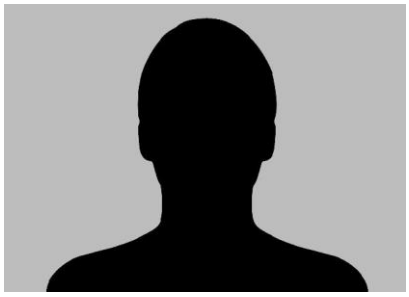
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

Acoustic Emanations Re-Revisited: Using recordings of keystrokes to find passwords and other secrets



Diplomierende
Daniel Dorigatti
Adrian Martin Eyholzer

Dozent
Stephan Neuhaus

Seitenkanalangriffe sind nach wie vor ein wichtiges Forschungsgebiet der Cybersicherheit. Obwohl sie im alltäglichen Leben nicht oft genutzt werden, können sie bei gezielten Angriffen von enormem Wert sein. In dieser Arbeit untersuchen wir einen Angriff der das Klangbild von Tastaturen ausnutzt. Unser Ziel war es, eine Arbeit zu replizieren, die eine Methode zur Erkennung von getipptem Text aus einer Audioaufnahme vorgestellt hat. Eine direkte Replikation der Arbeit konnte nicht vollständig umgesetzt werden, da entscheidende Details fehlten. Dennoch haben wir in der folgenden Arbeit eine ähnliche Pipeline rekonstruiert. Die Extraktion von Klangmerkmalen wurde mit MFCCs durchgeführt. Die Reduzierung der Koeffizientendimension wurde mit UMAP durchgeführt. DBSCAN wurde zur Erstellung von Clustern verwendet, mit dem Ziel, HMMs zur Buchstabenzuweisung zu trainieren. Mit der neu implementierten Pipeline konnte eine Zeichenerkennungsgenauigkeit von 87% erreicht werden und dies bevor ein Sprachkorrekturmodell eingesetzt wurde. Die ursprüngliche Genauigkeit von circa 60% konnte deutlich verbessert werden. Die Ergebnisse basieren sich auf einer Audioaufnahme eines englischen Textes. Die an der Pipeline durchgeführte Optimierung war somit erfolgreich. Es bleiben einige interessante Fragen offen. Wie sollte man zum Beispiel mit überlappenden Tastenanschlägen umgehen? Wenn die Leserlichkeit des Textes das Hauptziel ist, wäre die Entwicklung eines kontextbewussten Sprachmodells ein interessantes Forschungsgebiet.

Geclusterte UMAP-Darstellung von Mel-Frequenz-Cepstral-Koeffizienten, die aus Audioaufnahmen von Tastenanschlägen extrahiert wurden. Die von DBSCAN berechneten Cluster sind farblich kodiert und neben den Datenpunkten sind Ground-Truth-Labels angegeben.