PUBLICATION

I Can Hear Your Passwords

August 21, 2023

On August 3, British researchers published an Institute of Electrical and Electronics Engineers (IEEE) article explaining how the sounds of typing on a laptop keyboard can be heard and that deep learning can be used to determine keystrokes with over 93 percent accuracy from sounds and electrical emanations.

Deep learning is a subset of machine learning using neural networks and multiple layers of processing. The experiment in this attack used two acoustic sensors: a smartphone and the Zoom application. Voice over IP (VOIP) phones recorded a 74 percent accuracy, which will only improve with further research. Other listening devices potentially used for this attack include Internet of Things (IoT) devices such as Alexa and other collaboration applications such as Teams because the number of microphone-enabled devices in proximity to keyboards will only rise in the future due to the interconnectedness of devices.

Risk to organizations rapidly increases if passwords and other sensitive information such as intellectual property, as well as personally identifiable and financial information, are accurately deciphered from acoustics. Offices are typically "littered" with multiple devices that have microphones or are used for active online meetings through collaborative applications. The microphones do not have to be on the desk for this to work. Driven by increased online collaboration and increased sales of higher-quality microphones for work environments, as well as technology advancements in personal devices meant to overcome ambient noise, threats have occurred.

Mitigation Strategies

In response to this threat, multiple mitigations exist, although none alone completely stop the threat. We encourage multiple simultaneous mitigations.

1. Randomized passwords using multiple cases to defeat current language-based learning models. This can be further effective by using two-factor identification, such as tokens or biometrics for logging in to areas processing sensitive information.

2. Explicit policies about acceptable devices allowed in areas of sensitive information, as well as policies for muting microphones during online meetings and calls when not actively talking.

For those companies with a need for higher higher-level security, such as, but not limited to, organizations fulfilling Department of Defense contracts, performing classified work with other federal agencies, or handling large financial transactions, recommended measures include consideration of the following strategies to reduce the increased risk in conjunction with the previous concerns.

3. Mixing sounds or fake keystrokes into transmitted audio locally by the IT team is less distracting than audio played in the room to users — current audio software removes much of the perceived white noise.

4. Shifting to silent touchscreen, such as what exists natively on tablets, eliminates the acoustic signature of keys. However, research is uncovering that compromised smartphone microphones inferred text with concerning accuracy.

Takeaways

Outside counsel should assist in reviewing your data mapping considerations, creation of security programs, disaster recovery processes, and incident responses, and further ensuring that your policies and procedures reflect the correct operating stance to protect your information and devices, as well as implementation through review and tabletop exercises.

For any questions about how this vulnerability might affect your business or your clients, or how you can better prepare for these types of threats, please contact Dr. Michael Klipstein, CISM, CISSP, or any member of the Baker Donelson Data Protection, Privacy, and Cybersecurity Team.