Poster: Preventing Spatial and Privacy Attacks in Mobile Augmented Reality Technologies

Luis M. Claramunt
and Larissa Pokam Epse
Arizona State University
Tempe, Arizona, USA
{lclaramu, lpokamep}@asu.edu

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

Jaejong Baek
and Gail-Joon Ahn
Arizona State University
Tempe, Arizona, USA
{jbaek7, gahn}@asu.edu

2021 IEEE European Symposium on Security and Privacy (EuroS&P) | 978-1-6654-1491-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/EUROSP51992.2021.00056

Abstract—**The growing popularity of applications featuring Mobile Augmented Reality (MAR) raises serious concerns regarding the use of such a game-changing technology inside *sensitive* physical spaces, e.g., memorials, hospitals, museums, etc., such that the safety and privacy of users is preserved. To address such concerns, we present our ongoing work for mediating the way MAR *Content*, e.g., digital objects rendered on top of a video stream, is generated, distributed, and consumed by applications. We introduce a theoretical model, a supporting framework, as well as `SpaceMediator`, a *proof-of-concept* application implementing our approach.**

1. Introduction

Mobile Augmented Reality (MAR) is quickly becoming a major technological trend. Recently, several futuristic applications combining MAR along with *Online Social Networks* (OSNs), hereafter referred as *Space-Sensitive Applications* (S-Apps), have been downloaded millions of times, encouraging major companies in the industry to actively explore and invest in the technology. Unfortunately, new security challenges have emerged as well. First, there is a lack of control over the physical locations where MAR *Content*, e.g., digital objects on top of a video screen, can be displayed. This controversy became noticeable with the successful release of Pokémon GO in 2016, as it was considered disrespectful to use such an S-App in places such as the 9/11 Memorial in New York City [1]. Second, the safety of users interacting with the same S-App at the same physical location has also been affected. For example, crowds of players were noticed throughout the world alongside playing Pokémon GO, which resulted in incidents such as fights and robberies [2].

In this paper, we describe our ongoing effort for mediating the generation, distribution, and consumption of MAR Content among simultaneous users of S-Apps, such that the aforementioned issues can be better prevented. We start by describing the attacks that are facilitated by S-Apps (Sec. 2), and then present a preliminary case study on several S-Apps available in the market (Sec. 3). Then, we provide a description of our approach, which includes a theoretical *Content Mediation* (CM) model, a run-time supporting framework, as well as `SpaceMediator`, a *proof-of-concept* S-App implementation (Sec. 4). Finally, we revise future work and conclude the paper in Sec. 5.

Dr. Gail-Joon Ahn is also affiliated with Samsung Research.

2. Security and Safety Issues on S-Apps

Space Invasion. In the context of S-Apps, a *Space Owner* is an individual or group of individuals with a legitimate right to decide on the MAR Content that can be *released*, e.g, generated, distributed, or consumed, within a certain sensitive physical space[1]. Therefore, an Space Invasion Attack may occur when a given S-App releases MAR Content to users in a physical space without previous explicit authorization from the corresponding Space Owner [3]. For example, Pokémon GO was found to be inappropriate inside a WWII memorial [4].

Space Affectation. Similarly, the unrestricted release of *dangerous* MAR Content between users of S-Apps may result in unwanted affectations to their overall MAR experience, and/or their personal safety [5]. As an example, malicious users may want to place MAR Content to lure other users into certain physical spaces, ultimately resulting in robberies and other incidents [2].

Privacy Leak. Finally, alongside with other types of Android applications reported in the literature, sensitive information about one user may be disclosed to other users without explicit consent, or users may unwillingly share MAR Content with other users or third parties. That may include personal data collected directly by S-Apps, content generated as a part of MAR functionality, e.g., private content distributed to other users, or auxiliary data that is relevant in the context of MAR, e.g., GPS data.

3. A Preliminary Case Study on S-Apps

Methodology. As an initial step for our study, we located relevant S-Apps on Google Play by running a search using the keywords `augmented reality`, `mobile`, and `multi-user`. The resulting S-Apps were installed on a Samsung S9 device running Android 10. Next, for each S-App, we procured any usage information available online, and set up accounts for two experimental users. For the Space Invasion attack, we attempted to use each of the surveyed S-Apps inside a series of physical spaces. If such a procedure was conducted successfully without any constraints, the attack was then deemed as possible. For the Space Affectation attack, for each S-App we used the first user account to generate some MAR content, and

[1] The existence of a rightful *ownership* for a given space is assumed beforehand and therefore is out of the scope of this work.

© 2021, Larissa Pokam Epse. Under license to IEEE.
DOI 10.1109/EuroSP51992.2021.00056

TABLE 1. A PRELIMINARY CASE STUDY ON S-APPS OBTAINED FROM GOOGLE PLAY.

S-App	S. Invasion	S. Affectation	Privacy	Downloads	Rating	Google Play Id
Pokémon GO	√	-	-	100M	4.1	com.nianticlabs.pokemongo
Jurassic World Live	√	√	-	10M	4.3	com.ludia.jw2
The Walking Dead	√	-	-	5M	4.2	com.nextgames.android.ourworld
Snaappy	√	√	√	1M	4.2	com.snaappy
Color Quest AR	√	-	-	1M	3.6	com.stayhealthy.colorquest
AR Real Drive	√	-	-	500K	4.3	com.enteriosoft.arealdriving
Just a Line	√	-	-	500K	3.5	com.arexperiments.justaline
Weapon AR Simulator	√	√	-	100K	3.9	com.odvgroup.weaponarcamerathreedsimulator
WallaMe	√	√	√	100K	3.6	com.wallame
RealTag	√	√	-	100K	3.6	com.arfps.android
vTime XR	√	√	√	100K	3.5	net.vtime.cardboard
Real Note	√	√	√	50K	3.4	one.realnote.app
AnibeaR	√	√	√	10K	3.7	com.anipen.anibearar
MARK	√	√	-	1K	3.8	com.psst.app

later switched to the other user account and attempted to access the same content again. If such access was possible, e.g, visualizing a MAR digital object, the attack was deemed as possible. Finally, for the Privacy Leak attack, we looked for how sensible data, e.g., names and location, was collected from the first user account and distributed by the S-Apps to the second user account. If such release was possible without requiring any previous authorization, the attack was deemed as possible.

Results. As shown in Table 1, all surveyed S-Apps were found to be vulnerable to the Space Invasion attack, as they can be used in any physical space without any noticeable restrictions. The social media apps (e.g., WallaMe, Real Note, Snaappy, AnibeaR, and MARK) were vulnerable to Space Affectation, as there was no control of where MAR content could be placed or shared, and it could even be considered intrusive, which could potentially disrupt the users' experience. As an example, one of the surveyed S-Apps gives users the ability to save public messages using MAR digital objects on a physical location. Since there is no regulation over these messages, based on the usage description such a content could be even considered digital graffiti. Finally, some applications exhibited Privacy Leaks within them. For example, without a previous warning one of the surveyed S-App showed the user's current location.

4. Our Approach: Policy-Governed S-Apps

To prevent the attacks discussed on Sec. 2, Space Owners and Users are allowed to specify their preferences with respect to the generation, distribution, and consumption of MAR Content inside physical spaces, resulting in so-called *Policy-Governed* S-Apps, which observe such preferences to mediate the release of MAR Content at run-time. An example featuring Fig. 1 goes as follows:

(1) Policy Creation: User$_1$ starts by creating a policy limiting the MAR Content that will be released by S-Apps to anyone who enters the *protected* sensitive space. Policies are in turn specified using a large variety of security-relevant information modeled as *Attributes* [3], e.g., S-App name (id), user age, time frame, type of content, Android API level, etc. For example, foxes may be released only to users over 18 years of age.

(2) Protected Space Entry: When User$_2$ reaches a protected space, a policy evaluation request is sent to our supporting framework, to determine how the S-App should operate, e.g., if MAR Content should be released or not. Such requests are automatically generated, and they take into account any relevant information that could have been specified in a policy, e.g., values for the attributes listed in the policy. Outside of these zones S-Apps are unregulated.

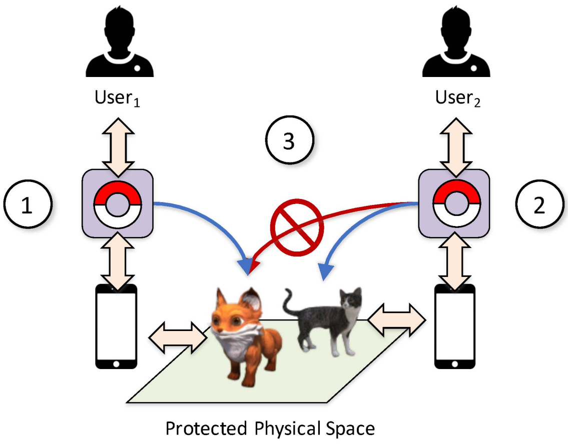


Figure 1. Policy-Governed S-Apps for Mediating MAR Content.

(3) MAR Content Mediation: After processing the request evaluation, a decision is sent back to the S-App, which will then enforce it accordingly. This way, User$_2$ will only be granted authorized functionality. For example, following Fig. 1, if User$_2$ is 16 years old then the S-App would not be allowed to distribute MAR Content such as foxes, but cats may be granted instead.

4.1. A Theoretical Content Mediation Model

Our approach for Policy-Governed S-Apps relies on a precise description of how *Entities*: Users, Space Owners, Protected Spaces, and Providers of S-Apps, e.g., companies and developers, interact with each other for releasing MAR Content. To this end, we are developing a theoretical *Content Mediation* (CM) model, graphically shown in Fig. 2, which is formulated in First-Order Predicate Logic and defines under what circumstances the attacks described in Sec. 2 may take place, based on the following:

Functionalities. Initially, our CM model defines a series of *Functionalities* that are relevant in the context of S-Apps. For instance, the predicate `Generates(U, C, P)` denotes the case when a User U generates MAR Content C and uploads it to the infrastructure of Provider

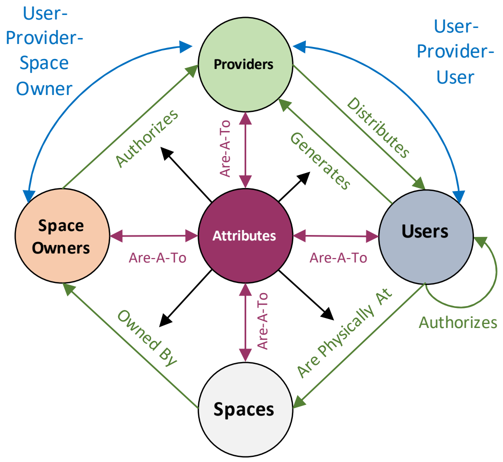


Figure 2. A Content Mediation Model for S-Apps.

P. Also, the predicate IsPhysicallyAt(U, S) denotes the case when a User U is located inside Space S.

Modes of Interaction. Also, our CM Model defines the way Entities and Functionalities are related to each other in the context of S-Apps. As an example, the predicate User-Provider-User (U$_1$, C, P, U$_2$, S) denotes an interaction in which a User U_1 generates MAR Content labeled as C, which is then uploaded to a Provider P, and later distributed to another User labeled as U_2 in the context of a Protected Space S. More specifically:

$$\frac{\texttt{Generates}(\texttt{U}_1,\ \texttt{C},\ \texttt{P}),\ \texttt{Distributes}(\texttt{P},\ \texttt{C},\ \texttt{U}_2),\ \texttt{IsPhysicallyAt}(\texttt{U}_2,\ \texttt{S}),\ \texttt{RendersAt}(\texttt{C},\ \texttt{P},\ \texttt{S})}{\textbf{User-Provider-User}(\textbf{U}_1,\ \textbf{C},\ \textbf{P},\ \textbf{U}_2,\ \textbf{S})}$$

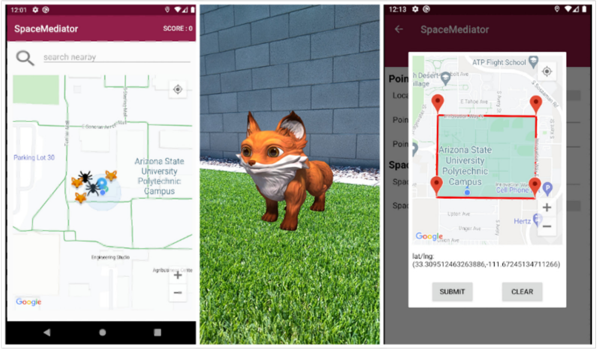
Authorization. In our CM model, policies restricting MAR Content are defined by means of a series of predicates relating Entities, Spaces, and Attributes. For instance, the predicate Authorizes(U$_1$,U$_2$,C,S,P) denotes the case when User U_1 has authorized the distribution of MAR Content C to User U_2, which is carried out by Provider P under the context of the Space S.

Attacks. Finally, our CM model defines attacks as modes of interaction between entities for whom authorization has not been granted. For instance, the predicate Space-Affectation(U$_2$, C, U$_1$, P, S, SO), denotes the case when MAR Content C, generated by User U_1, is distributed to User U_1 in an unauthorized way by Provider P over Space S, which in turn is managed by Space Owner SO. More specifically:

$$\frac{\texttt{User-Provider-User}(\texttt{U}_1,\ \texttt{C},\ \texttt{P},\ \texttt{U}_2,\ \texttt{S}),\ \texttt{Authorizes}(\texttt{SO},\texttt{U}_1,\texttt{C},\texttt{S},\texttt{P}),\ \texttt{Authorizes}(\texttt{SO},\texttt{U}_2,\texttt{C},\texttt{S},\texttt{P}),\ \texttt{!Authorizes}(\texttt{U}_1,\texttt{U}_2,\texttt{C},\texttt{S},\texttt{P})}{\textbf{Space-Affectation}(\textbf{U}_2,\ \textbf{C},\ \textbf{U}_1,\ \textbf{P},\ \textbf{S},\ \textbf{SO})}$$

4.2. Implementing a Proof-of-Concept S-App

We are developing a *proof-of-concept* S-App called SpaceMediator, shown in Fig. 3, which is inspired on Pokémon GO and other gaming S-Apps in which users are encouraged to explore their surroundings, encountering MAR objects to interact with and capture.


SpaceMediator
SCORE : 0
search nearby
Arizona State University Polytechnic Campus
Google
SpaceMediator
Arizona State University Polytechnic Campus
Google
SUBMIT
CLEAR

lat/lng: (33.309512463263886,-111.67245134711266)

Figure 3. SpaceMediator: A *Proof-of-Concept* S-App.

SpaceMediator allows for Space Owners and Users to easily create a content mediation policy for a specific location. Once a policy has been created, policy evaluation requests are issued for every user that enters the specified zone. MAR objects are generated with the Google AR-Core API. Policies and requests are written in the XACML 3.0 language by means of the AT&T's OASIS API.

5. Conclusion and Future Work

Despite their increasing popularity, S-Apps facilitate the deployment of attacks that may harm the MAR experience of users and may even affect their personal safety and well-being. To alleviate this, we are actively working towards an approach for Policy-Governed S-Apps, which can restrict the release of MAR Content depending on user-specified mediation policies. Our next steps include a comprehensive user study featuring our SpaceMediator S-App, a set of template policies, and a series of realistic scenarios that can assist us to better elucidate the advantages and limitations of our approach.

Acknowledgments

This work is partially supported by a grant from the National Science Foundation (NSF-SFS-1129561), a grant from the Center for Cybersecurity and Digital Forensics at Arizona State University, and by a startup funds grant from Texas A&M University – Corpus Christi.

References

[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] T. Mullen. (2016) Hundreds of pokemon go incidents logged by police. [Online]. Available: https://www.bbc.com/news/uk-england-37183161

[3] C. E. Rubio-Medrano, S. Jogani, M. Leitner, Z. Zhao, and G.-J. Ahn, "Effectively enforcing authorization constraints for emerging space-sensitive technologies," in *Proc. of the 24th ACM Symposium on Access Control Models and Technologies*, ser. SACMAT '19. New York, NY, USA: ACM, 2019, p. 195–206.

[4] (2016) Germany's auschwitz-birkenau museum says no pokemon go. [Online]. Available: https://www.dailysabah.com/europe/2016/07/14/germanys-auschwitz-birkenau-museum-says-no-pokemon-go

[5] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner, "Towards security and privacy for multi-user augmented reality: Foundations with end users," in *IEEE Symp. on Sec. and Priv. (S&P)*, 2018, pp. 392–408.