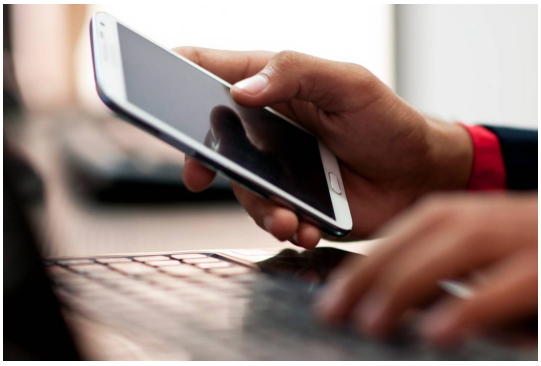
THE WALL STREET JOURNAL.
This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

https://www.wsj.com/articles/hackers-may-soon-be-able-to-tell-what-youre-typingjust-by-hearing-you-type-11559700120

BUSINESS | JOURNAL REPORTS: TECHNOLOGY

Hackers May Soon Be Able to Tell What You're Typing—Just By Hearing You Type

Research suggests that sound waves from typing on a phone can be intercepted and decoded



Researchers in one study cracked seven out of 27 passwords on a smartphone and 19 out of 27 on a tablet. PHOTO: ISTOCK

By Matthew Kassel
June 4, 2019 10:02 pm ET

Thanks to the increasing sophistication of smartphone technology, hackers soon may be able to intercept and analyze the sounds of typing—and figure out exactly what people are writing on their devices.

A growing body of academic research suggests that acoustic signals, or sound waves, produced when we type on our phones could be used by hackers to glean text messages, passwords, PINs and other private information. Such attacks could occur, experts say, if smartphone users were to download an app infected with malware that gains access to such smartphone sensors as microphones, accelerometers and gyroscopes.

One recent study, one of the latest demonstrations of hacking that exploits acoustics, found that the microphones in Android devices can be used to pick up the vibrations that are produced when you use the virtual keyboard on your phone or tablet. The sound waves that are recorded can then be interpreted to discern where on the screen you tapped and which keys you struck.

Based on results using 45 participants, the study's researchers, from the University of Cambridge in England and Sweden's Linköping University, were able to recover numerical codes, letters and whole words with some accuracy. For example, in 10 attempts, the researchers, using a machine-learning algorithm that classified each vibration, cracked seven out of 27 passwords on a smartphone and 19 out of 27 passwords on a tablet.

The study is available online in an archive of academic papers maintained by Cornell University, though it hasn't been published in an academic journal and hasn't yet undergone formal peer review. But computer-science experts who were asked to read it for this article say that it

JOURNAL REPORT

- Read more at WSJ.com/journalreporttech

MORE IN CYBERSECURITY

- The Quantum Threat to Encryption
- Our Emotional Attachment to Our Passwords
- The Tussle Over Facial Recognition
- How Not to Be Hacked at an ATM

shows a plausible avenue of attack, though certain current security constraints could make it unlikely, they add. Smartphones typically ask the user for permission when an app wants to access the microphone, for example, which could reveal a possible incursion. But no such permission is usually needed when an app wants to access another type of sensor such as the accelerometer, the built-in instrument that is used to measure acceleration, which hackers could use to steal data in a more discreet fashion.

Ilia Shumailov, a Ph.D. candidate in computer science and technology at the University of Cambridge, is an author of the study, which proposes that companies design smartphones that indicate to users when their microphones and other sensors have been turned on, indicating a possible breach.

A number of previous studies have examined other ways that acoustic hacking of smartphones can take place. In one early paper in the field, from 2012, researchers at the University of Pennsylvania looked at how a smartphone's accelerometer—which is used, for instance, to measure steps—can be repurposed by hackers to collect screen vibrations that can then be used to infer PINs and passwords. This paper hasn't been published but was presented at an apps security conference in Orlando, Fla., in 2012.

In controlled settings using 50 PINs and 50 Android swipe-to-unlock patterns (used by Android owners to access their phones rather than a numerical password), the researchers at Penn found that in five attempts their machine-learning technology could figure out a PIN 43% of the time and a pattern 73% of the time.

Adam Aviv, an author of the study and now an assistant professor of computer science at the U.S. Naval Academy, says that researchers are also examining whether accelerometers can be used to capture the vibrations from speech. Though it is difficult to parse exact phrases in this way, he says, hackers could possibly use the sound waves to determine personally identifiable information like age and gender.

Despite existing research, Dr. Aviv—who says Mr. Shumailov's study is plausible—thinks that concerns over acoustic attacks are somewhat overblown, at least at the moment. Right now, he explains, such attacks are more a subject of academic inquiry than a real-world threat. Acoustic hacking has long been of interest to researchers, he says, and the smartphone has over the past decade or so provided a new platform for experimentation. But it is still difficult to extract the acoustic information from smartphones with much reliability, he says, though that could change as the technology improves.

Murtuza Jadliwala, an assistant professor of computer science at the University of Texas at San Antonio, agrees that acoustic attacks are possible. Dr. Jadliwala also read the Shumailov study and says it seems plausible. Still, he thinks acoustic attacks would be hard to pull off now because machine-learning algorithms trained to evaluate sound waves in academic experiments would most likely prove unreliable when placed in a real-world setting where environmental factors could interfere with the acoustic signal.

In any case, there are simple precautions smartphone users can take to subvert a possible attack, according to Philip Brisk, an associate professor in computer science and engineering at the University of California, Riverside. Such steps include only installing apps from trusted sources and only granting microphone access to apps that legitimately need it, Dr. Brisk says.

Mr. Shumailov, for his part, says that despite current obstacles to such attacks, we need to get ready.

"If right now it's really hard to imagine anybody deploying these attacks," he says, "in the near

future they're definitely going to be there."

Mr. Kassel is a writer in New York. He can be reached at reports@wsj.com.

Appeared in the June 5, 2019, print edition as 'Hackers May One Day Be Able to Tell What You're Typing—Just By Hearing You Type.'

- **College Rankings**
- **College Rankings Highlights**
- **Energy**
- **Funds/ETFs**
- **Health Care**
- **Leadership**
- **Retirement**
- **Small Business**
- **Technology**
- **Wealth Management**

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.