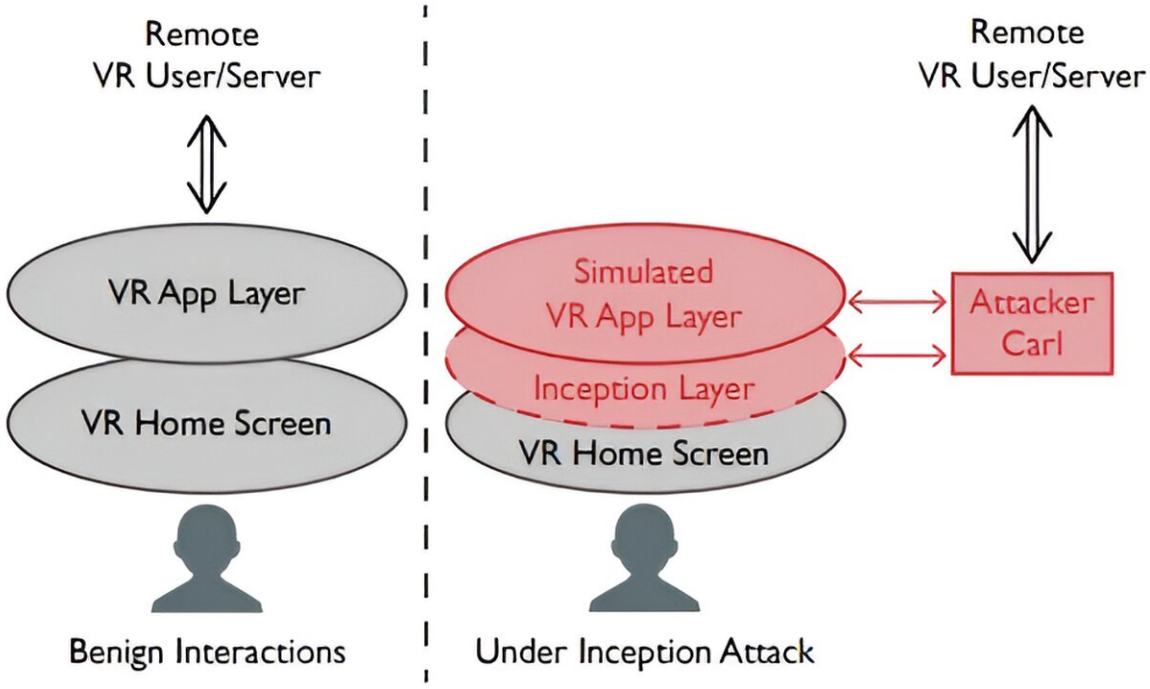
Vulnerability in virtual reality systems identified

March 25 2024, by Bob Yirka



Inception Attacks: A user thinks they are interacting directly with a VR app launched from the VR home screen, when they are in fact running a simulated VR app inside the attacker's inception layer. Credit: *arXiv* (2024). DOI: 10.48550/arxiv.2403.05721

A team of computer scientists at the University of Chicago has uncovered a potential vulnerability in virtual reality systems—one that could allow a hacker to insert what the team describes as an "inception layer" between a user's VR Home Screen and their VR User/Server. The team has posted a paper describing their work and their findings on the *arXiv* preprint server.

Virtual reality systems allow users to interact in a virtual world—one where virtually anything imaginable is possible. In this new effort, the research team imagined a scenario where hackers could add an app to a user's VR headset that tricks users into behaving in ways that could reveal sensitive information to the hackers.

The idea behind the app is that it could add a layer between the user and the virtual world the user normally sees when using their VR device. They call it an inception layer, after the movie where a character played by Leonardo DiCaprio has an altered layer of reality downloaded into his brain.

In this case, such a layer, the researchers suggest, could allow hackers to record information, such as a passcode entered into a virtual ATM. It could also intercept and alter information, such as cash amounts designated for a purchase—and routing the difference to the hacker's bank account.

It could even add imagery to the VR world, such as characters representing friends or family and use such a ruse to gain trust or access to secrets. In short, it could monitor or alter gestures, voice emanations, browsing activity and social or business interactions.

Such an app, the research team notes, could be downloaded on a user's

VR device if they managed to hack their WiFi network, or gain physical access. And once installed, it could run without notice from the user. The researchers tested this last possibility by enlisting the assistance of 28 volunteers who played a game using a demonstration VR headset.

The researchers then downloaded an app onto the devices, simulating a hacking, and then asked the volunteers if they had noticed anything—the download and activation process caused a tiny bit of a flickering. Only 10 of the volunteers noticed and just one of them questioned whether something nefarious was occurring.

The research team notified Meta, makers of the Meta Quest VR system that was used in the experiment, of their findings, and the company responded by reporting back that they plan to look into the potential vulnerability and fix it if it is confirmed. The researchers also note that such vulnerabilities are likely to exist on other systems and other types of apps that also seek to insert themselves between users and their VR devices.

More information: Zhuolin Yang et al, Inception Attacks: Immersive Hijacking in Virtual Reality Systems, *arXiv* (2024). DOI: 10.48550/arxiv.2403.05721