Towards Secure and Safe Distribution of Digital Content on Mobile Augmented Reality Applications

Motivation. *Mobile Augmented Reality* (MAR) has been regarded as the next big thing in computing, as the dynamic display of *content*, i.e., digital objects on top of a video stream, greatly increases the perception of users while they actively explore their surroundings, resulting in a large variety of potential applications. Not surprisingly, this has resulted in a lot of companies in industry now being interested and/or actively working on MAR. As an example, a wide range of applications featuring MAR, a.k.a., *MAR apps*, have been developed for different domains: education, military, healthcare, gaming, Smart Cars, etc.

Problem Statement. Whereas the potential of MAR is promising, **still no effective provisions exist for properly mediating the distribution of security-sensitive content between users of MAR apps**, preventing not only unauthorized access from external third parties, e.g., patient information in tele-medicine MAR apps, but also affectations to the users' experience that may result in harm to their personal safety, e.g., displaying incorrect navigation signals for Smart Car MAR apps. In general, solving this problem involves the following challenges: (1) *Content Distribution Modeling.* First, there is a need to unambiguously define how content is generated, stored, and distributed to users, including a representation of how *sensitive* content may be in terms of cyber-security and physical safety; (2) *Specifying User Preferences.* Second, users must be allowed to clearly and easily express their preferences for content distribution, taking into account factors such as the aforementioned sensitivity level, the type of MAR app being used, the application domain, e.g., military or healthcare, the current physical location, etc. (3) *Correct Run-time Enforcement.* Third, such preferences must be stored, retrieved, evaluated, and correctly enforced by MAR apps.

Proposed Approach. To address these concerns, I will develop a **Secure and Safe Software Construction Framework that will allow for MAR apps to correctly follow the users' preferences when distributing content at run-time**. Such a framework will consist of the following: (1) a *Content Representation* (CR) model, which will abstractly define different functionalities provided by MAR apps as well as the content associated with each of them, allowing for the identification of different content categories e.g., regular (non-security sensitive) and private (security-sensitive); (2) a *Content Mediation* (CM) model, which will leverage the aforementioned CR model to regulate under what circumstances content may be distributed; (3) a *Policy Specification and Evaluation Tool* (P-SET), which will assist users on writing and evaluating content distribution policies following the CR and CM models; (4) a *Verification and Validation Tool* (MAR-V&V), which will analyze the source code of MAR apps to correctly enforce the user's preferences and prevent the unauthorized distribution of content originated by erroneous implementations.

Intellectual Merit. The proposed approach will introduce a series of novel methodologies and techniques as follows: The CR and CM models will provide a well-defined, unambiguous description of the entities, functionality, and modes of interaction governing the distribution of content in MAR apps. In addition, the CM model and the P-SET tool will introduce novel techniques to write content distribution policies following the CR model, allowing for users to clearly and effectively express their preferences without requiring an advanced level of expertise. Finally, the P-SET and MAR-V&V tools will introduce new methodologies for verifying the correct enforcement of user preferences, as well as the CR and CM models by analyzing MAR apps regardless of their type, domain, and implementation frameworks and APIs.

Broader Impacts. This research project will have broad societal impacts as follows: (1) the resulting products will heavily contribute to producing better MAR apps, ultimately allowing for users to fully experience such emerging technology in a secure and safe way; (2) the PI will focus on building a stronger and diverse workforce pipeline by recruiting women, minorities, and other underrepresented groups, providing them with a unique opportunity to acquire a strong background in cyber-security, software V&V, and MAR technologies; (3) the topics of this project will be integrated into existing and new courses, e.g., a graduate research seminar, and to undergraduate, high school, and PK-12 competitions such as the South Texas Hackathon sponsored by the Computing Alliance of Hispanic-Serving Institutions (CAHSI).