Wearables to boost security of voice-based log-in

October 17 2017

Kang Shin, Kevin and Nancy O'Connor Professor of Computer Science and Professor of Electrical Engineering and Computer Science, demonstrates VAuth, a wearable voice authentication device. Credit: Joseph Xu, Michigan Engineering

A security-token necklace, ear buds or eyeglasses developed at the University of Michigan could eliminate vulnerabilities in voice

authentication—the practice of logging in to a device or service with your voice alone.

Talking to electronics has become a popular—even essential—way to command them. In this era of the internet of things, voice assistants connect people to their mobile devices, homes and vehicles. Through spoken interactions, we place calls, send text messages, check email, get travel directions, control appliances, and even access bank accounts. Barclays bank, for example, recently began using a technology that uses voice to verify the identity of call-in center customers.

But sound is what researchers call an "open channel" that can be easily spoofed by mediocre impersonators and sophisticated hackers alike.

"Increasingly, voice is being used as a security feature but it actually has huge holes in it," said Kang Shin, the Kevin and Nancy O'Connor Professor of Computer Science and professor of electrical engineering and computer science at U-M. "If a system is using only your voice signature, it can be very dangerous. We believe you have to have a second channel to authenticate the owner of the voice."

The solution that Shin and colleagues developed is called VAuth (pronounced vee-auth), and it's a wearable device that can take the form of a necklace, ear buds or a small attachment to eyeglasses. VAuth continuously registers speech-induced vibrations on the user's body and pairs them with the sound of that person's voice to create a unique and secure signature.

The process of speaking creates vibrations that can be detected on the skin of a person's face, throat or chest. The system works by leveraging the instantaneous consistency between signals from the accelerometer in the wearable security token and the microphone in the electronic device. You can only use voice authentication with your device when you're

wearing the security token.

The team has built a prototype using an off-the-shelf accelerometer, which measures motion, and a Bluetooth transmitter, which sends the vibration signal to the microphone in the user's device. They've also developed matching algorithms and software for Google Now.

"VAuth is the first serious attempt to secure this service, ensuring that your voice assistant will only listen to your commands instead of others," Shin said. "It delivers physical security, which is difficult to compromise even by sophisticated attackers. Only with this guarantee can the voice assistant be trusted as personal and secure, especially in scenarios such as banking and home safety."

That's a drastic departure from existing voice biometric mechanisms, which require training from each individual who will use them, said Kassem Fawaz, who worked on the project as a graduate student at U-M and is now an assistant professor at the University of Wisconsin.

"In addition, VAuth overcomes a key problem of voice biometrics," he said. "A voice biometric, similar to a fingerprint, is not easy to keep protected. From a few recordings of the user's voice, an attacker can impersonate the user by generating a matching 'voice print.'

"The users can do little to regain their security as they cannot simply change their voice. On the other hand, when losing VAuth for any reason, the user can simply unpair it to prevent an attacker from using their device."

The team tested VAuth with 18 users and 30 voice commands. It achieved a 97-percent detection accuracy and less than 0.1 percent false positive rate, regardless of its position on the body and the user's language, accent or even mobility. The researchers say it also

successfully thwarts various practical attacks, such as replay attacks, mangled voice attacks or impersonation attacks.

The researchers also surveyed 952 people to gauge their willingness to wear a security token.

"Seventy percent of them said they are willing to give VAuth a serious try in one of the three configurations we developed—and half of them said they are willing to pay $25 more for the technology," said Huan Feng, who worked on the project as a graduate student and currently works for Facebook.

A study on VAuth, titled "Continuous Authentication for Voice Assistants," will be presented Oct. 19 at the International Conference on Mobile Computing and Networking, MobiCom 2017, in Snowbird, Utah.

More information: Study (PDF): Continuous Authentication for Voice Assistants: kabru.eecs.umich.edu/wordpress … entication-voice.pdf

Provided by University of Michigan