New Side-Channel Hack Attack Uses Your Microphone to Read Your Screen Content

By Ionut Ilascu

0

Using regular microphones, academic researchers managed to pick up acoustic signals from computer displays and determine in real time the type of content on the screen.

The technique could potentially allow an attacker to run surveillance operations, exfiltrate information, or spy on the victim's browsing activity.

By studying the audio emissions from multiple LCD screens (with both CCFL and LED backlighting), the researchers noticed a connection between the images displayed and the sound they made. They found that what is shown on screen comes with a distinct audio signature.

The audio produced by computer screens comes from the power supply emitting a high-pitch noise when modulating current. The sound varies according to the power requirements needed to render the visual content; it is barely noticeable by the human ear, but common microphones have no problem detecting and recording it.

After working with simple visual models and analyzing the spectogram of their audio recording, the researchers were able to create a fingerprint that could be used to recognize content from other captures.

A successful attack needs planning

The researchers experimented with their technique from an attacker's perspective, who needs to be prepared to deal with variables that influence the recording, such as environmental noise, distance, type of microphone and its position relative to the screen.

To minimize the risk of failure, an attacker should have sufficient markers to identify the content they're interested in (websites, text), and a model to spot the patterns automatically.

"[I]n an off-line stage, the attacker collects training data (audio traces) to characterize the acoustic emanations of a given type of screen, and uses machine-learning to train a model that distinguishes the screen content of interest (e.g., websites, text, or keystrokes)," reads the research paper.

Getting relevant audio emissions

The next step is to grab the audio, a task that does not necessarily require proximity. Recordings of VoIP and video-conference calls include sounds pertinent to creating a fingerprint of the image on the screen.

"In fact, users often make an effort to place their webcam (and thus, microphone) in close proximity to the screen, in order to maintain eye contact during the video conference, thereby offering high-quality measurements to would-be attackers," explains the paper.

The researchers tested other methods to grab the audio data from the display. They were able to capture the leaks using a smartphone positioned near the screen and smart virtual assistants (Amazon Alexa and Google Home). They even tried a parabolic microphone from a 10m line-of-sight aimed at the back of the computer monitor.

Results are in

The tests ran in an office environment, to simulate a realistic scenario, with noise from other electronic equipment and people talking near the microphone.

The experiments used fingerprints of 97 websites, to determine if the attacker could identify which one was displayed on the victim's monitor screen.

Errors occurred in 8% of the close-range and phone attacks, and double that much in at-distance attempts. However, the scenarios that involved proximity of the recording device attained a validation set accuracy of 97%. For the at-distance experiments, the success rate was 90.9%.

A text extraction attack was also tested, to simulate the stealing of sensitive information. In this case, it is assumed that the attacker knows the content type shown on the monitor and that the text font is quite large.

Per-character validation typically ranged from 88% to 98%. From 100 recordings of test words, in 56 cases the most probable word on the list was the right one, and in 72 instances it popped in the top five most probable words. The algorithm had 55,000 words to pick from.

While it is only an experiment unlikely to become a popular attack method any time soon, the researchers discussed a variety of mitigations.

Measures that eliminate the acoustic emanation, mask or shield it, are costly for manufacturers, or they are difficult to implement.

A viable solution could be software mitigations similar to those against the electromagnetic Tempest attack.