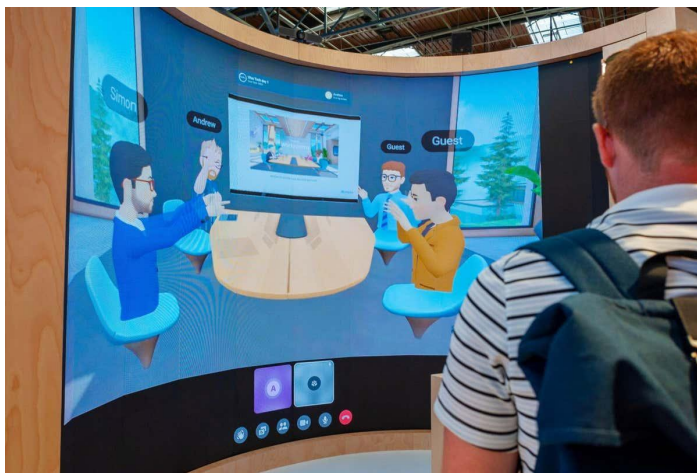


AI can steal passwords in virtual reality from avatar hand motions

Artificial intelligence can work out what someone is privately typing in VR meetings in Meta Horizon Workrooms by looking at the way their avatar's hands move

By [Jeremy Hsu](#) on November 14, 2023



A virtual meeting in the Meta Horizon Workrooms. Directphoto Collection/Alamy

Someone typing on a physical keyboard while attending a [virtual reality](#) meeting could end up leaking passwords and other sensitive information to an attacker who uses [artificial intelligence](#) to interpret the avatar's subtle hand movements.

Researchers trained AIs to analyse the hand movements of virtual avatars in Meta Horizon Workrooms, a virtual office platform provided by Meta. The AIs then used the hand movements to reconstruct the keystrokes typed by the avatar's user over the course of brief typing sessions.

"You don't even need to know the person," says [Haitao Zheng](#) at the University of Chicago. "As long as you can get into the same VR room with them, they're done."

Zheng and her colleagues demonstrated several keyboard inference attacks in [virtual reality](#), including some that accessed data from the target person's [VR headset](#). But the simplest method only requires the attacker to enter the same virtual space as the target and visually record the hand motions of the target's avatar.

Because VR headset sensors cannot yet perfectly track finger motions, any physical keyboard typing ends up being interpreted as more subtle avatar hand motions. So the researchers trained separate AI models to recognise keystroke motions, identify individual fingertips that are pressing a key and finally to predict the keys being typed, says [Zhuolin Yang](#) at the University of Chicago, who led the project. A paper describing this work has been accepted by the [USENIX Security 2024 conference](#).

The AI-powered attack recognised between 86 and 98 per cent of typed keys for 13 out of 15 people who participated in a virtual reality experiment. But noisier avatar motion data made it more difficult for the AIs to detect keystrokes for the remaining two people.

The fact that this attack worked accurately on multiple users with different keyboard typing patterns is “particularly alarming”, says [Amro Awad](#) at North Carolina State University. But he said the demonstration of the vulnerability “will help VR software vendors to develop privacy-preserving policies”.

The researchers have already begun experimenting with adding some noise to obscure the VR hand motion data to foil this AI-powered attack. Meta did not respond to a request for comment.