TechXplore

Researchers discover security vulnerabilities in virtual reality headsets

February 10 2022, by Emily Everson Layden

Credit: Pixabay/CC0 Public Domain

Researchers at Rutgers University-New Brunswick have published "Face-Mic," the first work examining how voice command features on virtual reality headsets could lead to major privacy leakages, known as "eavesdropping attacks."

The research shows that hackers could use popular virtual reality (AR/VR) headsets with built in motion sensors to record subtle, speech-associated facial dynamics to steal sensitive information communicated via voice-command, including credit card data and passwords.

Common AR/VR systems on the market include the popular brands Oculus Quest 2, HTC Vive Pro, and PlayStation VR.

Led by Yingying "Jennifer" Chen, associate director of WINLAB and graduate director of Electrical and Computer Engineering at Rutgers University-New Brunswick, the study will be presented at the annual International Conference on Mobile Computing and Networking in March. Other research collaborators include Nitesh Saxena of Texas A&M University and Jian Liu at University of Tennessee at Knoxville.

To demonstrate the existence of security vulnerabilities, Chen and her fellow WINLAB researchers developed an eavesdropping attack targeting AR/VR headsets, known as "Face-Mic."

"Face-Mic is the first work that infers private and sensitive information by leveraging the facial dynamics associated with live human speech while using face-mounted AR/VR devices," said Chen. "Our research demonstrates that Face-Mic can derive the headset wearer's sensitive information with four mainstream AR/VR headsets, including the most popular ones: Oculus Quest and HTC Vive Pro."

The researchers studied three types of vibrations captured by AR/VR headsets' motion sensors, including speech-associated facial movements, bone-borne vibrations and airborne vibrations. Chen noted that bone-borne vibrations in particular are richly encoded with detailed gender, identity and speech information.

"By analyzing the facial dynamics captured with the motion sensors, we found that both cardboard headsets and high-end headsets suffer security vulnerabilities, revealing a user's sensitive speech and speaker information without permission," Chen said.

Although vendors usually have policies regarding utilizing the voice access function in headset microphones, Chen's research found that built-in motion sensors, such as an accelerometer and gyroscope within a VR headset, do not require any permission to access. This security vulnerability can be exploited by malicious actors intent on committing eavesdropping attacks.

Eavesdropping attackers can also derive simple speech content, including digits and words, to infer sensitive information, such as credit card numbers, Social Security numbers, phone numbers, PIN numbers, transactions, birth dates and passwords. Exposing such information could lead to identity theft, credit card fraud and confidential and health care information leakage.

Chen said once a user has been identified by a hacker, an eavesdropping attack can lead to further exposure of user's sensitive information and lifestyle, such as AR/VR travel histories, game/video preferences and shopping preferences. Such tracking compromises users' privacy and can be lucrative for advertising companies.

Oculus Quest, for example, supports voice dictation for entering web addresses, controlling the headset and exploring commercial products. Rutgers' Face-Mic research shows that hackers may leverage these zero-permission sensors to capture sensitive information, leading to severe privacy leakages.

Chen said she hopes these findings will raise awareness in the general public about AR/VR security vulnerabilities and encourage manufacturers to develop safer models.

"Given our findings, manufacturers of VR headsets should consider additional security measures, such as adding ductile materials in the foam replacement cover and the headband, which may attenuate the speech-associated facial vibrations that would be captured by the built-in accelerometer/gyroscope," she said.

Chen and her WINLAB colleagues are now examining how facial vibration information can authenticate users and improve security, and how AR/VR headsets can capture a user's breathing and heart rate to measure well-being and mood states unobtrusively.

More information: Cong Shi et al, Face-Mic, *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking* (2021). DOI: 10.1145/3447993.3483272

Provided by Rutgers University

Citation: Researchers discover security vulnerabilities in virtual reality headsets (2022, February 10) retrieved 20 April 2024 from https://techxplore.com/news/2022-02-vulnerabilities-virtual-reality-headsets.html