Guarding against Screen Content Detection via Remote Acoustic Side Channels

By Julian de Gortari Briseno

Based on:
Genkin, Daniel et al. “Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels.” 2019 IEEE Symposium on Security and Privacy (SP) (2019).

Overall Project Goals and Specific Aims

Overall goal:

- Prove it is possible to guard laptop computers with LCD screens against acoustic side channel attacks by concealing the sound generated by these devices.

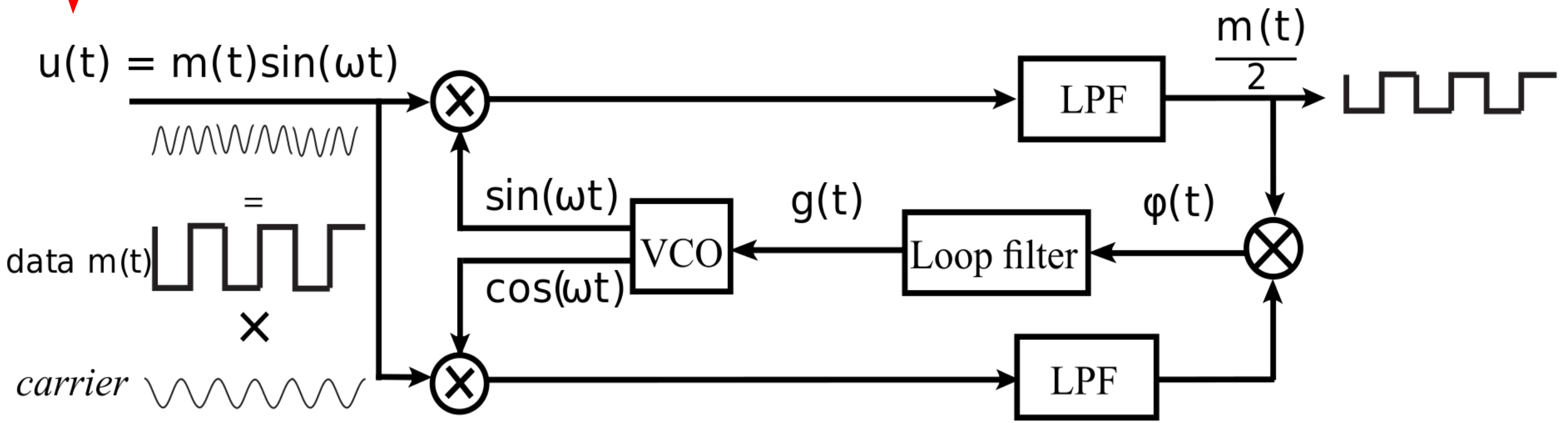
Specific aims:

- Analyze the frequency spectrum of the audio generated by the screen from a laptop in order to see if it's vulnerable to the attack.
- Process audio signals in order to obtain samples low in noise and in phase according to the screen's refresh rate.
- Train CNN to distinguish between websites visited.
- Test the accuracy of the CNN classifier with samples containing different levels of noise.

Technical Approach: Extracting the signal

Laptop's microphone records at 96 kHz

Costas loop used to demodulate band-pass filtered AM DSB-SC signal



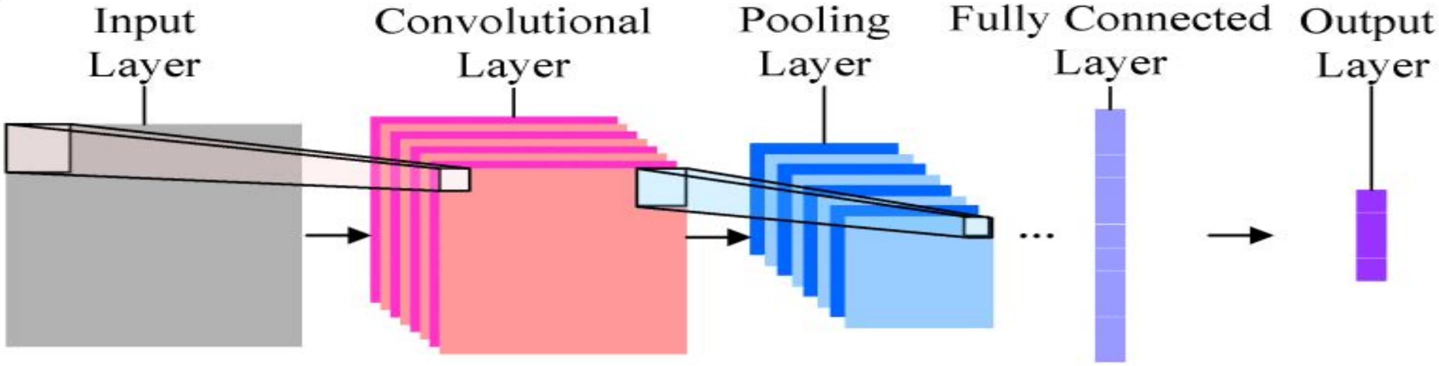
Technical Approach: Obtaining predictions

Denoising algorithm

Signal is divided into chunks according to the refresh rate of the screen (which is always slightly changing).

Correlated chunks are chosen and an average of the chunks is obtained.

CNN classifier

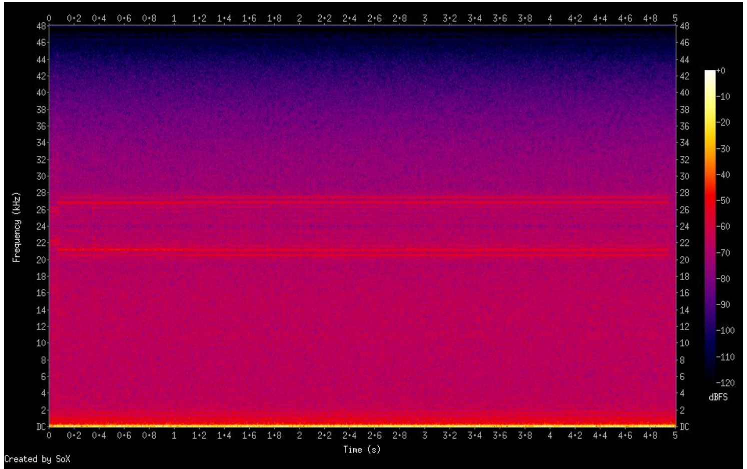


Technical Approach: Defense mechanism

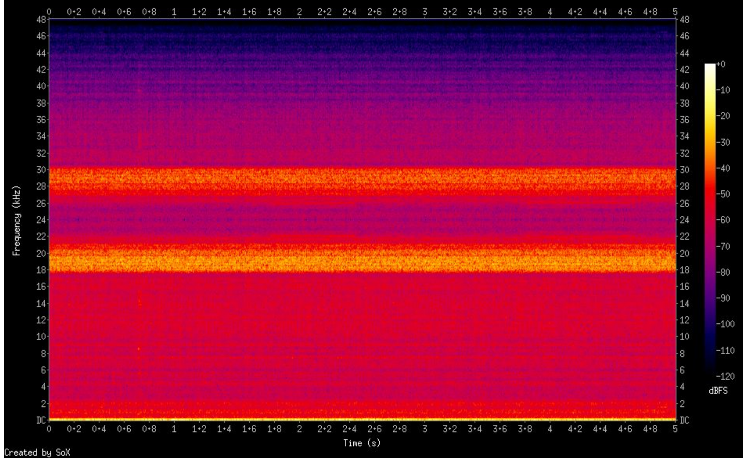
White noise
high-pass filtered
at 18 kHz

White noise is played at different sound levels relative to the maximum output of the speakers: -29 dB(60%), -37 dB(50%), -44 dB(40%), -51 dB(30%), -59 dB(20%), -66 dB(10%), -73 dB(1%)

Sample without noise

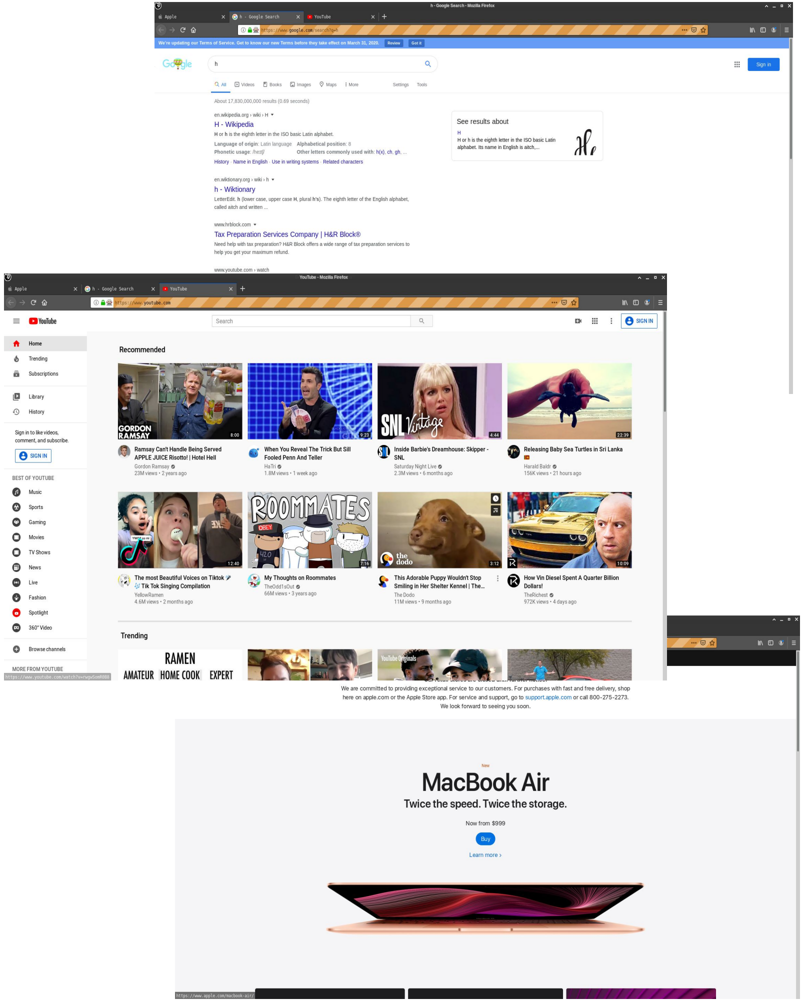


Sample with
-29 dB (60%)
noise



Implementation

- 5-second audio samples were obtained from 3 websites using Selenium.
- 1200 samples in total were captured for training (400 each), but only 450 in total were useful (150 each).
- 300 test samples without noise were captured in total but only 223 were useful.
- 150 test samples for each noise level were captured.
- Costas Loop and chunking algorithm were implemented in a Matlab program.
- Tensorflow was used for the CNN model.
- White noise was produced using SoX.



We're updating our Terms of Service. Get to know our new Terms before they take effect on March 31, 2020.

About 17,830,000,000 results (0.69 seconds)

en.wikipedia.org › wiki › H

H - Wikipedia

H or h is the eighth letter in the ISO basic Latin alphabet.

Language of origin: Latin language Alphabetical position: 8

Phonetic usage: /heɪtʃ/ Other letters commonly used with: h(x), ch, gh, ...

History · Name in English · Use in writing systems · Related characters

en.wiktionary.org › wiki › h

h - Wiktionary

LetterEdit. h (lower case, upper case H, plural h's). The eighth letter of the English alphabet, called aitch and written ...

www.hrblock.com

Tax Preparation Services Company | H&R Block®

Need help with tax preparation? H&R Block offers a wide range of tax preparation services to help you get your maximum refund.

www.youtube.com › watch

See results about

H

H or h is the eighth letter in the ISO basic Latin alphabet. Its name in English is aitch,...

Sign in to like videos, comment, and subscribe.

Ramsay Can't Handle Being Served APPLE JUICE Risotto! | Hotel Hell
Gordon Ramsay
23M views • 2 years ago

When You Reveal The Trick But Sill Fooled Penn And Teller
HaTri
1.8M views • 1 week ago

Inside Barbie's Dreamhouse: Skipper - SNL
Saturday Night Live
2.3M views • 6 months ago

Releasing Baby Sea Turtles in Sri Lanka
Harald Baldr
156K views • 21 hours ago

The most Beautiful Voices on Tiktok 🎤 🎶 Tik Tok Singing Compilation
YellowRamen
4.6M views • 2 months ago

My Thoughts on Roommates
TheOdd1sOut
66M views • 3 years ago

This Adorable Puppy Wouldn't Stop Smiling in Her Shelter Kennel | The...
The Dodo
11M views • 9 months ago

How Vin Diesel Spent A Quarter Billion Dollars!
TheRichest
972K views • 4 days ago

We are committed to providing exceptional service to our customers. For purchases with fast and free delivery, shop here on apple.com or the Apple Store app. For service and support, go to support.apple.com or call 800-275-2273. We look forward to seeing you soon.

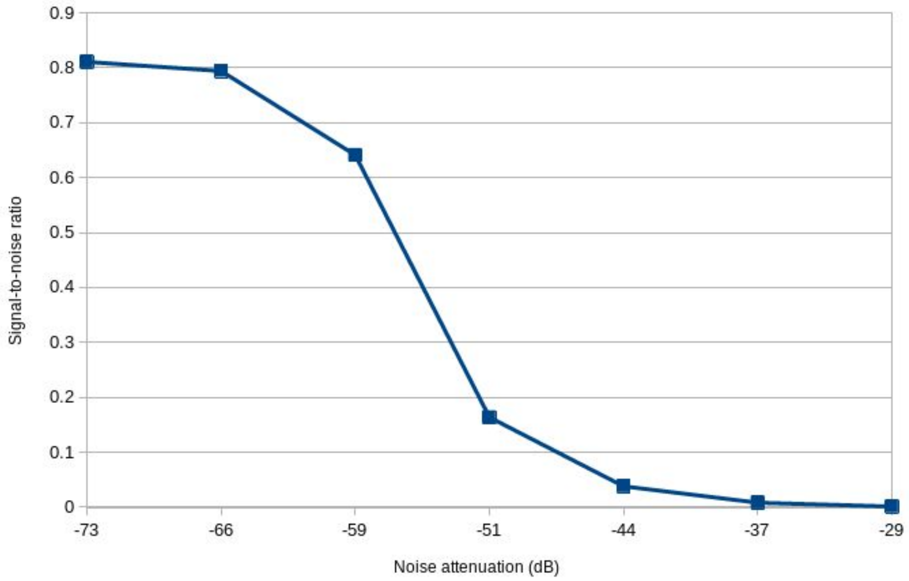
MacBook Air

Twice the speed. Twice the storage.

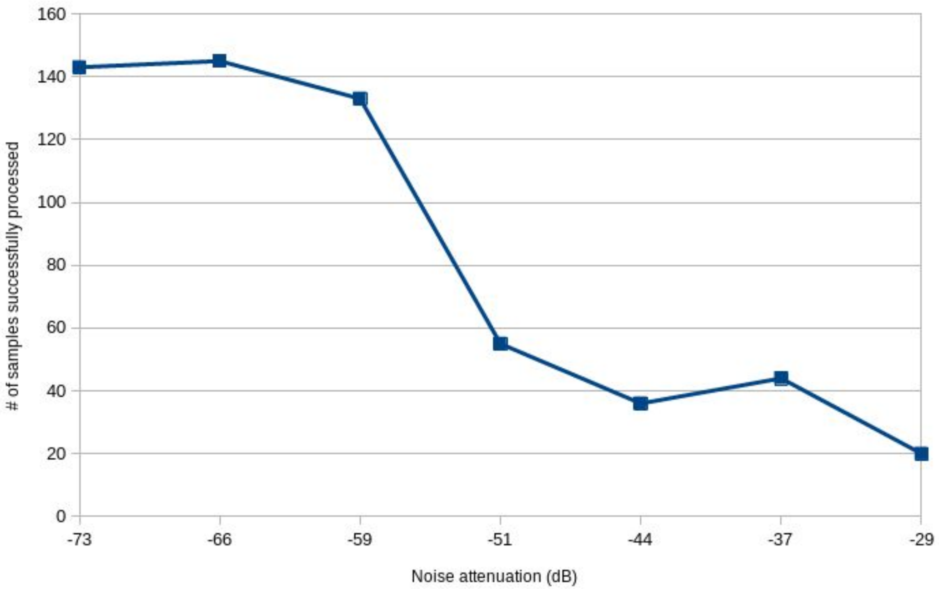
Now from $999

Results

Average signal-to-noise ratio of audio samples vs. sound level of white noise generated

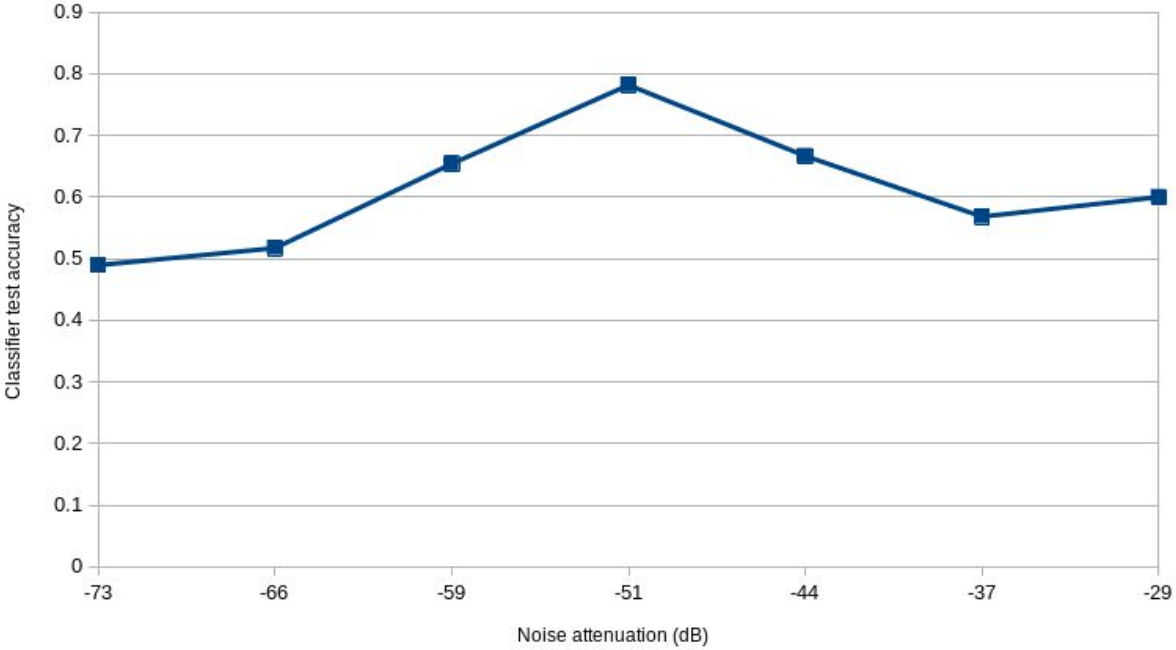


Number of audio samples successfully processed by chunking algorithm vs. sound level of white noise generated



Results

Classifier test set accuracy vs. sound level of white noise generated



Test accuracy without noise: 82.06%

Related Work

- Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. (2018). Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels (https://www.cs.tau.ac.il/~tromer/synesthesia/synesthesia.pdf)

- Markus G. Kuhn. (2004). Electromagnetic Eavesdropping Risks of Flat-Panel Displays (https://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf)

- Prakash Shrestha, S Abhishek Anand, Nitesh Saxena. (2017). YELP: Masking Sound-based Opportunistic Attacks in Zero-Effort Deauthentication (https://dl.acm.org/doi/abs/10.1145/3098243.3098259)

- Biamp Systems. Cambridge Sound Management (https://cambridgesound.com/)

Strengths

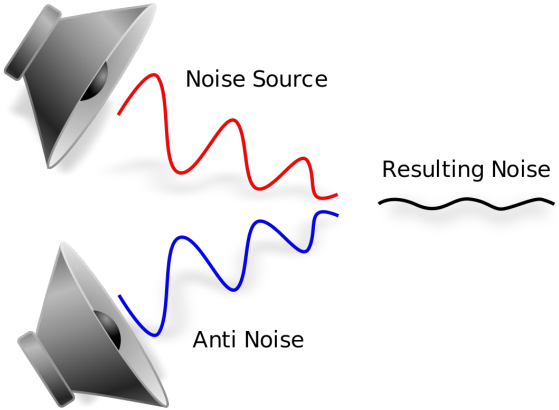
- This work discovered that in certain LCD screens, the AM signal that is supposed to appear has no carrier. A solution is proposed using a Costas Loop.
- The defense mechanism does reduce the number of potentially useful samples.
- The solution doesn’t require any external equipment to work and as the white noise is filtered, it doesn’t appear to be annoying to hear.

Weaknesses

- The classification accuracy didn’t show a strong relationship with noise level applied, but that could be related to the number of samples used as input.
- Considering that the attacker could have plenty of time to capture as much samples as he wants, as in the case where he could get control of the laptop’s internal microphone, reducing by some factor the number of usable samples isn’t likely to stop his attack.
- The Costas Loop process seems to introduce noise to the samples, but it can be also that the samples obtained are noisy.

Future work

- Keep adjusting the parameters of our filters, Costas Loop and chunking algorithm in order to get better quality in the data used for training.
- Develop an active noise control system that responds effectively in order to mask the leakage signal.
- Test the defense mechanism in LCD screens that emit complete AM signals.
- Increase the number of websites used.



GitHub

GitHub repo: https://github.com/kiototeko/ECE209AS_Winter2020

GitHub page: https://kiototeko.github.io/ECE209AS_Winter2020/