AI can identify passwords by sound of keys being pressed, study suggests

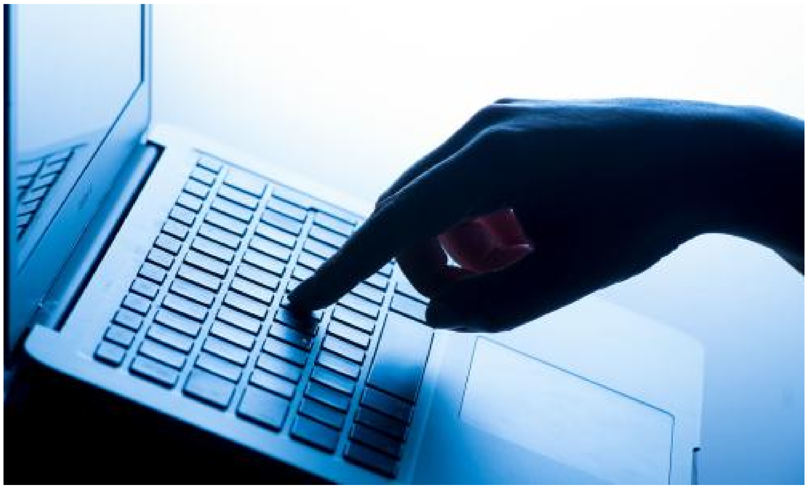
Publication Date: 2023-08-08

Author: Nicola Davis

Section: Technology

Tags: Artificial intelligence (AI), Privacy, Cybercrime, Computing, Mobile phones, news

Article URL: https://www.theguardian.com/technology/2023/aug/08/ai-could-identify-passwords-by-sound-of-keys-being-pressed-study-suggests



Tapping in a computer password while chatting over Zoom could open the door to a cyber-attack, research suggests, after a study revealed artificial intelligence (AI) can work out which keys are being pressed by eavesdropping on the sound of the typing. Experts say that as video conferencing tools such as Zoom have grown in use, and devices with built-in microphones have become ubiquitous, the threat of cyber-attacks based on sounds has also risen. Now researchers say they have created a system that can work out which keys are being pressed on a laptop keyboard with more than 90% accuracy, just based on sound recordings. “I can only see the accuracy of such models, and such attacks, increasing,” said Dr Ehsan Toreini, co-author of the study at the University of Surrey, adding that with smart devices bearing microphones becoming ever more common within households, such attacks highlight the need for public debates on governance of AI. The research, published as part of the IEEE European Symposium on Security and Privacy Workshops, reveals how Toreini and colleagues used machine learning algorithms to create a system able to identify which keys were being pressed on a laptop based on sound – an approach that researchers deployed on the Enigma cipher device in recent years. The study reports how the researchers pressed each of 36 keys on a MacBook Pro, including all of the letters and numbers, 25 times in a row, using different fingers and with varying pressure. The sounds were recorded both over a Zoom call and on a smartphone placed a short distance from the keyboard. The team then fed part of the data into a machine learning system which, over time, learned to recognise features of the acoustic signals associated with each key. While it is not clear which clues the system used, Joshua Harrison, first author of the study, from Durham University, said it was possible an important influence was how close the keys were to the edge of the keyboard. “This positional information could be the main driver behind the different sounds,” he said. The system was then tested on the rest of the data. The results reveal that the system could accurately assign the correct key to a sound 95% of the time when the recording was made over a phone call, and 93% of the time when the recording was made over a Zoom call. The study, which is also authored by Dr Maryam Mehrnezhad from the Royal Holloway, University of London, is not the first to show that keystrokes can be identified by sound. However, the team say their study uses the most up-to-date methods and has achieved the highest accuracy so far. While the researchers say the work is a proof-of-principle study, and has not been used to crack passwords – which would involve correctly guessing strings of keystrokes – or in real world settings like coffee shops, they say the work highlights the need for vigilance, noting that while laptops – with their similar keyboards and common use in public places – are at high risk, similar eavesdropping methods could be applied to any keyboard. The researchers add there are a number of ways the risk of such acoustic “side channel attacks” can be mitigated, including opting for biometric passwords where possible or activating two-step verification systems. Failing that, they say it’s a good idea to use the shift key to create a mixture of upper and lower cases, or numbers and symbols. “It’s very hard to work out when someone lets go of a shift key,” said Harrison. Prof Feng Hao from the University of Warwick, who was not involved in the new study, said people should be careful not to type sensitive messages, including passwords, on a keyboard during a Zoom call. “Besides the sound, the visual images about the subtle movements of the shoulder and wrist can also reveal side-channel information about the keys being typed on the keyboard even though the keyboard is not visible from the camera,” he said.