idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

CISPA Helmholtz Center for Information Security
Felix Koltermann
12/13/2024
http://idw-online.de/en/news844748

Research results
Information technology
transregional, national

Study reveals vulnerability of metaverse platforms to cyber attacks

Having access to virtual worlds from your home computer via your web browser and being able to interact with others in a secure and private manner: that is the promise of metaverse platforms. CISPA researcher Andrea Mengascini conducted a reality check on this promise and discovered significant risks in terms of a lack of privacy and the danger of cyberattacks. He presented his study "The Big Brother's New Playground. Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective" at the renowned Conference on Computer and Communications Security (CCS) in fall 2024.

"I've always been interested in virtual reality and online games," CISPA researcher Andrea Mengascini tell us. When he and his research group leader, CISPA-Faculty Dr. Giancarlo Pellegrino, started investigating the safety of VR headsets, they discovered something interesting: "We realized that it was the same technology used in online games that is also used in metaverses," says Mengascini. He defines a metaverse as a "virtual social space in which people can interact according to rules that in some way mirror the rules of the physical world". While the security of online games has been researched and defenses have been implemented, it was still an open question with regard to metaverse platforms. This is what caught Mengascini's interest.

"Accessing a metaverse has become much easier in recent years," explains Mengascini. "Today, all you need is a normal web browser to enter these rooms. Thanks to the WebXR API interface, it is also possible to use a VR headset." In the Metaverse, people find a kind of digital copy of the real world: there are rooms for private meetings, large or small public events, fun and entertainment. "These platforms run as web-based clients and use JavaScript to manage complex 3D environments, the avatars of users and real-time interactions. All of this is not only crucial for the smooth operation of the Metaverse, but also plays a major role in its security," says the researcher. Mengascini's goal was to find out if there are any security gaps when accessing the Metaverse via web browsers.

The researcher's questions and approach

For his study, Mengascini posed three specific questions: 1. Which entities, such as users and objects, exist in metaverses and which attributes, such as position, appearance, etc., are assigned to them? 2. Where exactly are these elements stored in the memory, and what access can attackers gain to this memory? 3. How can the memory be exploited for attacks? Via a Google search, the CISPA researcher first identified 27 metaverse platforms that use the WebXR API interface. In a next step, he examined three of them in more detail, as they performed best in terms of popularity, user activity, internet traffic and coverage of real events. Mengascini's method was to create so-called memory snapshots, a snapshot of the objects stored in the memory. The snapshots were taken before and after executing a specific action, such as moving an avatar from A to B. Afterwards, an algorithm was used to check if any changes had occurred and if this information could be read from the web browser's memory.

Memories are very easy to access

“The most important finding is that these platforms lack the most basic security mechanisms,” Mengascini explains. “The main issue is that the browsers' memory are too easy to access.” Even a non-expert could access both the source code and the actual objects in the memory with a little practice. “We also found that these platforms have messed up common good coding practices in web application development,” the CISPA researcher continues. “The developers of these platforms have missed the fact that due to a combination of unverified client-side information and excessive disclosure of information to the client, attacks are possible.”

To illustrate what all this means in concrete terms, Mengascini gives an example: “Let's assume there is a CISPA metaverse featuring an exact replica of our building. This would mean that every user's computer would receive all the information about what is currently happening at CISPA: Who is talking to whom in which room, where individual people are physically located and how they are moving, including the exact positions of the walls. Based on this, my computer calculates the virtual environment and ensures, for example, that I cannot listen to conversations in the director's office because of a wall. However, the browser receives information about what is being said in the room. And that is bad. Even if you are not able to listen in with a normal client, this information can be extracted quite easily by attackers. Therefore, it is important to not overshare information.”

Potential attack scenarios

According to Mengascini, this security gap gives rise to a number of possible attack scenarios. The key finding is that attackers can control the avatar and camera position of attackers and victims, as well as their appearance, independently of each other. For example, attackers can move their camera independently from their avatar, explains Mengascini. “This allows attackers to position themselves undetected in the room and to listen in,” Mengascini continues. Another possibility is that attackers can view another user's camera content without them noticing. “It is like attackers putting on the user's VR glasses without them realizing it,” explains the researcher. In order to prevent this, the server would have to retain as much information as possible, which would lead to increased computing power. Exactly this, is according to Mengascini, one of the reasons why the Metaverse platforms rely so heavily on web browsers.

New research questions to take away

In line with common practice in cyber security research, the three platforms were informed of the security gaps and given time to fix them. None of the three platforms has done this yet, which is why their names are still anonymized in the published paper. “From a researcher's perspective, I am obviously concerned that the platforms don't want to focus on security or don't have the manpower to do so,” says Mengascini. But at the same time, I think that we as researchers now have a open research question. Maybe it's time for us to propose security mechanisms to prevent attacks or at least make it harder to carry them out." And he already has ideas as to which protection mechanisms could be implemented. In particular, he plans to use the knowledge gained from the development of online games and transfer it to the Metaverse. However, Mengascini is aware that many approaches also have disadvantages and require extensive testing. A challenge that he wants to take up in the near future.

Original publication:

Mengascini, Andrea; Aurelio, Ryan; Pellegrino, Giancarlo (2024). The Big Brother’s New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User’s Perspective. CISPA. Conference contribution. https://doi.org/10.60882/cispa.27102151.v3

Visualization to the paper "The Big Brother’s New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User’s Perspective"
CISPA