INDIAN INSTITUTE
OF INFORMATION
TECHNOLOGY, KOTA

Indian Institute of Information Technology, KOTA

Exploiting user privacy using sensor data extracted from smart devices

Authors :
Puneet Saluja
Tanmay Sonkusle
Krishna Sharma

Supervisor:
Dr. Smita Naval

May 1, 2018

Acknowledgement

We are profoundly grateful to Dr. Smita Naval for her expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. Her timely and efficient contribution helped us shape our work into its final form and we express our sincerest gratitude for her assistance in any way that we may have asked. We appreciate her guidance in our project that has improved our project many folds, thanks for the comments and advise.

Puneet Saluja
Tanmay Sonkusle
Krishna Sharma

Contents

Acknowledgement **i**

Introduction **1**

1 Data Acquisition **3**

1.1 Une section 3

1.2 Input Action Detection 4

Conclusion **7**

List of Figures

1.1 Exemple d’image au format JPG. 4

1.2 Exemple d’image au format JPG. 5

Liste des sigles et acronymes

ASK	*Amplitude Shift Keying*
AWGN	*Additive White Gaussian Noise*
BABG	Bruit Additif Blanc Gaussien
BCJR	*Bahl, Cocke, Jelinek, Raviv*
BER	*Binary Error Rate*
BFDM	*Biorthogonal Frequency Division Multiplexing*

Introduction

Internet of things (IoT), which adds sensors and internet capability to everyday physical objects has transformed the lives of individuals dramatically. The real-time insights and analysis of IoT devices delivers ecient and smart decisions faster. Nowadays, users rely on these devices to carry their personal data and day-to-day activity information. Now, this data can be sensitive if it contains credentials for an email account, bank details, medical information to name a few. To capture this information, IoT devices utilize various sensors (Analog and Digital). An attacker can exploit this sensor data to extract the private details of the user as it has been seen in the past that security restrictions on sensors are negligible. Therefore, the sensor data can be exploited to threaten user's privacy.

Today's smart devices are packed with nearly 14 different type of sensors that produce raw data on motion, location and the environment around us. An attacker can use sensors like Accelerometer and gyroscope to infer user's input keystroke, Ambient light sensor to infer user's pin input. Currently, Android sensor manager asks for permission to access few sensors only such as Camera, GPS and Microphone but it does not impose permission on sensors like Accelerometer, Gyroscope, Magnetometer and Proximity Sensor. Android allows third-party applications to read and access sensor data without any limitations.

In our project we have performed two experiments to exploit the privacy of user using sensors in smart devices. The main observation that we have made during our work is that touch input actions at different position will bring different level of motion and posture change in smart-phones. In first experiment, we have used accelerometer sensor data to detect the motion activity of a user, if he is walking or stationary. In our second experiment we have demonstrated that accelerometer and gyroscope sensor data can be used to perform a side channel attack against secure input. We have used these two sensors to learn user PIN input and recognize each individual key-press with an accuracy of about 42%.

Chapter 1

Data Acquisition

1.1 Une section

For our experiments, we developed an android application which records accelerometer and gyroscope sensor data. The application can run in background and can be used to log the data from both sensors into a csv file. Since, android does not impose any security restriction on these two sensors, no permission is asked for accessing these two sensors at the time of installation.

Experiment 1 :

In Experiment 1, we have used Samsung Galaxy J2 2016 device to collect accelerometer data for detecting user motion activity : stationary or walking. The application logs the averaged value of the acceleration force applied on all three physical axes in m/s2 over time interval of 1 second. We collected data from 10 different users in hand held scenario for both stationary and walking.

Experiment 2 :

In Experiment 2, we have used One Plus 5 device to collect both accelerometer and gyroscope data for inferring user PIN input and to recognize each and individual key-press. The accelerometer gives the motion data along the three axis x, y and z. The gyroscope gives the orientation data for the three axis : pitch(x axis), roll(y axis) and azimuth(z axis). We collected this data from 10 different users where each user entered 50 random pins of four digit each and we allowed users to choose these pins at random of their choice.

1.2 Input Action Detection

To know at what instance of time, a key has been pressed, we found out the squared sum of the accelerometer readings and plotted a graph along with timestamp.

$$\mathrm{AccSum} = \mathrm{x}^2 + y^2 + z^2$$

where x, y and z are the readings of the accelerometer in the x, y and z axis respectively. This squared sum will give the magnitude of external force F on the touchscreen. The observed graph for the squared sum of accelerometer readings vs timestamp is as follows:

Figure 1.1: Exemple d'image au format JPG.

Though the graph had some peaks but these peaks were not quite distinguishable. Also, acceleromter sensor captures the raw data which also includes gravity component which makes it quite difficult to accurately infer the motion changes of the smartphones. Gravity component can be considered as a constant component. Thus, some filtering technique need to be employed in order to remove the gravity component from the accelerometer data.

We looked into the Android Developer documentation for the implementation of this filter. We then performed all the calculations within the application and now we captured the accelerometer readings without any gravity component. Once again we plotted the graph of the squared sum of accelerometer readings vs timestamp and this time we observed distinguished peaks at each keypress event. This curve can be used to accurately measure the occurrence of input actions since it exhibits periodic and obvious peaks.

Figure 1.2: Exemple d'image au format JPG.

Conclusion

In this Project, we have presented a study of analyzing accelerometer and gyroscope data to infer user input on an android smartphone. We were able to detect user motion activity (walking/stationary) using accelerometer data with an accuracy of 94%. In our second experiment we were correctly able to infer each individual key press on a number pad with an accuracy of 43%. We also examined size of training data size on performance of our model and found that accuracy increases with the increase in the training data size. We also observed position inference accuracy against different sampling rates of sensor data and observed input action detection were quite accurate in case of high sampling rate.

This apppli

Bibliography

1 Adam J. Aviv, Benjamin Sapp, Matt Blaze and Jonathan M. Smith,“Practicality of Accelerometer Side Channels on Smartphones", in *Proceedings of the 28th Annual Computer Security Applications Conference*, Pages 41-50.

2 ChaoShen, Shichao Pei, Zhenyu Yanga, Xiaohong Guan, “Input extraction via motion-sensor behavior analysis on smartphones", Volume 53 Issue C, September 2015, Pages 143-155.

3 Zhi Xu, Kun Bai, Sencun Zhu, “TapLogger: Inferring User Inputs On Smartphone Touchscreens Using On-board Motion Sensors", in *the Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, Pages 113-124.

4 Xiangyu Liu, Zhe Zhou, Wenrui Diao, Zhou Li, Kehuan Zhang, “When Good Becomes Evil: Keystroke Inference with Smartwatch", in *the Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Pages 1273-1285.

5 He Wang, Ted Tsung-Te Lai, Romit Roy Choudhury, “MoLe: Motion Leaks through Smartwatch Sensors", in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, Pages 155-166.

6 Raphael Spreitzer, “PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices", in *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones and Mobile Devices.*

7 Philip Marquardt, Arunabh Verma, Henry Carter, Patrick Traynor, “iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers", in *Proceedings of the 18th ACM conference on Computer and communications security*, Pages 551-562.

8 Amit Kumar Sikder, Hidayet Aksu, and A. Selcuk Uluagac, “6thSense: A Context-aware Sensor-based Attack Detector for Smart Devices", in *the Proceedings of the 26th USENIX Security Symposium, 2017.*

9 Yan Michalevsky and Dan Boneh, “Gyrophone: Recognizing Speech from Gyroscope Signals", *Proceedings of the 23rd USENIX Security Symposium, 2014.*