Ethan Jerram and Nate Sherman
Cal Poly San Luis Obispo, CSC 492
Professor Stephen Beard
06/06/2024

Senior Project Report: Mechanical Keyboard Acoustic Side Channel Attack

Abstract
For our senior project, we aimed to recreate an acoustic side-channel attack. We based our work on a specific study that achieved over 95% accuracy in identifying recorded keystrokes using a MacBook keyboard and Zoom recordings.

Introduction
To recreate the acoustic side-channel attack, we divided the project into several stages. First, we collected training data by recording the audio of individual keystrokes. Next, we developed a method to isolate these keystrokes from the recordings and convert them into a format understandable by a computer. Using the Python library Librosa, we determined the peak frequency of sounds in the audio recordings to isolate each keystroke. We then converted each isolated keystroke into a mel spectrogram, which visually represents the frequency spectrum of an audio signal over time. Finally, we trained a deep learning model to recognize which key corresponds to each spectrogram. Our goal is to test the model with new data and achieve high accuracy. The potential applications of this project are vast and potentially dangerous, including detecting PINs for bank accounts and passwords for sensitive information.

Background / related work (on an as-needed basis)
In this project we did not have much background experience in sound engineering or deep learning models. We had to develop our own understanding of how to isolate sound, converting sound into mel spectrograms, and how to train and create a deep learning algorithm. We found that learning from scratch was rewarding and we learned an extensive amount we had not in previous classes. It increased both of our interests in both deep learning and cybersecurity.

Requirements
For this project we did not have a lot of background in the fields of audio engineering and deep learning. We absorbed a lot of the information about isolating notes and the Librosa python library from YouTube and other internet sources. For the deep learning portion we used an open and public github repository implementation of CoAtNet developed by the user chinhsuanwu found here: https://github.com/chinhsuanwu/coatnet-pytorch. We also received help from Cal Poly San Luis Obispo professor Jonathan Ventura. We spoke to him about specific questions regarding the model and best practices.

Key Design Decisions and Ethical Considerations

One of the key design choices we made was implementing our deep learning model in TensorFlow or PyTorch. Both have certain advantages over the other and different user features. We found both Tensorflow and Pytorch implementations of CoAtNet on github and ultimately we decided to use PyTorch because we believed PyTorch was more user friendly and documented for beginners such as ourselves.

From an ethical standpoint, acoustic side channel attacks can have many malicious applications. They can be used to record and determine bank pins and sensitive passwords. However, understanding these vulnerabilities is crucial for developing countermeasures and improving security. By researching and demonstrating the potential risks, we can raise awareness and encourage the creation of more secure systems to protect against such attacks. Responsible disclosure and ethical use of this knowledge are essential to ensure it contributes positively to cybersecurity.

Future Work

There is a lot of future work that can be done in this project and the entire area of side channel attacks. For our project specifically, we hoped to get a higher testing accuracy. One method of improving the accuracy that we would have liked to implement is using Synthetic Minority Oversampling Technique (SMOTE) to duplicate the existing training data and making small tweaks to artificially create more training data and improve the accuracy of the model. By creating small tweaks in the training data and training using a vast amount of more data, it increases the accuracy because the test data is likely to be highly similar to some of the SMOTE data if not the real data.

We would have liked to create a live demo of our project as well. This would have involved saving the weights of the model and adapting our librosaPeaks.py peak detection python file to isolate a note in live time. We could then determine the note from the saved model weights and give a live time estimation of what key is being pressed. This would be an essential step for many practical applications of our project, such as secretly determining a password in live time.

Reflections

There are some parts of this project we look back on and think we did well and other things we think could have been done better. One example of something we think was helpful in our success was using an iterative model to develop our code. Instead of jumping straight into keystroke note isolation, we started with generated piano notes, something that is far more distinct than mechanical clacks on a keyboard. This helped us establish a proof of concept and helped with debugging for isolating the keyboard. On the other hand, this iterative model did not work in our favor when developing a deep learning model to train the data. We developed a model that trained on the specific piano notes. Unfortunately, the model was fitted properly for

the piano notes but did not translate to the more similar keystrokes. We had to pivot our model to a CoAtNet as recommended in the paper.

Conclusion

We are proud to have completed the work that we did. When running our CoAtNet model using a Kfolds split on the training data we reached an impressive 97-99% accuracy. This was done with the 26 different letters, with each letter pressed 25 times. Upon recording unique testing data and testing on the saved model weights from the training data, we found that the model lost a significant amount of accuracy. This is likely due to an extreme overfitting of the training model. One possible solution to fixing this problem would be to use the Synthetic Minority Oversampling Technique, as outlined in our Future Work section.