Poster: TapSnoop – Inferring Tapstrokes from Listening to Tap Sound on Mobile Devices

Hyosu Kim[1], Daehyeok Kim[1], Byunggill Joe[1], Yunxin Liu[2], Insik Shin[1]

[1]School of Computing, KAIST; [2]Microsoft Research

{hskim, dkim, byunggill}@cps.kaist.ac.kr, yunxin.liu@microsoft.com, insik.shin@cs.kaist.ac.kr

1. INTRODUCTION

Mobile device users tap a touch-screen for entering sensitive information such as passwords and PIN numbers, and many works have proposed an attack model snooping such tapstrokes especially with the use of built-in sensors [1, 2, 3]. These studies raise the serious security concerns with the following attack scenario. A malicious application runs in the foreground as a normal chatting application, collecting a training set of sensor data generated from tapstrokes. While a user types her credit card number for purchasing something on a shopping application, it sneakingly takes sensor streams in the background and infers the tapped number by comparing the streams with the training data.

However, in practice, the existing works have shown a limited inference accuracy, due to the following reasons. First, the intensity of tapstrokes is typically much low, resulting in a subtle change on sensor data. Second, mobile devices generally come with small on-screen keyboards where keys are very close to each other. Thus, it is essential to perform fine-grained tapstroke localization. Third, each mobile device has its own hardware characteristics with regard to screen's size and thickness, as well as built-in sensor's sensitivity. This inherently leads to different characteristics of tapstrokes for different devices. Last, smartphone users can use their devices in various places with different noise levels, while moving around. Therefore, it should be able to infer tapstrokes robustly against the environmental changes.

2. TAPSNOOP FRAMEWORK

We develop TapSnoop which allows an attacker to accurately detect and localize each tapstroke in mobile environments, by listening to sounds generated from the tapstrokes, called *tapsound*.

The key underlying technologies for enabling TapSnoop are as follows (see Figure 1). First, for the accurate localization, we take a deep exploration on the characteristics of tapsounds, in terms of intensity and discrimination. We leverage such observations to design and optimize acoustic features not only for differentiating tapsound and noise, but also for distinguishing each individual tapsound accurately. Second, we address the issue of device heterogeneity, by finding and adapting to device-specific characteristics. Last, we compensate for the lack of noise robustness with the use of motion sensors and stereo recording.

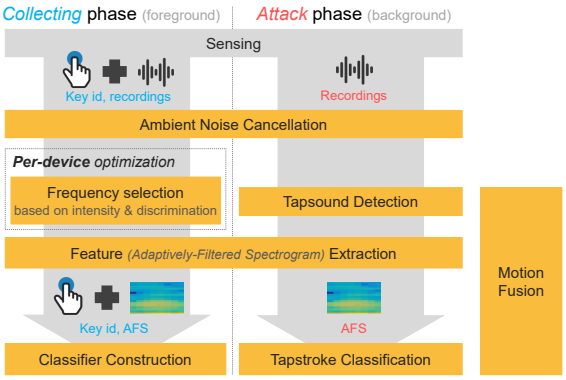

Figure 1: Overall procedures of TapSnoop. The whole set of procedures is performed for each device independently.

We evaluate the performance of TapSnoop with an extensive evaluation collecting data from 10 real-world users in various scenarios (i.e., number pad/qwerty keys, device holding styles, and noise). Our evaluation results show that TapSnoop achieves a high degree of accuracy in both detection (89.0% on average) and localization (92.1% and 78.7% for each type of keyboard), meaning that it outperforms all existing inference models. Moreover, with a moderate level of noise, it provides a similar degree of classification accuracy to the result obtained in a virtually noise-free environment.

3. ACKNOWLEDGMENTS

This work was supported by ICT/SW Creative research program (2015-R2215-15-1019) of IITP, Korea, and Microsoft Research.

4. REFERENCES

[1] L. Cai and H. Chen. Touchlogger: inferring keystrokes on touch screen from smartphone motion. In *Proc. HotSec*, 2011.

[2] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R. R. Choudhury. Tapprints: your finger taps have fingerprints. In *Proc. ACM MobiSys*, 2012.

[3] S. Narrain, A. Sanatinia, and G. Noubir. Single-stroke language-agnostic keylogging using stereo-microphones and domain specific machine learning categories and subject descriptors. In *Proc. ACM WiSec*, 2014.

MobiSys'16 Companion June 25-30, 2016, Singapore, Singapore.

ACM ISBN 978-1-4503-4416-6/16/06.

DOI: http://dx.doi.org/10.1145/2938559.2938595