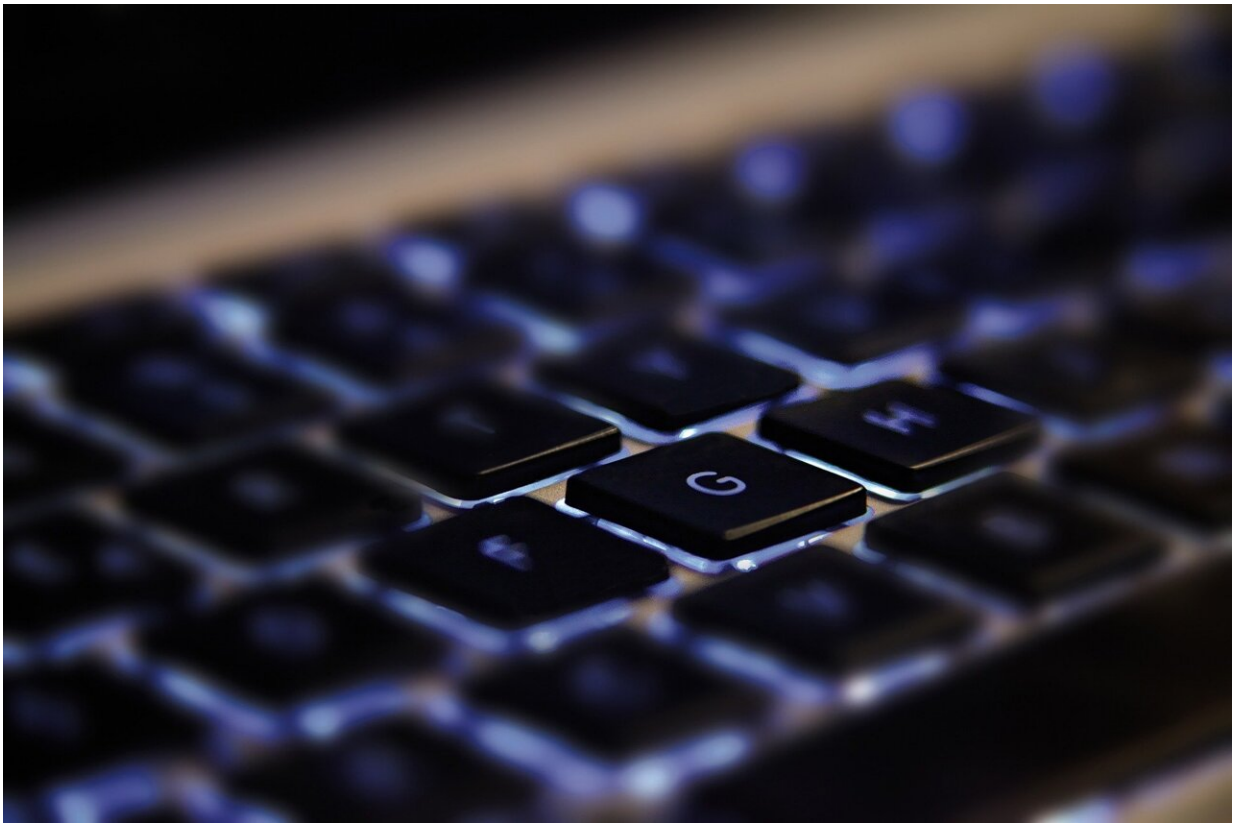
Research shows snoops can decipher keystrokes during Zoom calls

August 8 2023, by Peter Grad



Credit: Pixabay/CC0 Public Domain

One upon a time we thought the worst things that could happen during a Zoom conference were accidentally leaving the microphone on while cursing out your cat, hearing someone snoring during your stellar

summation of your latest project, or standing up to run to the kitchen while forgetting you have no pants on.

However, a team of British researchers reported last week that hackers sitting nearby in a coffee shop can pick up and identify keystrokes over a Zoom call.

It is the latest variation of lifting data based on physical properties of the target devices. Side channel attacks can listen to keystrokes from keyboards, ATMs or smartphones; detect vibrations emitted by various computer components that have their own acoustic signatures; discern electromagnetic signals from a screen or even the vibrations of a lightbulb in the same room as a digital device, all of which can be captured and analyzed to decrypt sensitive information.

Researchers Joshua Harrison, Ehsan Toreini and Marhyam Mehrnezhad said their latest work shows that the latest technologies in audio and video, coupled with machine learning, "present a greater threat to keyboards than ever."

Using a MacBook Pro and an iPhone, researchers from Durham University in England recorded keyboard typing sounds and then ran them through an algorithm that achieved an extremely high rate of accuracy identifying the keystrokes.

Recordings made with the iPhone displayed a 95% degree of accuracy. Sounds captured through a Zoom conference call had an accuracy rate of 93%.

The researchers noted the ease with which they were able to decipher conversations and their concerns about security.

"Our results prove the practicality of these side channel attacks via off-

the-shelf equipment and algorithms," they said in a paper on the project. "The ubiquity of keyboard acoustic emanations makes them not only a readily available attack vector, but also prompts victims to underestimate [and therefore not try to hide] their output."

The researchers explained that people often reflexively hide their screens when typing in passwords or other sensitive data, but don't generally concern themselves with the sounds their keypads are making.

Given the greater sensitivity and availability of today's microphones and easily transportable recording devices such as smart watches, the threat of interception becomes greater, they said.

The team noted that most of the decryption errors stemmed from misidentification of acoustics of keys that were nearby the correct keys. They said incorporating machine-learning algorithms should mitigate that problem.

What can users do to protect themselves from such acoustic side channel attacks?

The researchers noted several options:

- Alter typing style, such as using touch-typing techniques that involve the use of all fingers, increasing acoustic variance.—Insert fake keystrokes at random points to throw algorithms off.
- Use random passwords with multiple case changes. The researchers note that the release peak of the shift key, used for capitalization, is not easily detected.
- Use biometric logon features such as face or fingerprint recognition.

The research paper, "A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards," appears on the preprint server *arXiv*.

More information: Joshua Harrison et al, A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards, *arXiv* (2023). DOI: 10.48550/arxiv.2308.01074