Researchers aim to protect cyber space in virtual reality environments

August 4, 2021
in CERI, Cybersecurity, Electrical Engineering & Computer Science, Faculty, Research, Research and Creative Works
by Janese Heavin

Virtual reality (VR) is becoming a popular replacement for in-person gatherings. Today, VR is used to provide remote classroom experiences, create realistic workplace settings and simulate training scenarios in realistic environments. But as the technology becomes more mainstream, the potential for malicious attacks on VR systems is growing.

Now, a Mizzou Engineering team is beginning to study possible threats and develop ways to combat them.
“We are excited that this is the first project — at least to the best of our knowledge — that actually deals with the cyber security issue around networked virtual reality,” said Khaza Anuarul Hoque, an assistant professor of electrical engineering and computer science and director of the Dependable Cyber-Physical Systems (DCPS) Laboratory.

Hoque received funding from the National Science Foundation to develop and test threats against social virtual reality environments. Hoque is the principal investigator (PI) working with co-PI Prasad Calyam, who is Gilliam Professor of Cyber Security and director of the Cyber Education, Research and Infrastructure Center (Mizzou CERI).

Identifying potential problems

The researchers will investigate types of attacks — including some evolving attacks — that could threaten the safety, security and privacy of those participating in VR groups.

VR environments are already known to cause physical illness in some individuals. For instance, a slow network or glitch that alters the visual surroundings can make someone nauseous. Hoque and his team are considering the possibility of someone trying to cause that cyber sickness intentionally.

“We know VR might have associated cyber sickness, but in this proposal, we’re studying how might an attacker induce attacks or faults that lead to cyber sickness,” Hoque said.

In an example scenario, a hacker could access the network and take on an administrative role to create system disruptions. Or, cloud-based VR could create a security gap that allows someone to access an otherwise secure network.

Hoque, Calyam and their students will initially develop theories around these possibilities. From these so-called threat models, they’ll build a knowledge base that will provide guidance to those using VR environments on how to design more secure systems or detect red flags.

The team will also test their theories and potential defense systems in realistic settings. At the end of the three-year grant, Hoque expects to have open-source code or software that others can use to better protect social virtual reality systems. It will incorporate machine learning, allowing the system to remember security issues and identify new types of attacks that come into play.
Leaders in social virtual reality

The grant builds on Calyam’s previous work on vSocial around using social virtual reality to connect students with autism spectrum disorder.

“As we built the vSocial system, we saw the network is prone to a lot of cyber-attacks, attacks that can not only disrupt the experience but can disconnect sessions and even cause safety issues,” Calyam said. “When we saw that there are bigger implications than just performance issues, we set out to formally study what causes problems in virtual environments and how cyber-attacks might contribute to those issues. This is a great second grant in this area to show we are leading the efforts in creating high-performance VR systems that can be networked and secured.”

Calyam anticipates the project leading to additional studies using a new NSF-funded CAVE. The CAVE is a visualization facility that provides users with immersive virtual environments that don’t require VR goggles. Right now, the CAVE, which is located in the CERI Center, is not connected to a network, but Calyam envisions testing that in the future.

“This opens up a lot of opportunities to study VR and its applicability to various domains,” he said. “Both projects will have synergistic benefits and help us advance the state of the art in the social virtual reality space.”

Study cutting-edge technologies with leading experts in the field. Learn more about electrical engineering and computer science at Mizzou Engineering!