

A password of another kind: User identification through the skull

May 12 2016



Computer scientists use the human skull and the sensors on the Google Glass to authenticate users. Credit: Oliver Dietze

Passwords or personal identification number are often not secure, because users do not choose or store them well. With so-called biometric

identifiers such as fingerprints, voice or iris scans, users can be identified more easily and securely. Computer scientists from the University of Saarland and the University of Stuttgart are now introducing the skull as a new biometric identifier which can be used with the eyewear computer Google Glass.

"Eyewear computers such as Google Glass are already being used in companies and universities, for helping with physics experiments and in chemistry labs, documenting medical examinations and assisting pediatricians during operations," says Andreas Bulling from the Cluster of Excellence on "Multimodal Computing and Interaction" at Saarland University. There the 35-year-old computer scientist leads the research group "Perceptual User Interfaces" and researches at the neighboring Max Planck Institute for Informatics. "Not only may the users have no hands free to enter a password, they often share a Google Glass among each other and save sensitive data on the device," explains Bulling.

To protect the eyewear computer and its data in case of theft, and to identify legitimate users and prove their authenticity, Andreas Bulling has developed, along with Youssef Oualil, also from Saarland University, and Stefan Schneegass, from the University of Stuttgart, a new method. The key: The researchers use components the Google Glass already has. Besides the miniature microphone, they use the so-called [bone conduction](#) speaker, which is barely visible and is embedded in the frame near the right ear. Using bone conduction, it transmits sounds to the ear in the same way as special hearing aids do. It directs sound vibrations through the surrounding [skull bone](#) directly to the inner ear.

"Because the skull is individual, the sound signal is changed in a way which is unique for every person. Hence, we can use it as a biometric identifier," Bulling explains. The researchers have the bone conduction speaker play a signal covering a broad frequency spectrum. The signal resulting from the skull is recorded with the Google Glass' built-in

microphone. From this recording, the scientists extract the identification features using a special algorithm and compose them into a kind of digital fingerprint. "This is characteristic for each person, and hence it is stored," Bulling says. If someone wears the eyewear computer afterwards, the process starts automatically. The signal echoes through the skull, and the microphone picks it up. If the current audio fingerprint matches the stored one, the person gets access to the miniature computer. "The main advantage of the method is," Bulling adds, "the recognition of the user could also take place implicitly in the future, for example by sounds the device gives as feedback to the user anyway."

Together with his colleagues, he named the new method "SkullConduct" and tested it on ten people. They were authenticated by "SkullConduct" with an accuracy of 97 percent. "However, we have done these tests in a room with no background noise," says Bulling. The researchers reported further details at the conference "Human Factors in Computing Systems (CHI)", which has just been held in California. They also discussed the new system in the published paper "SkullConduct: Biometric User Identification on Eyewear Computers Using Bone Conduction Through the Skull."

As a next step, Bulling and his colleagues want to test whether their method works in everyday life. They want to investigate the frequency range of ultrasound, which would have the advantage that the user would not hear the signal. The researchers can also imagine their method being used by smartphones. "If the smartphone has a correspondingly placed bone conduction speaker and a microphone, and the user presses it with bone contact to his [skull](#), it could possibly work even with the normal ringtone of the smartphone," Bulling says.

Provided by Saarland University

Citation: A password of another kind: User identification through the skull (2016, May 12)
retrieved 2 May 2024 from

<https://techxplore.com/news/2016-05-password-kind-user-identification-skull.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.