Keystroke recovery using mobile phone accelerometers

Akshay Mittal
Princeton University

Wathsala Vithanage
Princeton University

Stephen Lin
Princeton University

Jennifer Guo
Princeton University

ABSTRACT
[to - fill]

1. INTRODUCTION

Mobile phones [1] are becoming increasingly powerful devices. In addition to being able to run applications ranging from email clients to web browsers, a progressively sophisticated set of sensors are enabling these devices to more actively interface with the world around them. From gestures captured by accelerometers for games to augmented reality applications displaying metadata tags on video from the camera in real-time, mobile phones are becoming adept at capturing and harnessing rich features and data from their surroundings. Unfortunately, the array of sensors in these devices can also be used in unintended ways. As many have suggested, malware could potentially gain access to a mobile phone's camera to take photos or video of the owner and their surroundings [2]. In cases where the camera may not be pointed at an interesting target, a malicious application could instead attempt to activate the device's microphone and record ambient sounds or syphon GPS data to track the target's location [3, 4, 5, 6]. Recognizing the potential for the leakage of sensitive information, many modern mobile phone operating systems provide mechanisms by which access to such sensors is protected by explicit permission from the user. For instance, the manifest files included with every Android application provide an unambiguous list of all of permissions an application may ever request at installation time. Should an application not request access to these resources or the user deny the application such rights, the application will not be able to potentially abuse these resources. However, access to all of the sensors contained in these devices are not so tightly controlled.

In this paper, we demonstrate that unfettered access to the accelerometers available on many mobile phones can allow for significant unintended leakage of information from a user's environment. We show that a malicious application with access to the accelerometer feed can record and reconstruct the keypresses made on a nearby keyboard based solely on the observed vibrations. We develop profiles for keypress events using boosted Random Forests, which creates an abstract representation of the relationship between the keystroke signal and the alphabet typed. We then recover the typed content by translating from our intermediary form to English words using a number of different dictionaries. Such tasks are not a trivial application of standard techniques, especially when compared to previous efforts in this space. Specifically, we must overcome much lower sensor sampling rates than has been experienced in the related acoustic and electromagnetic-based eavesdropping attacks, which makes deciphering individual keypresses extremely difficult.

Through this, we make the following contributions in this paper:

1. **Develop an infrastructure for characterizing keypress vibrations**: We capture, analyze and develop profiles of keypress events on a nearby keyboard based on the vibrations created when they are pressed. Our inputs are then processed using a set boosted Random Forests to create an intermediary representation, which is combined with candidate dictionaries to successfully recover words at rates as high as __

2. **Dataset made publicly available**: To the best of our knowledge, there does not exists a dataset with the keystrokes for the vibrations recorded using an accelerometer. In this paper, we demonstrate we construct the dataset of keystroke vibrations, recorded using the accelerometer, present in a smartphone and make the dataset publicly available to enhance further research on this topic. Given the widespread about security breaches and email leaks, we perceive this to be of great importance in motivating the mobile operating system manufacturers to restrict the usage of accelerometers to permitted applications only.

Note that our approach is greatly influenced by the work of Marquardt *et. al* [1] and we present key differences with our approach.

2. RELATED WORK

3. THREAT MODEL

4. FRAMEWORK DESCRIPTION

5. IMPLEMENTATION

6. EXPERIMENTAL RESULTS

7. CONCLUSIONS

This paragraph will end the body of this sample document. Remember that you might still have Acknowledgments or Appendices; brief samples of these follow. There is still the Bibliography to deal with; and we will make a disclaimer about that here: with the exception of the reference to the LaTeX book, the citations in this paper are to articles which have nothing to do with the present subject and are used as examples only.

8. ACKNOWLEDGMENTS

This section is optional; it is a location for you to acknowledge grants, funding, editing assistance and what have you. In the present case, for example, the authors would like to thank Gerald Murray of ACM for his help in codifying this *Author's Guide* and the **.cls** and **.tex** files that it describes.

9. REFERENCES

[1] Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp) iphone: decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011.

[2] Zhu Cheng. Mobile malware: Threats and prevention. *McAfee Avert*, 2007.

[3] David Dagon, Tom Martin, and Thad Starner. Mobile phones as computing devices: The viruses are coming! *Pervasive Computing, IEEE*, 2004.

[4] Liang Cai, Sridhar Machiraju, and Hao Chen. Defending against sensor-sniffing attacks on mobile phones. In *Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds*, pages 31–36. ACM, 2009.

[5] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol Sheth. Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones. In *OSDI*, 2010.

[6] Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. Pios: Detecting privacy leaks in ios applications. In *NDSS*, 2011.

APPENDIX

A. APPENDIX SECTION

Lorem ipsum dolor sit amet, et alienum salutatus cotidieque has, per an fugit dictas saperet. Cu nec odio denique, qui at assum omnium. Nihil maluisset vituperatoribus eu ius, insolens facilisis te eos. Enim elit appetere ne has, cu eos delectus inciderint. Nam ea lucilius efficiendi.

A.1 Appendix Subsection

Lorem ipsum dolor sit amet, et alienum salutatus cotidieque has, per an fugit dictas saperet. Cu nec odio denique, qui at assum omnium. Nihil maluisset vituperatoribus eu ius, insolens facilisis te eos. Enim elit appetere ne has, cu eos delectus inciderint. Nam ea lucilius efficiendi.