Security for Augmented Reality Applications

Augmented reality (AR) applications are becoming increasingly pervasive in our modern world. This innovation addresses the critical challenges in the management of AR security, including input/output management, the resolution of conflicts between content and the real world, and the running of concurrent AR applications.

What is the Problem?

In our world of rapidly advancing technology, augmented reality (AR) systems are becoming more and more commonplace. From tech innovations as high-end as the Apple Vision Pro to the accessible experience of Pokémon Go, AR is transforming the way we interact with both the physical and the digital world. However, this rapid advancement brings with it a host of security and privacy challenges.

In considering the security challenges, both the input and output to the device must be considered. On the input side, AR applications operate with unrestricted access to sensors, which means they can potentially see sensitive information. As the range of AR applications expands, so does the risk of malicious software. On the output side, an application's interference with a user's perception can lead to a host of issues. Applications can block important details in real life, conflict with each other's visuals, or disrupt the user physiologically such as with sudden flashing lights. Additionally, in multi-person AR scenarios, other users present potential risks such as unwanted flooding of a user's display with objects from another user, or vandalism of created artwork by other passing users.

Technology ID

BDP 7692

Category

Software/Enterprise Software
Software/Security
Selection of Available Technologies

Authors

Tadayoshi Kohno

Learn more

These challenges underscore the need for robust, multi-faceted security solutions in AR systems. It is important that these issues are considered and resolved, to provide frameworks for the further development of AR applications.

What is the Solution?

The suite of technologies available for licensing offers a comprehensive solution to the security and privacy challenges in AR systems. These technologies, developed over several years and detailed in various research papers and patents, address the critical issues in AR output management, content sharing, and concurrent application operation.

One of the foundational innovations of this work is the proposition that AR objects are to be managed at the operating system level, instead of directly by applications. This change in paradigm allows visuals from multiple applications to be managed together and opens the door for the rest of the work.

This technology handles conflicts between AR applications, or with the real world, through the use of an output policy module enforcing policy-based constraints on application outputs. These can be based on real-world policies; for instance, a guideline that real-world trees should not block road signs is adapted that virtual objects should not block road signs. Similarly, an input module determines whether applications requesting sensor access should be allowed to have the input information. The technology controls the policies for these input and output sources, aiming to combat the wide range of security issues potentially present in the evolving AR world.

What is the Competitive Advantage?

This platform for AR security offers several advantages:

- Comprehensive Outlook: The technologies aim at several important areas of AR security and privacy concerns, ranging from potentially sensitive input data to the handling of multi-user AR experiences.

- Proven Effectiveness: Developed over years with support from academia and industry, this is not only a proposed design for a system, but one that has been prototyped and evaluated.

- Market Need: With the continual development of AR integration such as the work done by Microsoft, Meta, and BMW, this technology is essential in combating the issues of AR security before the applications become even more mainstream.

Patent Information:

US20220012923

US20170162177

US20200364915A1

References

1. Kiron Lebeck, Tadayoshi Kohno, Franziska Roesner(2016-02-23) , https://dl.acm.org/doi/10.1145/2873587.2873595, https://dl.acm.org/doi/proceedings/10.1145/2873587, 45–50
2. Kimberly Ruth, Tadayoshi Kohno, Franziska Roesner(2019) , https://www.usenix.org/conference/usenixsecurity19/presentation/ruth, https://www.usenix.org/conference/usenixsecurity19
3. Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, Franziska Roesner(2017-05) , http://ieeexplore.ieee.org/document/7958585/, https://ieeexplore.ieee.org/xpl/conhome/7957740/proceeding, 320–337