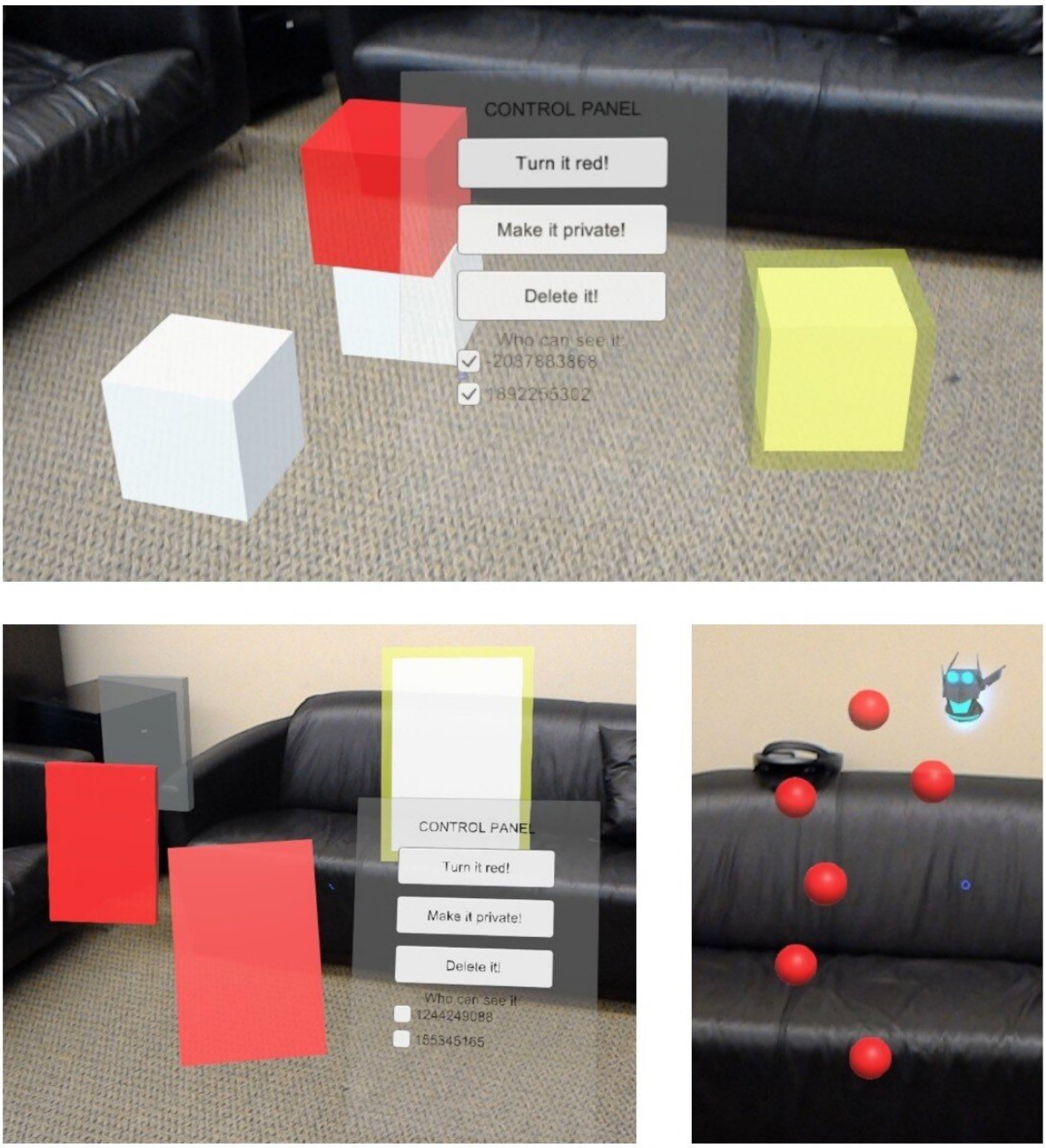
New tools to minimize risks in shared, augmented-reality environments

August 20 2019, by Sarah Mcquate



The team tested ShareAR with three case study apps: Cubist Art (top panel), which lets users create and share virtual artwork with each other; Doc Edit (bottom left panel), which lets users create virtual notes or lists they can share or keep private; and Paintball (bottom right panel), which lets users play paintball with virtual paint. In the Doc Edit app, the semi-transparent gray box in the top left corner represents a "ghost object," or a document that another user wishes to

remain private. Credit: Ruth et al./USENIX Security Symposium

A few summers ago throngs of people began using the Pokemon Go app, the first mass-market augmented reality game, to collect virtual creatures hiding in the physical world.

For now, AR remains mostly a solo activity, but soon people might be using the technology for a variety of group activities, such as playing multi-user games or collaborating on work or creative projects. But how can developers guard against bad actors who try to hijack these experiences, and prevent privacy breaches in environments that span digital and physical space?

University of Washington security researchers have developed ShareAR, a toolkit that lets app developers build in collaborative and interactive features without sacrificing their users' privacy and security. The researchers presented their findings Aug. 14 at the USENIX Security Symposium in Santa Clara, California.

"A key role for computer security and privacy research is to anticipate and address future risks in emerging technologies," said co-author Franziska Roesner, an assistant professor in the Paul G. Allen School of Computer Science & Engineering. "It is becoming clear that multi-user AR has a lot of potential, but there has not been a systematic approach to addressing the possible security and privacy issues that will arise."

Sharing virtual objects in AR is in some ways like sharing files on a cloud-based platform like Google Drive—but there's a big difference.

"AR content isn't confined to a screen like a Google Doc is. It's embedded into the physical world you see around you," said first author

Kimberly Ruth, a UW undergraduate student in the Allen School. "That means there are security and privacy considerations that are unique to AR."

For example, people could potentially add virtual inappropriate images to physical public parks, scrawl virtual offensive messages on places of worship or even place a virtual "kick me" sign on an unsuspecting user's back.

"We wanted to think about how the technology should respond when a person tries to harass or spy on others, or tries to steal or vandalize other users' AR content," Ruth said. "But we also don't want to shut down the positive aspects of being able to share content using AR technologies, and we don't want to force developers to choose between functionality and security."

To address these concerns, the team created a prototype toolkit, ShareAR, for the Microsoft HoloLens. ShareAR helps applications create, share and keep track of objects that users share with each other.

Another potential issue with multi-user AR is that developers need a way to signal the physical location of someone's private virtual content to keep other users from accidentally standing in between that person and their work—like standing between someone and the TV. So the team developed "ghost objects" for ShareAR.

"A ghost object serves as a placeholder for another virtual object. It has the same physical location and rough 3-D bulk as the object it stands in for, but it doesn't show any of the sensitive information that the original object contains," Ruth said. "The benefit of this approach over putting up a virtual wall is that, if I'm interacting with a virtual private messaging window, another person in the room can't sneak up behind me and peer over my shoulder to see what I'm typing—they always see the same

placeholder from any angle."

The team tested ShareAR with three case study apps. Creating objects and changing permission settings within the apps were the most computationally expensive actions. But, even when the researchers tried to stress out the system with large numbers of users and shared objects, ShareAR took no longer than 5 milliseconds to complete a task. In most cases, it took less than 1 millisecond.

Developers can now download ShareAR to use for their own HoloLens apps.

"We'll be very interested in hearing feedback from developers on what's working well for them and what they'd like to see improved," Ruth said. "We believe that engaging with technology builders while AR is still in development is the key to tackling these security and privacy challenges before they become widespread."

Provided by University of Washington