELATED WORK

This section starts by providing some basic background on Mobile Augmented Reality in § 2.1 and moves on to describe incidents caused by it in § 2.2. Later, we revise related work in § 2.3.

2.1 Mobile Augmented Reality

Mobile Augmented Reality (MAR) is a portable implementation of *Augmented Reality* (AR) that enables real-time interaction between 3D digital content and the actual physical world [6] It is commonly implemented in mobile applications, thereby referred to as MAR-Apps, accessible through hand-held devices such as smartphones and tablets. The popularity of MAR has considerably grown as it tends to enrich users' experience and improve satisfaction [17]. MAR-Apps have diverse categories, e.g., games, shopping, entertainment, productivity, education, etc. Also, there are some geolocation-based MAR-Apps in which MAR objects are displayed depending on the user's location [15]. For example, Live View Google Maps provides directions with AR arrows which are consistently updated to guide the user to navigate the surroundings [10]. Another example is the very successful MAR-App Pokémon GO [26], in which users must reach the precise spot assigned to a Pokémon to *capture* it by touching the screen to throw a *Poké Ball*.

Furthermore, as the requirement for MAR is for AR technology to be portable, it is worth pointing out that MAR is not limited to hand-held devices, as highly-specialized supporting hardware, e.g., AR *headsets* and AR *smart-glasses*, are reportedly under development and are expected to be released to the public in the next few years [8]. Generally, as these novel devices are expected to be *wearable*, they may lead to more extended utilization with constant modification of surroundings through virtual content. However, as of today, the high-quality AR output they tend to offer brings affordability issues. Therefore, in this paper we focus on regulating the operations of MAR-Apps on hand-held devices as they are the major trend in MAR utilization and are also more accessible since no extra gear is required. However, we believe our approach can be also extended to specialized AR hardware in the future.

2.2 Incidents Involving MAR

Currently, there is an absence of regulations regarding how should MAR-Apps operate. For example, there are no restrictions over where MAR-Apps can be launched, no restrictions over the MAR content available to users, and no restrictions on how MAR objects are distributed among users. As a result, as the popularity of MAR-Apps increases, more incidents caused by MAR have been recorded. For example, people have been able to play Pokémon GO at the 9/11 Memorial in New York City, which was viewed as irreverent by many within the community [27]. Similar situations occurred in Poland's Auschwitz Memorial and Washington's D.C. Holocaust Museum, which requested MAR-Apps to be unplayable sites [1]. The regulation deficiency over how MAR objects are distributed has also compromised users, as it is common for everyone in a MAR-App to have access to the same MAR objects. This has raised security and safety issues as malicious users waited at places where interactive MAR objects were available to assault or rob other users [3]. Moreover, the lack of regulations has also caused crowds of hundreds of players leading to unpleasant noisy environments [4]. Finally, MAR-Apps users have also been involved in general incidents. For example, users broke into private properties as they did not respect the boundaries of deployed MAR objects, had car accidents as they used MAR-Apps while driving, or were injured because of distracted behavior while utilizing MAR-Apps [18].

2.3 Related Work

Recognizing the potential of MAR content technologies, as well as the security and safety issues just described, the computer science research community has kept its initiative and explored AR operations, identified vulnerabilities, and proposed remediations.

Rubio-Medrano et al. [22] proposed *Space-Sensitive Access Control* (SSAC), a mechanism to regulate MAR-Apps over claimed physical spots, e.g., museums, hospitals, memorials, etc. Such SSAC represented an efficient authorization model suitable for MAR-App developers. Although, only Space Owners and developers were capable of regulating MAR-Apps' performance. Regular users, identified as the ultimate target of MAR-Apps, were left vulnerable, for example, to hostile MAR content as featured by the Space Affectation attacks further discussed in § 3.2.

Lebeck et al. [12] recognized security risks in virtual content. Although they utilized virtual reality, i.e., HoloLens, while we focus on accessible MAR-Apps, both technologies output virtual content that merges with the physical world and alters users' perspective. Furthermore, virtual content genuinely impacts the physical world, affecting users' actions and behaviors. Thus, maliciously placed AR content might cause dangerous or undesired actions among users. Alongside, a threat was detected in multi-user AR, especially among co-located users who modified each other via available AR, e.g., drawing, placing AR objects, etc. Similarly, users were concerned about inappropriate or hostile AR content. As a result, the necessity for further AR regulation was acknowledged, along with challenges in its multi-user implementation: users shall manage their personal space, interact with AR objects personally, and control access to them, resulting in avoidance of unwanted interchange with others.

Lebeck et al. [11] identified security risks involved in MAR-Apps' abilities to modify users' surroundings, as malicious MAR-Apps were identified as capable of causing incidents by obscuring the real world. As a result, to prevent such happenings, MAR-Apps constraint their visual content through policies, which modify MAR content through specified attributes (e.g., size, rotation, etc.). However, while such policies restructured the output, they did not contain regulations that limited available MAR content.

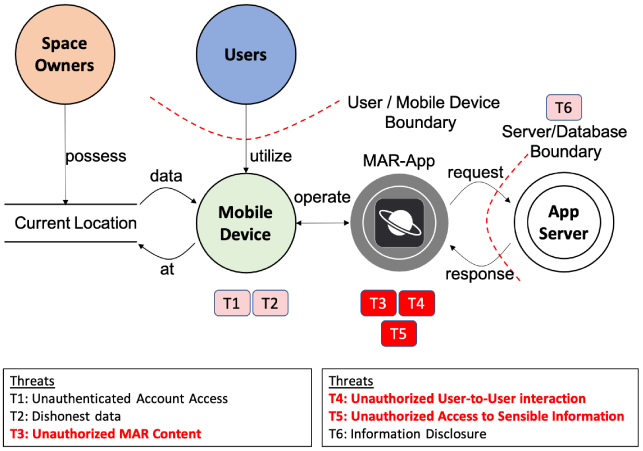


Figure 1: A Threat Model for MAR-Apps.

Some AR content may be considered safety-critical as risks over incorrect AR output may lead to dangerous side effects (e.g., driving, medicine, airplane maintenance, etc.). Therefore, research to analyze and prevent threats over such AR output has been conducted [13]. However, this safety-critical AR is less accessible than MAR-Apps because it requires more expensive tools. Nonetheless, we agree that AR output impacts users as they perceive the AR content, meaning varies, along with decisions taken afterward. Thus, mitigation of risky AR implies avoiding particular AR objects and reducing dangerous usage consequences, i.e., limiting usage time.

Finally, privacy issues over AR are also a primary concern as several researchers have assessed it. For example, Shang et al. [23] developed a successful tracking system to follow users' location in multi-user geolocation-based MAR-Apps. While we did not implement such a system, we recognize a threat to mishandling sensitive information exchange between mobile devices and a cloud service, alongside limiting MAR-Apps permissions. Also, Zhang et al. [30] noticed missing mechanisms in Android to check if MAR collected unnecessary information, leading to a suggested framework to evaluate all information sent to a server. Alongside, we let users manage data gathered from them, as we explain later in § 4.4.

3 PROBLEM STATEMENT

As MAR offers a wide variety of services, it is possible to find distinct types of vulnerabilities throughout MAR-Apps. Therefore, it is essential to specify which ones are our priority throughout this paper. We start with a discussion on our threat model in § 3.1, and continue with a description of the *Space Invasion*, the *Space Affectation*, and the *Privacy Leak* attacks in § 3.2.

3.1 Threat Model

Figure 1 provides a graphical depiction of a Threat Model featuring the security implications for a MAR-App implemented with a

cloud service. MAR-Apps communicate with cloud services and provide comparative data, e.g., location, username, etc., to supplement available MAR content to users. Communication frequency and available content vary according to each MAR-App. Generally, MAR content is available 24/7 and saved for future use. Typical uses include capturing MAR objects, leaving MAR object traces in defined spaces, etc. Some of the denoted threats are ways attackers could exploit mobile apps in general, i.e., stealing poorly stored login credentials (T1), modifying data provided by cellular devices to apps (T2), and intercepting insecurely exchanged information (T6) [14, 19, 25]. In this paper, we focus mostly on threats applicable to unregulated MAR-Apps with possible malicious MAR content (T3), leading to dangerous interaction (T4), and with forbidden access to sensitive data (T5). As shown in § 3.3 and Table 1, we analyzed several MAR-Apps currently available in practice and found them vulnerable to at least one of these threats.

3.2 Spatial and Privacy Attacks

Space Invasion Attack. This attack results from the successful exploitation of T3, and occurs when the *Space Owner*, the entity responsible for *sensitive spaces*, is unsatisfied with the MAR-Apps that can be executed within the location. There are two possible ways MAR-Apps negatively affect sensitive spaces. First, unwanted MAR content that merges with the physical world conducts negative interaction and virtual editing of its surroundings, as described in § 2.1. Second, geolocation-based MAR-Apps could lead users to sensitive spaces and stimulate undesired behaviors, e.g., conglomerations, noisy environments, etc. As a result, space invasion attacks are triggered by unwanted MAR content or subjects that come around to interact with it, as mentioned in the real-world scenarios featured in § 2.2.

Space Affectation Attack. This attack results from the successful exploitation of T4, and is a result of meanly degraded MAR-Apps users' experience, triggered by intrusive MAR content, through which users must interact with MAR objects they despise, and negative user-to-user interaction. Geolocation-based MAR-Apps may lead towards user-to-user interaction as two players meet at the exact spot assigned to a MAR object to play with it. Unfortunately, malicious users have taken advantage of such scenarios, and the multiplayer concept implemented throughout certain MAR-Apps has led to robberies, armed assaults, and other situations [18].

Privacy Leak Attack. This attack results from the successful exploitation of T5. There have been several mobile applications with recorded privacy incidents [5]. Even when privacy issues are not restricted to MAR-Apps, it is noticeable that MAR-Apps share sensitive information between users and even without their explicit consent resulting in Privacy Leak. There is no specific range over the collected data as it could be distributed, i.e., location [16].

3.3 An Exploratory Study on Vulnerable MAR-Apps in Practice

In order to establish the potential occurrence of the aforementioned attacks in practice, we conducted an exploratory study in which we allocated relevant MAR-Apps on Google Play.

Table 1: MAR-Apps with Security/Safety Issues.

MAR-Apps	SI	SA	PL	Downloads	Rating
Pokémon GO	✓	✓	-	100M	4.1
Jurassic World Live	✓	✓	-	10M	4.4
The Walking Dead	✓	✓	-	5M	4.2
Color Quest AR	✓	-	-	1M	3.6
Snaappy	✓	✓	✓	1M	4.2
AR Real Driving	✓	-	-	500K	4.2
Just a Line	✓	-	-	500K	3.5
Weapon AR	✓	✓	-	100K	3.9
vTime XR	✓	✓	✓	100K	3.9
WallaMe	✓	✓	✓	100K	3.6
RealTag	✓	✓	-	100K	3.6
Real Note	✓	✓	✓	50K	3.6
My world	✓	✓	✓	10K	3.7
Tendar	✓	-	-	5K	3.9
MARK	✓	✓	-	1K	3.7

Dataset. Initially, we located a set of potential MAR-Apps by running a search with relevant keywords, i.e., *augmented reality*, and exploring the results in the AR category as provided by Google Play. Next, the suitability of each candidate MAR-App for our study was determined by manually exploring the AR features implemented as a part of their run-time functioning, and by reading their corresponding documentation (if available). As shown in Table 1, a total of 15 out of 22 MAR-Apps were ultimately located, evaluated, and installed for experimental purposes on a Samsung S9 running Android 10 and a Motorola G6 running Android Pie. Also, for each MAR-App, the number of downloads, as well as the user rating, as reported by Google Play by March 2021, was also collected.

Methodology. We utilized the two devices to operate the MAR-Apps with different accounts and replicate multi-user interaction, one represented a *benign* entity while the other a *malicious* one. Through such a process, we examined vulnerabilities and possible attacks. We attempted to use each of the studied MAR-Apps within a series of physical spaces for the Space Invasion attack. If the operation was possible, exposing Space Owners to intrusive MAR, an attack was carried out as successful. For Space Affectation attacks, we evaluated the MAR content offered by the MAR-Apps and how it handled multi-user interaction. A successful attack was conducted by dangerous MAR content, and if the malicious user could compromise other's security via the MAR-App. Finally, we looked at how the MAR-Apps collect and handle sensitive information.

Results. As shown in Table 1, all surveyed MAR-Apps (15/15, 100%) were vulnerable to Space Invasion as they executed in the physical locations, and there was no provided way to limit their operations. In addition, several of the surveyed MAR-Apps (11/15, 73.33%) were found vulnerable to Space Affectation. Some were geolocation-based MAR-Apps (e.g., Pokémon GO, Jurassic World, etc.) where the location assigned to MAR objects was publicly known. As described in § 3.2, this has led to security incidents. Others were social MAR-Apps with no limitations over where MAR content could be shared or published, e.g., Snaappy, RealTag, WallaMe, MARK, etc. One user left traces with hostile MAR content as digital graffiti, and the attack was possible if the other user could interact with such MAR content. Also, some of the MAR-Apps had violent MAR content, i.e., Weapon AR, leading to possible user

experience degradation. Finally, some MAR-Apps demonstrated Privacy Leak Attacks (5/15, 33.33%) as they gathered sensitive information but did not handle it properly. For example, the user's current location was part of a public post without any warning.

4 OUR APPROACH: POLICY-GOVERNED MAR-APPS VIA SPACEMEDIATOR

To prevent the security issues covered in § 3, we propose the adoption of Policy-Governed MAR-Apps, which regulates MAR functionality at run-time. We implement our approach via SpaceMediator, a proof-of-concept MAR-App that imitates Pokémon GO, the most popular MAR-App as denoted by the number of downloads up to March 2021 (Table 1). SpaceMediator is developed in Android and implements Augmented Reality through Google's library *ARCore* [9]. Also, it emulates geolocation-based MAR-Apps by assigning specific coordinates to MAR objects. The content of such MAR objects is limited to Foxes and Spiders in the current version, as shown in Figure 2(b). Similar to the interaction of Pokémon GO, users move around different locations to capture the available MAR objects and score some points. We start by presenting the theoretical foundations of our work in § 4.1, and then we elaborate on how they are implemented into SpaceMediator. Specifically, we address the regulation of sensitive spaces in § 4.2, the restrictions over user interaction in § 4.3, and the privacy of users in § 4.4.

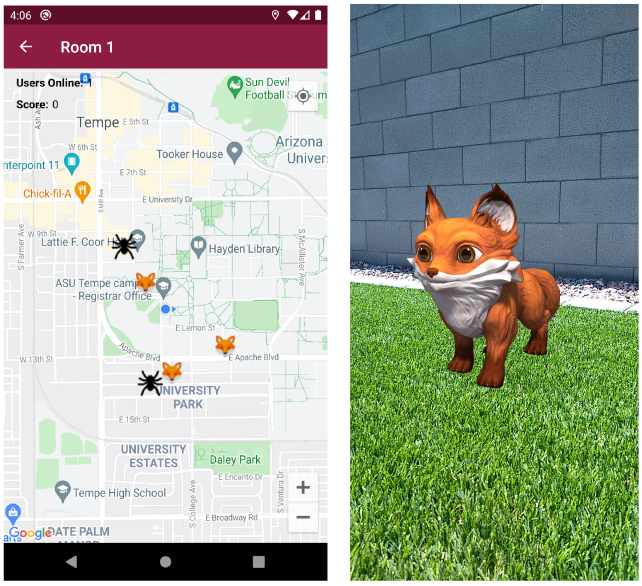
4.1 A Model for Policy-Governed MAR-Apps

In order to effectively implement Policy-Governed MAR-Apps, a theoretical *model* detailing how MAR content is generated, distributed, and eventually delivered to Users is needed. That way, restrictions can be specified to decide what content is displayed within the physical spaces they control, e.g., a player controlling if he/she is *visible* via a 3D avatar to other players over a specific space. Our proposed model, shown in Figure 3, is composed of a set of *Entities* associated with attributes that distinguish them, a set of MAR-related *Functionalities*, as well as different *Modes of Interaction* relating Entities and Functionalities.

Attributes. Our approach for representing the different pieces of security-relevant information required for Policy-Governed MAR-Apps is *attributes*, a convenient abstraction largely explored in the literature [7]. Attributes are typically composed of 3-tuples consisting of (i) a unique *identifier* (ID), e.g. *age*, (ii) a *datatype*, e.g., integer, and (iii) a set of values over the range defined by the datatype, e.g., the range of 0-110 to denote the age of a human being. In addition, attributes may also be obtained from multiple different sources: government, companies, schools, makers, etc.

Authorization Policies. Our policies are then written using attributes obtained from users, e.g., a person using an MAR-App, the MAR-Apps themselves, the hand-held devices, the physical spaces, e.g., home or a park, as well as some other relevant aspects such as time. This way, authorization to distribute MAR content is only granted if all attributes listed in a given policy are shown by the requesting MAR-App at runtime.

Entities and Functionalities. Following Figure 3, the Entities and the MAR-related Functionalities comprised within our model can be described as follows:



(a) Distributed MAR Objects. (b) MAR Objects Interaction.

Figure 2: SpaceMediator: A Geolocation-Based MAR-App.

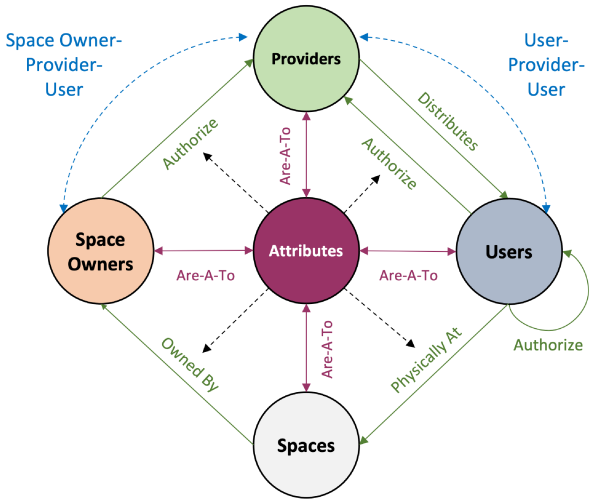


Figure 3: A Theoretical Model for Policy-Governed MAR-Apps. Entities and Functionalities, defined through Attributes, are related to each other via Modes of Interaction.

- *Providers.* A Provider is an Entity primarily associated with *generating*, e.g., developing and maintaining a MAR-App. Generally, they can be related to attributes such as IP addresses as mobile apps are associated with servers. In addition, they *distribute* MAR content for user interaction inside Spaces.
- *Users.* The Users are the Entities who regularly operate a MAR-App. Therefore, they are the ones who interact with the supplied MAR content. As each User is unique, they are associated with attributes that distinguish them or personal information, e.g., ID, name, date of birth, etc. In a Policy-Governed MAR-Apps, Users shall have the opportunity to authorize who they interact with if multi-user interchange is possible and regulate MAR content.

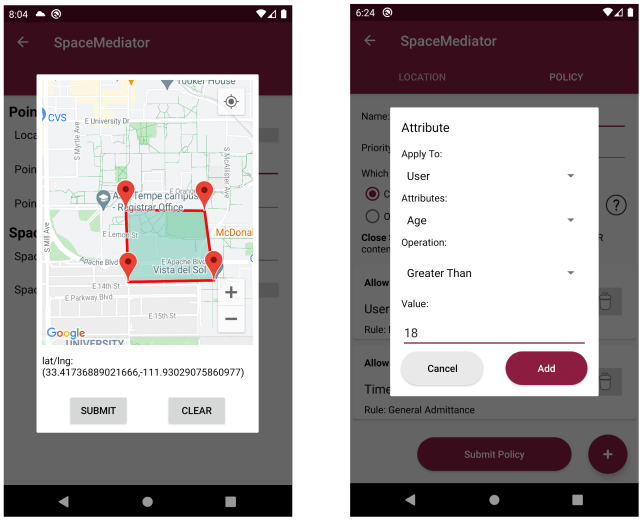
- *Spaces.* A Space represents the physical location of Users while interacting with MAR. As previously discussed in § 2.1, MAR merges 3D digital content and the physical world. Therefore, leading to virtual manipulation or alteration of the surrounding. Some attributes that identify Spaces may include a set of geographical coordinates, distance, altitude, etc.
- *Space Owners.* Finally, the Space Owners are the Entities who have the right of deciding if MAR content can be displayed inside a Space, therefore, they are said to *own* a Space. There is a wide range of possible Space Owners as MAR can influence various areas, e.g., parks, museums, businesses, residential areas, schools, etc. They are associated with attributes that assist in distinguishing them since each one is unique, e.g., ID, name, etc. Space Owners shall be able to avoid unwanted MAR content and antagonistic behavior on their property. In this paper, we assume space ownership has been previously determined by external means, and, therefore is outside the scope of our research.

Modes of Interaction and Attacks. To recapitulate, we have described the Entities involved in our model, their roles, how attributes are suitable to identify them, and their essential relationship with one another. Although, we must look deeper into how the implementation of authorization policies prevents security issues. Therefore, it is worth examining the two *Modes of Interaction* that result from the presented regulations among Entities:

- *Space Owner-Provider-User*: Space Owners set regulations over MAR content and usage in a sensitive space, a claimed area, to Providers. Afterward, Providers will consider such regulations before delivering MAR to Users within the established sensitive space. As a result, Users are limited to authorized interactions within the specified boundaries. Therefore, the enforced restrictions potentially prevent the Space Invasion Attack.
- *User-Provider-User*: Users shall also establish regulations to Providers over the operation of the MAR-Apps that might impact them. Overall, they must regulate two parameters. First, the scope of MAR content they authorize for interaction. Then, if the MAR-App has multiplayer interaction, Users shall establish who they are willing to encounter. As a result, Providers will only distribute benign MAR content and avoid user-to-user interaction with unwanted parties. Therefore, limiting malicious third-parties exposure via MAR and potentially preventing the Space Affectation Attack. Likewise, Users must control the data MAR-Apps collect from them. They must be aware of any gathered sensitive information and manage to deliver it to Providers according to their will. Thus, stopping unawareness of personal data received by third parties and potentially preventing the Privacy Leak Attack.

4.2 Regulating Sensitive Spaces

As previously explained in § 3.2, the sensitive spaces are areas exposed to Space Invasion attacks by mishandled MAR. Therefore, it is necessary to offer Space Owner, the entities in charge of such sites, the possibility to regulate the operation of the MAR-Apps within such locations. As a result, we implement through `SpaceMediator` the *Space Owner-Provider-User* Mode of Interaction, described in § 4.1, such that Space Owners are capable of enforcing restrictions over their sensitive spaces.



(a) Defining a Sensitive Space. **(b) Creating a Constraint.**

Figure 4: Policy Creation for a Sensitive Space.

Policy Creation. Space Owners write policies to establish how they want to regulate MAR-App operations over their claimed sensitive space. This process starts with Space Owners specifying their claimed area via geographical points, where the policy will go into effect, as shown in Figure 4(a). Then, they select the regulation type they want to implement in the policy, which will decide the policy's combining algorithm and rules' effect. There are two regulation types offered in `SpaceMediator` to offer a wider variety of possible policies. First, the *Open Space*, designed for Space Owners with low restrictive parameters, which is compatible with the XACML policy featuring the *permit-unless-deny* rule combining algorithm with Deny rules [28]. Second, the *Close Space* facilitates high restrictive constraints, resulting in an XACML *deny-unless-permit* policy with Permit rules. Finally, as displayed in Figure 4(b), they specify the attributes they want as part of the policy, e.g., Age > 18, Username = $User_1$, Time ≤ 12:00:00, etc. It is important to point out that whether such attributes are permitted or denied depends on the selected regulation type. Therefore, let us look into each of the mentioned regulation types, i.e., policy structure and rules.

Open Space. This regulation consists of two policies used for different purposes. Selecting an Open Space implies a predefined structure for these policies. As shown in Figure 5, both have an XACML *permit-unless-deny* combining algorithm, rules with Deny permission, and attributes appended by *OR* logical operators. As a result, met statements in the policy result in a Deny authorization when evaluated, otherwise in a Permit. Therefore, Space Owners just define reject parameters through an Open Space.

- *MAR Distribution Policy.* In `SpaceMediator`, this policy describes how to handle MAR content within a sensitive space. It is used throughout MAR object distribution from the Provider.
- *MAR Interaction Policy.* In `SpaceMediator`, this policy controls users' interaction with available MAR objects within a sensitive space. There are two rules applicable to users:
  (1) *Deny List Rule.* This rule consists of unauthorized usernames that shall not interact with the available MAR objects within the sensitive space.

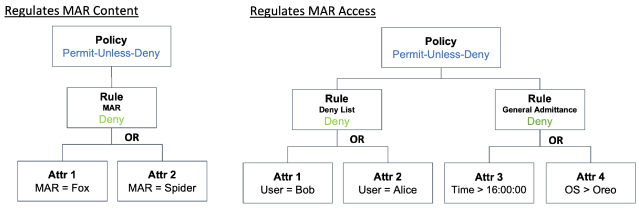


Figure 5: Open Policies.

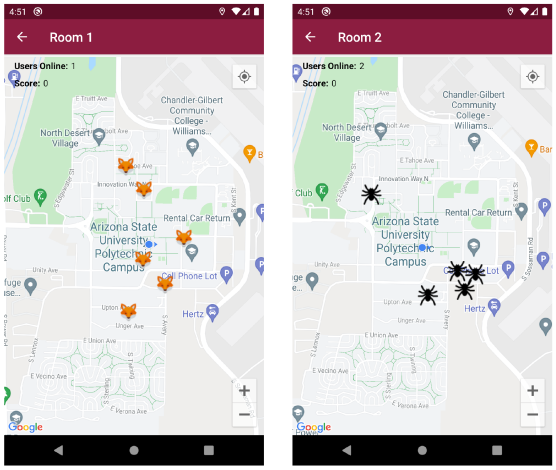
(2) *General Admittance Rule.* This rule considers attributes that apply to all users, e.g., Time, OS Version, Device Manufacturer, etc. Those who meet any of the specified conditions in this rule shall be unauthorized.

Close Space. The structure of Close spaces is very similar to Open Spaces. It also consists of two policies, but the resulting limitations are different as it utilizes an XACML *deny-unless-permit* combining algorithm, rules have Permit permission, and the General Admittance Rule has its attributes appended by *AND* the logical operators. Therefore, these are more restrictive as policy statements are used are requirements for authorization, and failing to meet them results in denial. Although, the two policies within a Close Space hold the same purpose as in an Open Space.

4.3 Regulating Users Interaction

As previously mentioned in § 3.2, malicious parties have compromised the security of users by exploiting the known locations of MAR objects in multi-user geolocation-based MAR-Apps. Thus, to possibly prevent such scenarios and Space Affectation overall, we implement in SpaceMediator the *User-Provider-User* Mode of Interaction, described in § 4. As a result, MAR objects distribution among users is done through *Rooms*: isolated and regulated MAR environments for users to join.

Rooms. Regulating multi-user interaction brings alongside the challenge of assembling an easy-to-use process for users. Because of this, SpaceMediator implements such regulations through Rooms, an extra layer to protect users from Space Affectation. Through them, users are separated into different groups, they decide whom to interact with, access is restrained, and each Room is provided with unique MAR objects for interaction. In addition, SpaceMediator offers a Lobby that displays the available Rooms and applicable constraints. At the Lobby, users select a Room to join or create a new one, implementing their desired user interaction regulations. Afterward, users enter a Room and operate SpaceMediator by capturing available MAR objects. Rooms are isolated as a user can only be in one Room at a time, and the MAR objects provided to each Room are distinct. Also, they are regulated as they have admission requirements for users, and it filters the content of MAR objects to avoid undesirable ones. As shown in Figure 6, the two Rooms available in the Lobby are provided with their respective MAR objects for interaction, and the location and content of such MAR objects vary since Room 1 only allows foxes while Room 2 rejects them. There could be several users within a Room, but only one with the role of *HOST* establishes the applicable policies. Rooms implementation through SpaceMediator is reflected in Figure 7, and can be outlined in the following three steps:



(a) Room 1. **(b) Room 2.**

Figure 6: Distribute MAR Objects per Room.

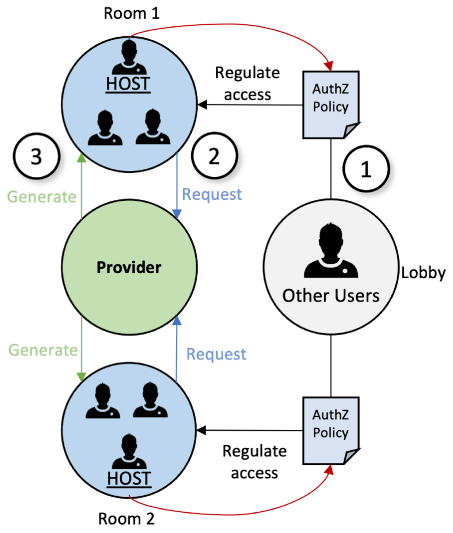


Figure 7: User Interaction via Rooms.

(1) *Join Room:* Users find available Rooms through a Lobby. There they try joining an existing Room, regulated by the HOST's policies. For example, a Room could only allow underage players. Users could also create new rooms if unable to join any.
(2) *Room Interaction:* Users request new MAR objects for interaction within the Room. For example, such demands are generated as they move to distinct locations where no MAR objects are available. In general, SpaceMediator submits automated requests to the Provider for new MAR objects to keep users entertained.
(3) *Regulated MAR:* If the new content request is authorized, the Provider distributes new MAR objects within the Room.

Policy Creation. In SpaceMediator, the user assigned the *HOST* role is in charge of a Room's policy. This role is automatically appointed to whoever created a Room, and it is reassigned in a First-In-First-Out order if the HOST leaves. Thus, users efficiently implement their desired regulations by creating a Room in SpaceMediator's Lobby. Besides, there is no limitation on having one

HOST per Room as creating a new Room is a simple process. `SpaceMediator` offers two regulation types for User Interaction: *Open Interaction* and *Close Interaction*, which define the structure of the policies. Overall, these structures' design is the same as those used for Open and Close Spaces, as shown in Figure 5, as the apply the same combining algorithms, rules' permission effect and relations among attributes. Although, the policies have a different purpose.

- *MAR Distribution Policy:* The Provider evaluates this policy when distributing MAR objects to a Room, omitting intrusive MAR content that degrades the HOST experience.
- *MAR Interaction Policy:* This policy evaluates users who want to join a Room. Thus, only authorized personnel by the HOST may enter and view available MAR objects.

4.4 Respecting Privacy

MAR-Apps are also vulnerable to Privacy Leak issues when gathering data from users, as explained in § 3.2. Likewise, `SpaceMediator` collects data from its users, for example, as they move around to interact with MAR objects. Furthermore, information is retrieved from users to create an *access request*, which contains valuable facts for authorization decisions as it is evaluated against a policy, as described in § 2. Therefore, to respect users' privacy while enforcing regulations, we implement in `SpaceMediator` an *Attribute Wallet*, graphically shown in Figure 8. Through it, users are aware of any information gathered from them. To this end, all data used throughout `SpaceMediator` is within the Attribute Wallet's scope. Most of it is utilized for authorization purposes and represents attributes, e.g., birth date, device manufacturer, current geographical coordinates, etc. The Attribute Wallet also allows users to stop `SpaceMediator` from collecting sensitive information they do not want to provide. Although, there is data outside the Attribute Wallet's range as it is appended at the servers, i.e., time. Users' privacy is respected in `SpaceMediator`, as there is clarity over the compiled information, and users can control it.

5 EVALUATION AND RESULTS

This section presents the methodology and the results of a user study formally approved by our Institutional Review Board (IRB) office. We start with a general overview in § 5.1, covering our objectives, implementation methods, and evaluation techniques. It concludes by presenting and discussing the results in § 5.2.

5.1 User Study

As previously discussed in § 3, several MAR-Apps are available across the different mobile operating systems with millions of downloads, growing popularity, and vulnerability to space and privacy attacks. In our approach to prevent these attacks, we allow users to regulate the functionality of a MAR-App. It intends to be helpful to all users, regardless of their prior knowledge, e.g., access control, computing, etc. To verify the feasibility of our approach, we conducted a user study involving seven *research questions* (RQ):

RQ1 Can participants understand the concepts of space invasion, space affectation, and privacy leak attacks?
RQ2 Can participants identify security issues, with respect to the three attacks just mentioned?.
RQ3 Can participants write effective Space Protection Policies?.

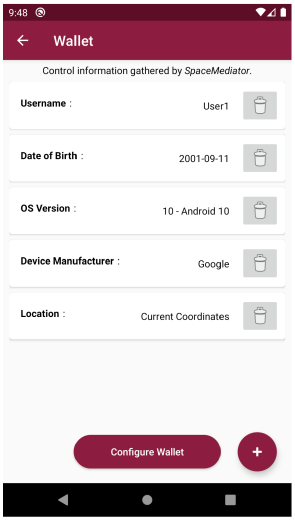


Figure 8: An Attribute Wallet.

RQ4 Can participants write effective User Interaction Policies?.
RQ5 Can participants understand the policies to counteract space attacks?.
RQ6 Can participants utilize our attribute wallet properly?.
RQ7 Do participants agree with the regulation of MAR-Apps?.

Participants and Methodology. For our study, we recruited 40 participants through advertisements placed throughout the university campus. Furthermore, we focused on having participants with distributed background knowledge to identify if prior familiarity with computing was necessary to properly utilize a Policy-Governed MAR-App. As a result, half of the participants identified as having a background in Computer Science (CS). In contrast, the other half pursued degrees in different fields (Non-CS), e.g., engineering, arts, business, etc. The user study was conducted in timeframe group sessions with an average of 60 min. Through them, we gathered data from participants anonymously to evaluate the efficiency of the proposed methodology to regulate MAR-Apps to prevent space and privacy attacks. In addition, as participation was voluntary and we appreciated their collaboration, each participant received a $20 Amazon gift card by the end of each session. The procedure implemented in each group session throughout the user study consisted of three phases: introduction, MAR-App interaction, and a questionnaire. Through them, we assured participants had a basic knowledge on relevant topics, used `SpaceMediator` when ready, and finalized by gathering feedback, all within a reasonable timeframe to maintain focus.

Phase 1: Introduction. In this first phase of the user study, within 15 minutes, we explained our project's scope to participants. This covered topics such as the current status of MAR-Apps, security issues triggered by MAR-Apps (§ 2.2), vulnerabilities on MAR-Apps (§ 3), our approach to preventing such vulnerabilities (§ 4), etc. We covered the topics gently for understandability regardless of familiarity with cybersecurity. By the end of the introduction, we wanted participants to understand MAR, its vulnerabilities, and the regulations implemented in `SpaceMediator`.

Table 2: SpaceMediator Regulations.

Policies	Rules	Attributes	Operations
Distribution	MAR	Content	=
Interaction	Permit/Deny	Username	=
	Admittance	Age	=, >, ≥, <, ≤
		OS Version	=, >, ≥, <, ≤
		Manufacturer	=
		Time	≥, ≤
		Other	=

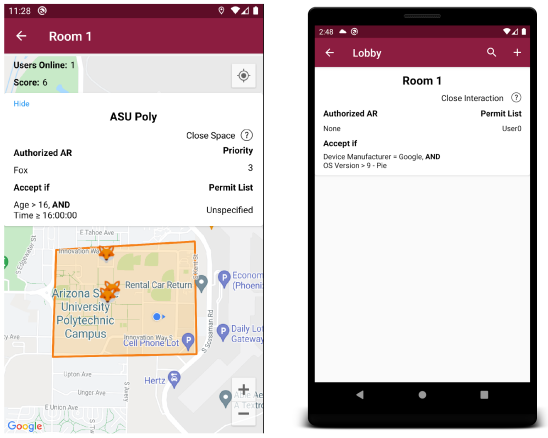
Table 3: User Study Policy Exercises.

ID	Policy Description	Regulation
1	At the university campus, block spiders MAR content, and deny Eve or anyone with an OS less than Android Pie.	Open Space
2	At the college building, allow spiders MAR content and grant access to adults only after 6:00 p.m. or Bob.	Close Space
3	Within the room, allow MAR content of foxes and grant access to university students.	Close Interaction
4	Deny access to Eve or anyone else who has a Samsung device, is underage, or has an OS version less than Android 10.	Open Interaction

Table 4: Questionnaire Policy Making - Sensitive Space.

Policy Description	Answer
At the university campus allow foxes and deny interaction with users who are over 16 years of age after 4:00 p.m.	-
At the university campus allow foxes and authorize interaction with users who are over 16 years of age after 4:00 p.m.	✓
At the university campus allow foxes and deny interaction with users who are less than 16 years of age after 4:00 p.m.	-
At the university campus allow foxes and authorize interaction with users who are over 16 years of age before 4:00 p.m.	-

Phase 2: MAR-App Interaction. Once participants were familiar with the purpose of our project and the essential topics covered within it, we allowed them to use SpaceMediator, our MAR-App with regulated functionality. Using SpaceMediator, they followed a set of predefined exercises to write four policies. Table 3 shows the English-written policy descriptions provided to the participants. Through such descriptions, we specified the authorized or unauthorized entities. As a result, each participant wrote two policies to prevent space invasion as Space Owners of a specified location and two to avoid space affectation by regulating user interaction in a room. The crafted policies were associated with an account given to each participant, stored in a database, and analyzed afterward. In addition, provided supplementary material for the first exercise of each category offered a quick review of the topics covered in the introduction phase, i.e., graphs of policy structure. With SpaceMediator installed on four different devices, participants could complete these exercises in an average of 30 min. We utilized two



(a) Policy for Sensitive Space. (b) Policy for User Interaction.

Figure 9: Questionnaire Policies Displayed.

Google Pixel 3XL with Android 11 and 4 GB of RAM, a Samsung S9 with Android 10 and 4 GB of RAM, and a Motorola G6 with Android Pie and 2 GB of RAM.

Phase 3: Questionnaire. To conclude a session, participants answered a questionnaire with relevant inquiries to reflect their understanding of the covered topics and provide feedback. We gathered this data through an online questionnaire divided into four sections, completed in an average of 15 minutes. The content used throughout the questionnaire is available upon request to the authors. The first section, *scenario recognition*, consisted of five scenarios with different security issues; and participants had to identify the undergoing attacks. Next, the policy-making section consisted of two types of questions involving SpaceMediator's GUI. First, *policy-making description* through which participants associated a displayed policy, as Figure 9(a), with its proper description, as shown in Table 4. Second, the *policy-making attribute wallet* consisted of selecting the attributes required to gain access over a stated policy, as Figure 9(b), while protecting their privacy. Subsequently, participants provided a scale representation, ranged 1 to 5, to reflect comprehension of the security topics throughout the *policy understanding* section. Finally, they let us know their agreement on MAR-Apps regulations by the *exit* section.

Policy Evaluation. By following the English-written policy descriptions presented in Table 3 and using SpaceMediator, each participant created a total of four policies to regulate MAR and prevent space attacks. These policies had specific regulation goals stated in the descriptions, i.e., specifying the regulation type and applicable attributes. To evaluate if a policy was written correctly, we evaluated it against a request sequence that tested how authorization was handled over expected entities. For further clarity, let us consider the following example in which Exercise 1 states requirements to block three attributes (MAR spiders, user Eve, OS Pie) in the following way:

At the university campus, block spiders MAR content, and deny Eve or anyone with an OS less than Android Pie.

In SpaceMediator, users selected the regulation type for the policy, i.e., open or close, and added relevant attributes. The side effects of the regulation type were adequately reflected on the GUI.

Table 5: Access Requests for Testing Exercise 1.

Attribute	Request 1	Request 2	Request 3
MAR Content	Spider	-	-
Username	-	Eve	Alice
OS Version	-	Android 10	Oreo

Nonetheless, participants could *miswrite* the policy, e.g., incorrect regulation type, missing relevant attributes, etc. By evaluating each policy against a sequence of requests containing essential details, as Table 5 for Exercise 1, we assessed if a policy managed authorization properly. These policy-request evaluations were conducted through an automated process using the same API implemented in `SpaceMediator` and described in § 4. Furthermore, policy syntax was also reviewed manually to verify each request's Permit/Deny results. Finally, we followed an evaluation scheme to categorize a policy as: *ideal*, carried out all expected regulations; *permissive*, vulnerable to security problems; *restrictive*, compromised functionality. For example, following Table 5, the ideal policy meets the standards by denying access to only three expected entities: spider, Eve, and Android Oreo; a permissive policy grants access to undesired parameters, i.e., Android Oreo; and a restrictive policy only allows limited attributes, i.e., Alice is given access but not Android.

5.2 Results

As previously described in § 5.1, participants were evenly distributed in terms of background field, CS vs. Non-CS. However, we also worked with a population with distinct educational ranks since 22.50% recognized the high school as their highest level, 42.50% had concluded an undergraduate major, and 35.00% had achieved a graduate degree. Also, they identified different experience levels of familiarity with MAR as 65.0% had no prior knowledge, 32.5% held medium experience, and only 2.5% rated it as well known. As a result, we worked with a diverse population, gathered helpful information, and further analyzed it to answer our RQs.

RQ1. Can participants understand the concepts of space invasion, space affectation, and privacy leak attacks? To address RQ1, we performed the questionnaire's policy understanding described in § 5.1. The results are shown in Figure 10, with an average on each security issue per background field. Overall, participants successfully comprehended the issues described throughout the user study, as they provided good ratings reflecting it. However, space affectation had the lowest ranking with 3.55 within the CS, 4.30 among the Non-CS, and a prevailing norm of 3.93. On the other hand, space invasion had better ratings with 4.30 within the CS, 4.60 in the Non-CS, and an average of 4.45. Finally, privacy leak was the best-understood security issue with 4.70 for CS, 4.60 for Non-CS, and a standard of 4.65.

RQ2. Can participants identify security issues, with respect to the three attacks just mentioned? To manage RQ2, we conducted the questionnaire's scenario recognition. The outcomes are shown in Figure 11. Privacy Leak was the most recognizable security issue, with 92.50% of participants identifying a such problem in the expected scenario. Afterward, space invasion had a distinction rate of 82.50%, followed by space affectation with 72.50%. Also, an uncompromised scenario with no undergoing attacks was identified by 65.00% of participants. Finally, with a 60.00% success rate,

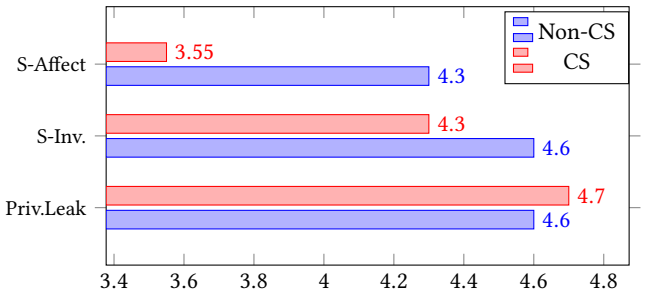


Figure 10: Comprehension of Security Issues.

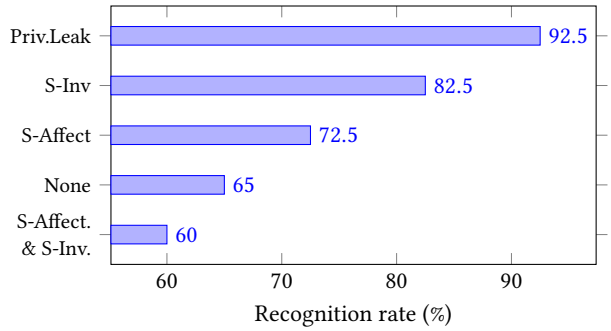


Figure 11: Detection of Security Issues.

participants recognized simultaneous space invasion and space affectation attacks. Noticeably, the understandability reflected in RQ1 goes along with the identifiability success rates in RQ2. For example, privacy leak was the most understandable security issue by participants in RQ1, and at the same time, it had the highest identifiability success in RQ2. Furthermore, the exact trials apply to space invasion and space affectation in second and third places. Therefore, we can notice consistency over the user study data reflecting comprehension over security issues.

RQ3. Can participants write effective Space Protection Policies? To answer RQ3, we evaluated the policies participants wrote as Space Owners throughout the MAR-App interaction via a procedure described in § 5.1. The results are displayed in Figure 12, with the results from Table's 3 Exercises 1-2. Overall, 55.00% of the policies were ideal as they effectively regulated a sensitive space, preventing a space invasion attack. The remaining set of improperly written policies contained different types of errors. For example, most of the incorrect policies for introductory Exercise 1 were restrictive at 30.00%, and the remaining 15.00% were permissive; on the other hand, the more challenging Exercise 2 had the opposite results with 30.00% permissive and 15.00% restrictive. It is noticeable that in Exercises 1 and 2, Non-CS participants had a higher success rate since at least 50.00% of them wrote ideal policies.

RQ4. Can participants write effective User Interaction Policies? We followed the same procedure for RQ4 as in RQ3. Therefore, results are also shown in Figure 12, but with results from Table's 3 Exercises 3-4. Interestingly, the success rate of ideal policies was higher for user interaction, with 70.00% in introductory Exercise 3 and 65.00% in the more demanding Exercise 4. Although, there were still unsuccessful policies in terms of regulations. In Exercise 3, the mistaken policies had 15.00% for both permissive and restrictive; meanwhile, Exercise 4 had results of 22.50% permissive and

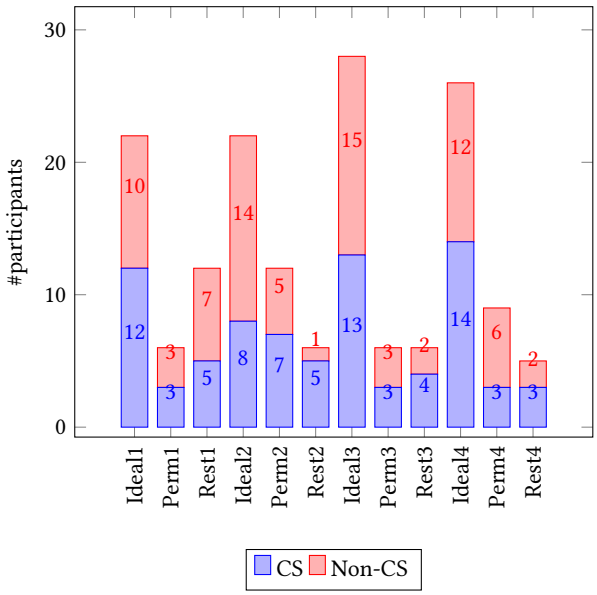


Figure 12: Performance in User Study Policy Writing.

12.50% restrictive. The higher success rate on Exercises 3-4 may be related to increased familiarity with SpaceMediator. By the time participants reached these exercises, they had written the space protection policies from Exercises 1-2. Therefore, they likely had a better understanding of how to operate SpaceMediator, considering the importance of a step-by-step guide to ensure the GUI offered to write policies to regulate MAR-Apps is well understood. Although, more research is necessary to confirm this idea.

RQ5. Can participants understand the policies to counteract space attacks? To handle RQ5, we performed the questionnaire's policy-making, described in § 5.1. In general, participants performed pretty well throughout these exercises. For example, the space regulation policy displayed in SpaceMediator GUI was associated with its appropriate description by 87.50% of the participants. In contrast, the user regulation policy had a lower success rate of 75.00%. Still, these are satisfactory results as they reflect comprehension by the majority of the population over the regulations implemented in a MAR-App. It is possible the long and complex description used through the questionnaire's policy-making confused participants. Therefore, breaking them into multiple easy-to-read questions could improve the outcomes. Of course, further research is necessary to understand the requirements for better results.

RQ6. Can participants utilize SpaceMediator's attribute wallet properly? To address RQ6, we conducted the questionnaire's policy-making - attribute wallet. The results are shown in Figure 13. In the first question, which consisted of two details, i.e., username and SSN, 92.50% of the participants successfully selected necessary features for proper policy evaluation as one rule could be satisfied. Concurrently, 37.50% of them provided additional unnecessary information for the policy, e.g., date of birth, device manufacturer, OS version, etc. The results were similar throughout the second question in terms of access with 95.00%. Although, there was better awareness of privacy as only 18.42% of such participants supplied unneeded traits. Overall, a significant portion of participants provided only the necessary attributes. It is an excellent first step

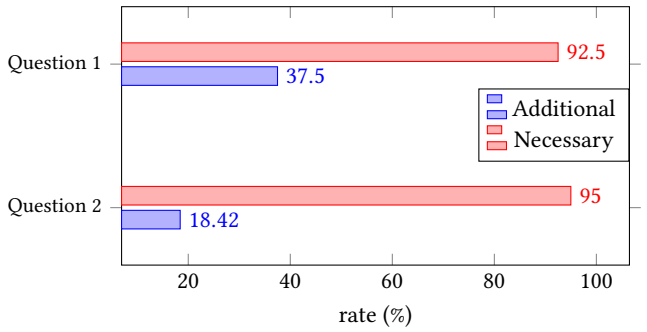


Figure 13: Performance in Privacy.

towards evaluating how an attribute wallet would respect users' privacy without compromising the functionality of MAR-Apps.

RQ7. Do participants agree with the regulation of MAR-Apps? To manage RQ7, we performed questionnaire's exit described in § 5.1. We found out that 87.50% of participants agreed that businesses and institutions should be able to regulate MAR-Apps, 7.50% were uncertain, and 5.00% were against it. Similarly, 82.50% of participants would regulate MAR-Apps if possible, 15.00% would consider it, and only 2.50% discarded it. Overall, there is high interest in the MAR-Apps regulation, preventing space invasion attacks and space affection.

6 DISCUSSION AND FUTURE WORK

In the user study, we addressed the participants' understandability of the space and privacy attacks covered in § 3.2. As a result, we found out that a significant majority of the participants correctly comprehended the security issues. Furthermore, they successfully identified threats that compromised security on a given set of scenarios, as discussed in § 5.2. There was no noticeable difference in the performances between CS and Non-CS participants, indicating users can handle these issues without any specific background.

Upgrading the GUI. We also addressed the usability of our *proof-of-concept* Policy-Governed MAR-App SpaceMediator, with the Control Model covered in § 4 and implementation in § 4. Overall, participants' performance was decent as most of their policies enforced ideal regulations. Nonetheless, there are areas for improvement in this field. For example, considering that Non-CS participants had a slightly better performance than CS, along with the high prevailing understandability of the security issues, we suggest that better results on policy writing depend on further development in SpaceMediator's front-end. As covered in § 4.3, SpaceMediator wrote policies through a GUI that reflected applicable attributes and their effect on them, i.e., permit or deny. Therefore, we did take care of having an understandable GUI. However, this was not our top priority, and several participants missed the data pointed out, leading to erroneous policies. As a result, we are now aware of the importance of MAR-Apps front-end when crafting regulations. Thus, SpaceMediator's subsequent versions should bring an upgrade within this scope, and there is a wide possibility of advancements. For example, a noticeable distinguishment between permit and deny, pointing out the relationship between attributes, building one rule at a time for better interpretation of policy structure, and vibration when updating policy's regulation type.

Need for Further Analysis. As a result, there might be a higher result on ideal policies. Furthermore, we should also take into account the policy evaluation types. As addressed in § 5.1, policy evaluation resulted in three categories: ideal, permissive, and restrictive. Through these evaluations, we classified the possible side effects an erroneous approach could have while regulating a MAR-App. Although, the reality is that participants had different errors within the same type. For example, permissive policies had security problems, but some only allowed one unauthorized entity while others had no restrictions. Therefore, through our evaluations, we know whether erroneous policies tend toward security or usability issues, but further analysis is required to adequately assess the scalability of their consequences.

Ownership of Spaces. Finally, we are aware that participants were capable of specifying the sensitive spaces whenever writing a policy as a Space Owner, as explained in § 5.2. Still, there is a concern for further action to verify ownership over the claimed areas. Since `SpaceMediator` is a *proof-of-concept* Policy-Governed MAR-App, we considered such a process out of our scope, even though we agree it may be necessary to prevent malicious entities from meanly regulating a space they do not legitimately own.

7 CONCLUSION

MAR-Apps have been problematic due to a lack of regulations since they are still in early development. However, as the MAR market is expected to grow at substantial rates, it is crucial to evaluate recorded issues to prevent further ones. In this paper, we introduced the concept of Policy-Governed MAR-Apps, which is implemented in the *proof-of-concept* `SpaceMediator`, which protects sensitive spaces as only authorized MAR merges with the physical surroundings, at the same time it only allows benign multi-user interchange through controlled user interaction, and respects users' privacy by granting management over gathered sensitive information. Additionally, our study showed a high interest throughout the user study community for further implementation of Policy-Governed MAR-Apps, along with high understandability over the risks MAR-Apps involve, and effective success rates in enforcing `SpaceMediator`'s regulations. showing that Policy-Governed MAR-Apps is a convenient regulatory mechanism to protect Space Owners and users.

ACKNOWLEDGMENTS

This work was partially supported by the grants from the National Science Foundation (NSF-CICI-2232911), the Institute for Information & Communications Technology Promotion (IITP-MSIT-2017-0-00168), and Texas A&M University - Corpus Christi.

REFERENCES

[1] Allana Akhtar. 2016. Holocaust Museum, Auschwitz want Pokémon Go hunts out. https://www.usatoday.com/story/tech/news/2016/07/12/holocaust-museum-auschwitz-want-pokmon-go-hunts-stop-pokmon/86991810/.
[2] Apple. 2023. ARkit. https://developer.apple.com/augmented-reality/arkit/.
[3] BBC. 2016. Hundreds of Pokemon Go incidents logged by police. https://www.bbc.com/news/uk-england-37183161.
[4] BBC. 2016. Pokemon Go away: Troublesome Sydney Pokestop shut down. https://www.bbc.com/news/technology-36948331.
[5] Aaron Beach, Mike Gartrell, and Richard Han. 2009. Solutions to Security and Privacy Issues in Mobile Social Networking. *2009 Int. Conf. on Computational Science and Engineering* 4, 1036–1042.
[6] Mark Billinghurst, Adrian Clark, and Gun Lee. 2015. A Survey of Augmented Reality. *Foundations and Trends in Human–Computer Interaction* 8, 2-3 (2015), 73–272. https://doi.org/10.1561/1100000049
[7] Chung, David Ferraiolo, David Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. 2019. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927500.
[8] Forbes. 2023. I've Seen The Future Of AR Glasses At CES 2023 - And It's Amazing. https://www.forbes.com/sites/barrycollins/2023/01/05/ive-seen-the-future-of-ar-glasses-at-ces-2023and-its-amazing/. Last accessed: February 23, 2023.
[9] Google. 2023. ARCore. https://developers.google.com/ar.
[10] Todd Haselton. 2021. Google Maps has a wild new feature that will guide you through indoor spaces like airports. https://www.cnbc.com/2021/03/30/google-maps-launches-augmented-reality-directions-for-indoor-spaces.html.
[11] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2017. Securing Augmented Reality Output. *2017 IEEE Symposium on Security and Privacy (SP)*, 320–337.
[12] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2018. Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. *2018 IEEE Symposium on Security and Privacy (SP)*, 392–408.
[13] Robyn R. Lutz. 2018. Safe-AR: Reducing Risk While Augmenting Reality. , 70-75 pages. https://doi.org/10.1109/ISSRE.2018.00018
[14] Chen Lyu, Amit Pande, Xinlei Wang, Jindan Zhu, Dawu Gu, and Prasant Mohapatra. 2015. CLIP: Continuous Location Integrity and Provenance for Mobile Phones. *2015 IEEE 12th Int. Conf. on Mobile Ad Hoc and Sensor Systems*, 172–180.
[15] Gabriel Meyer-Lee, Jiacheng Shang, and Jie Wu. 2018. Location-leaking through Network Traffic in Mobile Augmented Reality Applications. *2018 IEEE 37th Int. Performance Computing and Communications Conf. (IPCCC)*, 1–8.
[16] R.P. Minch. 2004. Privacy issues in location-aware mobile devices. *37th Annual Hawaii Int. Conf. on System Sciences, 2004. Proc. of the*, 10 pp.–.
[17] José Miguel Mota, Iván Ruiz-Rube, Juan Manuel Dodero, and Inmaculada Arnedillo-Sánchez. 2018. Augmented reality mobile app development for all. *Computers & Electrical Engineering* 65 (2018), 250–260.
[18] CBS News. 2016. Terrible things happening to Pokemon Go players. https://www.cbsnews.com/pictures/terrible-things-happening-to-pokemon-go-players/2/.
[19] Lucky Onwuzurike and Emiliano De Cristofaro. 2015. Danger is My Middle Name: Experimenting with SSL Vulnerabilities in Android Apps. , 6 pages.
[20] PTC. 2023. Vuforia. https://www.ptc.com/en/products/vuforia.
[21] Allied Market Research. 2021. Global Mobile Augmented Reality Market to garner $184.61 billion by 2030: Allied Market Research. https://www.globenewswire.com/news-release/2021/09/15/2297215/0/en/Global-Mobile-Augmented-Reality-Market-to-Garner-184-61-Billion-by-2030-Allied-Market-Research.html.
[22] Carlos E. Rubio-Medrano, Shaishavkumar Jogani, Maria Leitner, Ziming Zhao, and Gail-Joon Ahn. 2019. Effectively Enforcing Authorization Constraints for Emerging Space-Sensitive Technologies. *Proc. of the 24th ACM Symp. on Access Control Models and Technologies*, 195–206.
[23] Jiacheng Shang, Si Chen, Jie Wu, and Shu Yin. 2022. ARSpy: Breaking Location-Based Multi-Player Augmented Reality Application for User Location Tracking. *IEEE Transactions on Mobile Computing* 21, 2 (2022), 433–447.
[24] Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, and Mika Ylianttila. 2021. A Survey on Mobile Augmented Reality With 5G Mobile Edge Computing: Architectures, Applications, and Technical Aspects. *IEEE Communications Surveys Tutorials* 23, 2 (2021), 1160–1192.
[25] Pasquale Stirparo, Igor Nai Fovino, Marco Taddeo, and Ioannis Kounelis. 2013. In-memory credentials robbery on android phones. , 88-93 pages. https://doi.org/10.1109/WorldCIS.2013.6751023
[26] Ailie K.Y. Tang. 2017. Key factors in the triumph of Pokémon GO. https://www.sciencedirect.com/science/article/pii/S0007681317300940. *Business Horizons* 60, 5 (2017), 725–728.
[27] Time. 2016. Pokémon Go Players Anger 9/11 Memorial Visitors: 'It's a Hallowed Place'. https://time.com/4403516/pokemon-go-911-memorial-holocaust-museum/.
[28] Fatih Turkmen, Jerry den Hartog, Silvio Ranise, and Nicola Zannone. 2017. Formal analysis of XACML policies using SMT. *Computers & Security* 66 (2017), 185–203.
[29] Yahoo! 2022. CEOS of snap, XTMIF, OGGFF and MQ leading disruptive innovation and revenue growth in fintech, augmented reality and plant-based foods. https://finance.yahoo.com/news/ceos-snap-xtmif-oggff-mq-130400034.html.
[30] Xueling Zhang, Rocky Slavin, Xiaoyin Wang, and Jianwei Niu. 2019. Privacy Assurance for Android Augmented Reality Apps. *2019 IEEE 24th Pacific Rim Int. Symposium on Dependable Computing (PRDC)*, 114–1141.