Reconstruction of Texts by Keyboard Acoustic Emanations

Rajeev B N
M.Tech. Student, Department of Computer Science, UBDTCE, INDIA

***Abstract*- Any breach of privacy and security in a digital medium is a serious issue. Keyboard acoustic emanation one of many side channel attack. The sound from keystroke of physical keys input can be reconstructed to extract information without the awareness of the user from a system. In this paper such keyboard acoustic emanations achieved by the process of record sample, filter sample, peak detection and classification for basic keystroke recognition. Cluster keystrokes provide the initial guess of sequence, both language model and supervised classifier work repeatedly classify, spellcheck over the result then retrieve classifier with corrected labels. The improved method increases the accuracy of text recovery of supervised data. The acoustic data of keystrokes properties and recording limiting factors are explored.**

Index terms- Keyboard Acoustic Emanations, Keystroke Extraction, Feature Extraction, Cluster Keystrokes, Supervised Classifier

1. INTRODUCTION

The exchange of information and transfer of data is abundant in a computer or between the computers, which can be extracted with various methods. One such method is the keyboard acoustics method can be used to extract information from the target computer.

The overwhelming use of electronic devices by us today, used for most personal and sensitive information exchange and stored in such devices. Provision of security and privacy is achieved by encryption. Where it restricts the attacker by unauthorized access and data manipulate. Before encryption, the eavesdropping attacks were physical signals, like electromagnetic emanations. Whereas the latest electronic devices consist abundant of sensors like microphone, accelerometer, and gyroscope, GPS, biometric sensors, external peripherals, such as mice, keyboards, touch screens.

In this paper solely interest in acoustic emanations of keyboard keystrokes, when the user presses a key while being typed eavesdrops. Such attack retrieves what is being typed by the user, such data can be gathered by just using a microphone situated within the laptop or a pc. The idea behind acoustic emanations that each individual key pressed makes a sound different from one key to another. To the human ear, the differentiation of such individual key sound is not possible.

*Address correspondence to this author at the Department of xxxy, Faculty of xxx, xxx University, P.O. Box: 0000-000, City, Country; Tel/Fax: ++0-000-000-0000, +0-000-000-0000; E-mails: author@institute.xxx

The tool like a stethoscope is effective for listening heartbeat, which is inexpensive and cutting-edge technology, similarly, this eavesdropping is inexpensive and non-intrusive of physical space, the need is a computer in addition microphone. The physical breach into the system not necessary as the sound can be recorded by a distance, microphones are accurate and can record a range of surrounding sound without invasion.

This attack achieved not only in PC and laptops, but can also be extended to touchtone devices, mobile devices vibration, ATM keypads by the sound of keystrokes. Acoustic side channel attack is successful, when victim system typing keystrokes are recorded using the microphone, such collected sound information stream is processed to reconstruct typing input using supervised or unsupervised learning and machine learning techniques. The ultimate result obtained is a complete or partial reconstruction of actual typing input.

The limitation can be found only the recorded sound is from the situated microphone on a laptop, but this limitation can be overcome by smartphones

compromised microphone located in the victim's system location.

This paper present and explore acoustic eavesdropping attack by (i) overcoming the limitation of microphone location on the target device, and (ii) well trained limited amount of data is sufficient to achieve acoustic side channel attack.

2. RELATED WORK

Eavesdropping on keyboard input side channel attack has gained interest in the research area. Here the related previous work is overviewing attacks uses acoustic emanations to recover the victim's typed text.

Attacks Using Sound Emanations. Research on keyboard acoustic eavesdropping by Asonov and Agrawal [3] who showed that training a neural network on a specific keyboard, good performance can be achieved in eavesdropping on the input to the same keyboard, or keyboards of the same model. This work is proposed over the mechanical keyboard switches, which produces different acoustic signals than traditional keyboard like laptop and membrane PC keyboards. And typically used machine learning over-supervised and unsupervised learning techniques.

Supervised learning techniques require many labeled samples and rely on: (1) the specific keyboard used for training, and (2) the typing Overall, supervised learning approach provides very high accuracy. The disadvantage is obtaining labeled samples from the target system.

Unsupervised learning approaches can cluster together keys from sounds, or generate sets of constraints between different key-presses. The disadvantage is less effective when keyboard input is random. An alternative approach involves analyzing timing information.

Attacks Using Other Emanations. Other methods focused on keyboard eavesdropping via non-acoustic side-channels. Typing on mobile devices produces vibrations of the surface under the keyboard. These vibrations can be collected by an accelerometer. And other methods that rely on wi-fi signals, touch-sensitive pad,etc.

3. METHODOLOGY

The actual attack involves two phases: (i) data processing, and (ii) data classification. Each phase involves two steps:

1. Data processing includes data segmentation and feature extraction steps.
2. Data classification phase includes target-device classification and key classification steps

3.1 Data Processing Phase

The main goal in this phase is to extract meaningful features from acoustic information gathered while emanations. The first step is data segmentation to isolate distinct keystroke sounds within the recording. Using these sound samples, the derived values (called features) that represent properties of acoustic information. This step is commonly referred to as feature extraction.

Data Segmentation

Perform data segmentation according to the following observation: the waveform of a keystroke sound presents two distinct peaks, shown in Figure 1. These two peaks correspond to the events of (1) the finger pressing the keypress peak, and (2) the finger releasing the key – release peak. use the press peak to segment the data and ignore the release peak. because the former is generally louder than the latter and is thus easier to isolate, even in very noisy scenarios.

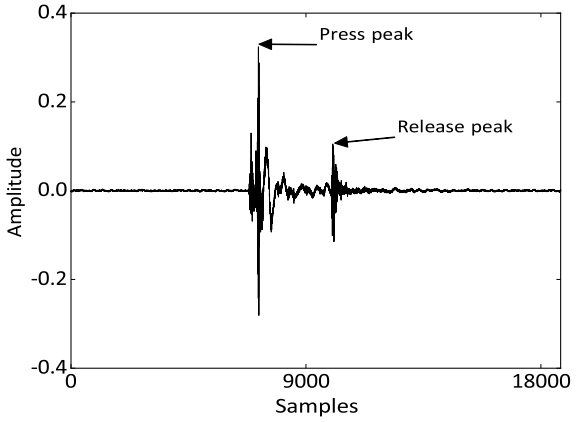

Figure 1: Waveform of the "A" key

Feature Extraction

As features, extract the mel-frequency cepstral coefficients (MFCC). These features capture the statistical properties of the sound spectrum, which is the only information that is used.

3.2 Classification Phase

In this phase, apply a machine learning algorithm to features extracted in the Data Processing phase, in order to perform:

- Target-device classification using all keystroke sound emanations that the attacker received.
- Key classification of each single keyboard key of the target device, by using sound emanations of the keystrokes. Each classification task is performed depending on the scenario.

Target-device Classification

The task of target-device classification as a multi-class classification problem, where different classes correspond to different target-device models known to the attacker.

Key Classification

The key classification to be a multiclass classification problem, where different classes correspond to different keyboard keys. To evaluate the classifier's quality using accuracy and top-n accuracy measures. Given true values of k, accuracy is defined in the multiclass classification case as the fraction of correctly classified samples over all samples. Top-n accuracy is defined similarly. The sample is correctly classified if it is present among the top n guesses of the classifier.

4. DATA COLLECTION

Collected data from five distinct users. For each user, the task was to press the keys corresponding to the English alphabet, sequentially from "A" to "Z", and to repeat the sequence ten times, first by only using the right index finger (this is known as Hunt and Peck typing, referred to as HP from here on), and then by using all fingers of both hands.

5. EVALUATION

We compare HP and Touch typing data in Figures 2 and 3. Figure 2 attack accuracy as a function of the number of guesses, and Figure 3 highlights top-1 and top-5 accuracies. We observe that S&T attack is as accurate with Touch as with HP typing data, within best 4 guesses. From the 5th guess onwards, there is a slight advantage with HP typing data; however, the difference is very small – around 1.1% in the worst case.

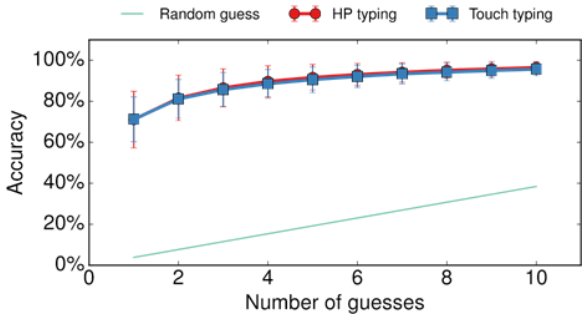

Figure 2: Average accuracy of HP and Touch typing data

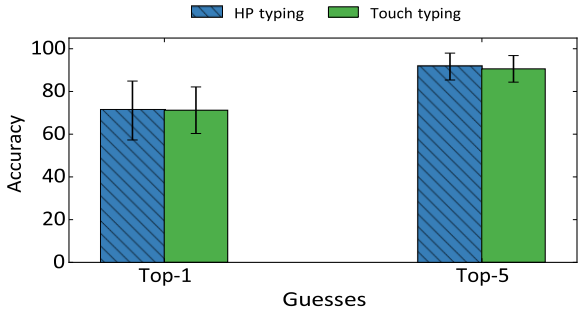

Figure 3: top-1 and top5 accuracies of HP and Touch typing data.

6. CONCLUSION

In this paper explored acoustic emanations of keyboard-like input devices to recognize the input being typed by the victim. After providing a detailed description of the basic attack on a PC keyboard, we successfully applied this attack to other types of push button input devices, such as notebook keyboards. A sound-free (non-mechanical) keyboard is an obvious countermeasure for the attack. However, it is neither comfortable for users nor cheap. We identified possible reasons that cause the keys to sound slightly different to draw preliminary conclusions that produce indistinguishable clicks can be constructed. The work presented in this paper points to many avenues for further research.

REFERENCES

[1] Li Zhuang, Feng Zhou, and J. D. Tygar. "Keyboard Acoustic Emanations Revisited". In: ACM Trans. Inf. Syst. Secur. 13.1 (Nov. 2009), 3:1–3:26. issn: 1094-9224. doi: 10.1145/1609956.1609959. url: http://doi.acm.org/10.1145/1609956.1609959.

[2] Andrea Barisani and Daniele Bianco. “Sniffing Keystrokes With Lasers and Voltmeters”. In: (2009). http://dev.inversepath.com/download/ tempest/blackhat_df-whitepaper.pdf.

[3] Andrew Kelly. “Cracking Passwords using Keyboard Acoustics and Language Modeling”. In: (2010). http://www.inf.ed.ac.uk/ publications/thesis/online/IM100855.pdf.

[4] D. Asonov and R. Agrawal. “Keyboard acoustic emanations”. In: Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on. 2004, pp. 3–11. doi: 10.1109/SECPRI.2004.1301311.

[5] Li Zhuang, Feng Zhou, and J. D. Tygar. “Keyboard Acoustic Emanations Revisited”. In: Proceedings of the 12th ACM Conference on Computer and Communications Security. CCS ’05. Alexandria, VA, USA: ACM, 2005, pp. 373–382. isbn: 1-59593-226-7. doi: 10.1145/1102120.1102169. url: http://doi.acm.org/10.1145/1102120. 1102169.

[6] Yigael Berger, Avishai Wool, and Arie Yeredor. “Dictionary Attacks Using Keyboard Acoustic Emanations”. In: Proceedings of the 13th ACM Conference on Computer and Communications Security. CCS ’06. ACM, 2006, pp. 245–254. isbn: 1-59593-518-5. doi: 10.1145/1180405.1180436. url: http://doi.acm.org/10.1145/1180405. 1180436.

[7] C.E. Shannon. “Prediction and entropy of printed English”. In: Bell System Technical Journal, The 30.1 (1951), pp. 50–64. issn: 00058580. doi: 10.1002/j.1538-7305.1951.tb01366.x.

[8] Bernard EM Jones. “Exploring the role of punctuation in parsing natural text”. In: Proceedings of the 15th conference on Computational linguistics-Volume 1. Association for Computational Linguistics. 1994, pp. 421–425.

[9] Teresia R Ostrach. “Typing speed: How fast is average”. In: Five Star Staffing, Inc., Orlando, FL (1997). IJRASET24289