EXPLOITING USER PRIVACY USING SENSOR DATA EXTRACTED FROM SMART-DEVICES

Project-1 (CSD300)

Presented By :
Puneet Saluja (2015KUCP1019)
Tanmay Sonkusle (2015KUCP1023)
Krishna Sharma (2015KUCP1040)

Supervisor:
Dr. Smita Naval

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, KOTA

May 3, 2018

Overview

INTRODUCTION

- Internet of things (IoT), which adds sensors and internet capability to everyday physical objects has transformed the lives of individuals dramatically.
- Nowadays, users rely on these devices to carry their personal data such as email account, bank details, medical information to name a few.
- An attacker can exploit this data to extract the private details of the user as it has been seen in the past that security restrictions on sensors are negligible.

Permission required	**Permission not required**
Camera, GPS, Microphone	Accelerometer, Gyroscope, Magnetometer, Proximity Sensor

OBJECTIVES

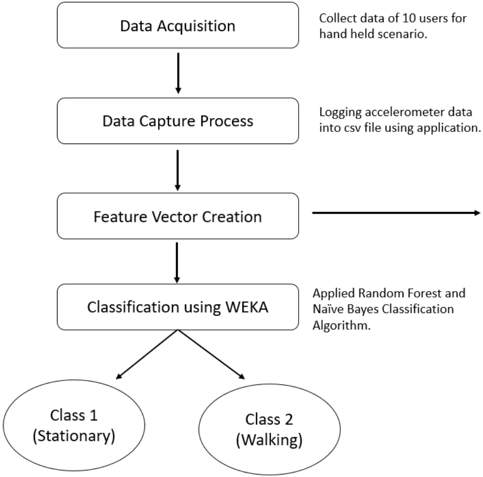
- Exploiting the privacy of user using sensors in smart devices.
- Create awareness among users regarding privacy breach through sensors.
- Demonstrate with the help of experiments that user's private information can be leaked through sensor data.

LITERATURE REVIEW [1/2]

Paper	Objective
Raphael spreitzer *et. al.* [6] (SPSM, 2014)	Infer user PIN input using ambient light sensor.
Chao shen *et. al.* [2] (2015)	Infer user input using accelerometer and magnetometer.
Arunab verma *et. al.* [7] (CCS, 2014)	Decoding vibrations from nearby keyboard using acceleromter sensor.
Dan Boneh *et. al.* [9] (CCS, 2014)	Recognizing Speech from Gyroscope Signals.
Xiangyu liu *et. al.* [4] (CCS, 2015)	Investigate security issues in smart watches using accelerometer and microphone.

LITERATURE REVIEW [2/2]

Paper	**Objective**
He wang *et. al.* [5] (MobiCom, 2015)	Mine acceleromter and gyroscope data from smart watches to infer user input.
Adam J. Aviv *et. al.* [1]	Learn user tap and gesture-based input using accelerometer sensor data.
Zhi Xu *et. al.* [3]	Infer password of screen lock using motion sensors.
Hidayet Aksu *et. al.* [8] (USENIX, 2017)	A Context-aware Sensor-based Attack Detector for Smart Devices.



	T1.x	T1.y	T1.z	.	.	Class
User1						W
User2						S
User3						S
.						.
.						.
User10						W

Feature Vector

USER ACTIVITY DETECTION [2/2]

- Device Used: Samsung Galaxy J2 2016.
- Sensor Used: Accelerometer.

Data Collection:

- Developed an Android application to log sensor data without any user permission.
- Collected data from 10 different volunteers for activities: Stationary, Jogging, Walking upstairs, Walking downstairs, Normal walking.

- Used 10 fold cross-validation to train and test data using different classification technique such as Random Forest, Naive Bayes on WEKA.
- Random Forest correctly classified user's activity data with the best accuracy of 94%.

INPUT ACTION DETECTION [1/2]

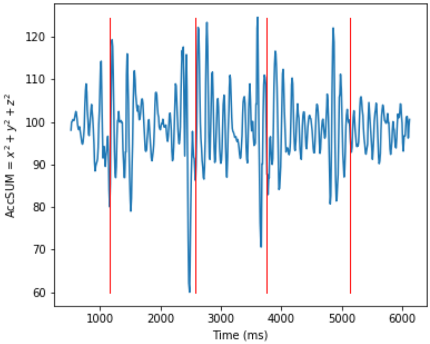
- Device Used: One Plus 5.
- Sensor Used: Accelerometer and Gyroscope.

Data Collection:

- Developed an Android application to log sensor data without any user permission.
- The application can run in background and can be used to log the data from these sensor in .csv file.
- Since, android does not impose any security restriction on these sensors hence, no permission is required at the time of installation.
- Collected data from 10 different users, where each user entered 50 random pins of 4 digit.

INPUT ACTION DETECTION [2/2]

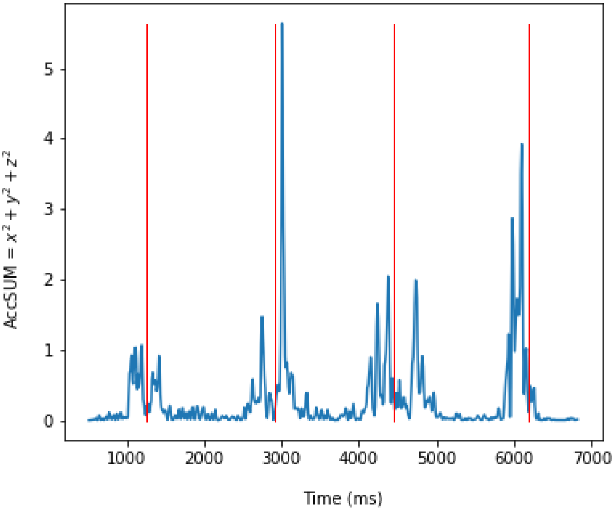
- To accurately detect the occurrence of an input action, we used $AccSum = x^2 + y^2 + z^2$
  where x, y, z are the accelerometer values in three axis.
- AccSum represents the magnitude of the external force F on the touch screen.



REMOVAL OF GRAVITY COMPONENT [1/2]

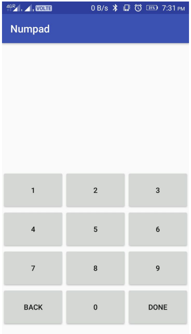
- Raw accelerometer data include the gravity component, which make it hard to accurately reflect the motion change of smart-phone.
- Gravity component can be considered as the constant component and acceleration data as alternating component.
- Thus, some filtering technique is needed in order to remove the gravity component from acceleration data.
- We plot a graph of AccSum vs time-stamp and observed distinguished peaks at each key press event.
- This curve exhibits periodic and obvious peaks, which can be used to measure the occurrence of the input action with a high accuracy.

REMOVAL OF GRAVITY COMPONENT [2/2]



SCREEN DIVISION

- A user might enter valuable information such as password, pin via an interface from smart-phone.
- These interface are usually composed of similar layout which include one display interface and one input interface.
- Thus, this input can be easily divided into different areas, each of which corresponds to a singe digit on a number pad.



OBSERVATIONS AND ASSUMPTIONS

- We observed a right-handed person will slightly tilt the smart-phone towards right side while he enters the pin digits in the middle and left column i.e 1, 2, 4, 5, 7, 8 because while making any input user will try to push the smart-phone display towards his thumb.
- We assumed that user holds smart-phone in his right hand while making any pin input.
- We ignored the case when laying on a flat surface because in this case there will be only minor changes in the readings of the sensor data.

INPUT MAPPING

- The input interface usually consist of several buttons for user to enter information.
- One can obtain the tapped button by simply mapping the inferred position to input interface.
- During the testing phase, we recorded the pressed number and labeled it as class corresponding to the readings of sensor data.

FEATURE EXTRACTION

- To pre-process the raw data, we calculated Z-score and applied mean normalization on data.
- Feature vector includes the readings of the accelerometer and gyroscope with timestamp as a feature.
- It also includes additional descriptive-statistical attributes of A_x, A_y, A_z, G_x and G_y like min, max, median, kurtosis, mean, standard-deviation and variance.

TRAINING AND TESTING

- Used the Random Forest Classifier to train and test the data using 10 fold cross-validation on WEKA.
- Model correctly predicted the entered digits with an accuracy 57.3.
- input: 2 4 8 3 5 9 6
  1st attempt predictions: 2 4 8 3 5 6 5
  2nd attempt predictions: 2 4 8 3 5 3 6
- It is observed that digits 5, 8, and 9 are hard to predict for a right hand user.

CONCLUSION

- We have presented a study of analyzing accelerometer and gyroscope data extracted from smart-devices to infer user input on an android smart-phone.
- 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 57.3%.
- With this work we have successfully demonstrated that the leaked information from these sensors can act as a side channel to compromise user's privacy.

FUTURE WORK

- This work could be extended in future to infer other kinds of attack like inferring user input text.
- We can use some more sensors such as magnetometer and ambient light sensor or use combination of these sensors to carry out more attack.

REFERENCES[1/2]

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.

REFERENCES[2/2]

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*.