Hacking the metaverse: Cybersecurity researchers help protect people in immersive virtual reality

November 9 2022

Credit: Pixabay/CC0 Public Domain

About 2 million people connected to virtual reality headsets every month in 2020. Virtual reality, or VR, industry revenues are projected to grow from $12 billion to $100 billion in the next five years. In the race to develop the most popular VR applications and capture the most

consumer demand, VR software developers and companies are not always implementing measures to protect consumers from getting hacked. Oftentimes the products are released while still under development.

LSU Cybersecurity Professor Abe Baggili is one of the first people in the world to study the security of immersive virtual reality, or X-reality, systems, and to provide solutions to this fast-paced industry to protect people who use these new products.

"Everyone needs to be aware that all technology has security risks. Once someone can access your device, they can potentially steal your money by accessing your banking and credit card accounts and wreak havoc on your life," said Baggili, who is a professor in the LSU Department of Computer Science and the Center for Computation & Technology.

His new research is published in *Computers & Security*.

Baggili and his cybersecurity students, including lead author Martin Vondráček who is now a security researcher and a Ph.D. student at Brno University of Technology in the Czech Republic, tested a popular social and entertainment XR application primarily used by people to watch movies with others in a virtual environment to see if they could hack into users' headsets and computers.

The researchers discovered they could, and were able to take over a user's VR headset, look at their screen, turn on their microphone and install a virus on their computer all without them knowing it. When another user entered the virtual room and interacted with the unknowingly infected user, they became infected too similar to how viruses spread between people in reality.

In addition, the researchers were able to enter the virtual room using a

different and undetected device and act like a virtual invisible peeping Tom.

"No one would expect an invisible intruder in their real living room, watching their activities and every move. This intrusion can disturb people's privacy on a very personal level," Baggili said.

Children and young people are gravitating towards and using many of these virtual reality applications and headsets, which makes ensuring safety and security measures even more important.

"VR and XR devices are collecting a lot of personal information such as the structure of the physical room you're in as well as your eye, hand and body movements. This information can be used to cause you and your family physical, emotional and financial harm," he said.

By hacking into a VR headset and camera, the researchers were able to disorient users, delete physical boundaries to make them walk into walls or fall down staircases in reality.

Fortunately, the company that developed the VR application Baggili and his students tested in this paper accepted all of the recommendations the researchers provided in the responsible disclosure. Developers and scientists can now use the tools the researchers developed to make secure VR software.

"The vulnerabilities that we discovered could have been prevented. As a part of our research, we implemented several analytical and attacking tools, example exploits and vulnerability signatures. We opted to publish them as free and open-source software to improve the state of the art of vulnerability detection and prevention in VR," Vondráček said.

In addition, virtual reality applications are being used in education,

healthcare, critical infrastructure and military defense.

"This research is critical to identify the security weaknesses in popular XR applications. We need legislators and organizations to know the potential harm it can cause and require the companies developing these new technologies to find the right balance between security, privacy and safety, before the massive adoption," said Kavya Pearlman, founder and information security researcher of global non-profit Standard Developing Organization, XR Safety Initiative, or XRSI.

How to join the metaverse safely

"Be diligent and understand new technology has both positive and negative consequences. Veer on the side of not always trusting it and use it like you're a scientist: experiment with things, be very critical of the technology you're using and try to understand what they're doing with your data," Baggili said.

Unfortunately, there are not many platforms in which users can educate themselves about these new technologies and most of the information people see comes from the companies selling VR products, which naturally do not draw attention to potential privacy and security risks.

"We react to this by bringing our research to public attention in global media. Our hope is that it will help raise awareness of VR, its strengths and also its associated dangers," Baggili said.

More information: M. Vondrek et al, Rise of the Metaverse's Immersive Virtual Reality Malware and the Man-in-the-Room Attack & Defenses, *Computers & Security* (2022). DOI: 10.1016/j.cose.2022.102923