7th National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(1st and 2nd March 2019)
International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

An Analysis of Sensor Based PIN and Password Detection Techniques

Aditi Patil[1], Saniket Kudoo[2]
Department of Computer Engineering, Mumbai University, MUMBAI

Abstract*—Smartphones are equipped with various sensors intended to provide more salient features to end users to interact with their real-world surroundings. Sensors are employed in numerous devices such as smartphones, computers, television and microwave. Internal sensors play a vital role in handling sensitive information of user in computer security. Smartphones consist of plethora of sensors such as GPS, proximity, pedometer, camera, NFC, microphone, magnetometer, gyroscope and accelerometer. Many mobile applications and websites need not seek permission to access most of these sensors. With the use of malicious programs, sensor's data can be recorded without notifying the user. PINs and graphical pattern passwords can be guessed using the sensors. This paper aims to provide a study of different techniques used for guessing PINs and Password using sensors.*

Keywords*— *Password, Pattern, PIN, Sensors, Smartphones.

I. INTRODUCTION

The tremendous rise in use of smartphones increases the use of various sensors. Cell phones come in great use in day to day lifestyles. People use smartphones for even the simplest task. Smartphone devices and devices with numerous sensors have brought a revolution since then. These devices with vital sensors help to overcome the traditional use of separate devices. Many smartphone devices provide a security for unlocking the device such as entering PIN or pattern lock. Some devices even perform face detection and finger print capture. The present cell phones are delivered with different inserted movement sensors, for example, the accelerometer, gyroscope, and orientation sensors [5]. These movement sensors are valuable in supporting the versatile UI development and movement based commands. Nonetheless, they additionally bring potential dangers of spilling client's private data as they permit outsider applications to screen the movement changes of cell phones. These sensors create a huge database which resides on the devices. Such smart devices reveal data of the user to the third parties.

The PIN used for password protection or to unlock a device usually consists of a sequence of numbers. Most of the time, these numbers repeat. Similarities can be found even in the combination of characters of the password. With the use of different trojan applications, the PIN and passwords of the user operating the device can be tracked down. Various Machine Learning and Deep Learning approaches are used to learn the patterns of the password entries. The behavior of the password pattern can be observed using different sensors residing on the devices. Based on the study and use of such trojan applications, the PIN and password can be discovered in very few attempts. Hardware as well as software manipulation are combined together to detect the private data generated by the sensors.

II. RELATED WORKS

A model based on machine learning was developed to read the accelerometers that are not dependent on sample rate and was also based on signal processing and polynomial fitting techniques [5]. They even represented that there is some sort of consistency between the users and the devices. The smartphones present in the market seek permission for accessing the sensor's data, and the permission asked is for accessing all of the sensor's data. Permission cannot be granted by excluding one or two requests. All the sensors have to be allowed for access. For PINs and password patterns, the accelerometer sensor plays a vital role. Inputs given to the device such as touching, tapping, swiping and other gestures reveal more information about the password [6]. The way in which the device was held, the rotation of the device, the light on the screen, the pressure applied is used to detect the behavior of the user's pattern.

Sensitive information of the sensors is shared with the third party applications without the consent of the user. In most cases, the user is lured to install trojan applications or carried away with fake interface. So as to construct the component vector as the

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

contribution to our classifier calculation, they think about both time area and recurrence space highlights. They enhance their proposed highlight vectors by including some increasingly intricate highlights, for example, the connection between the estimations. This expansion enhances the outcomes, unique groupings gotten from the gathered information incorporate introduction (ori), increasing speed (acc), quickening including-gravity (accG), also, revolution rate (rotR) with three arrangements (either x, y also, z, or α, β and γ) for every sensor estimation. As a pre-handling step and so as to expel the impact of the underlying position and introduction of the gadget, we subtract the underlying incentive in each grouping from consequent values in the grouping [7].

III. APPROACH FOR ATTACKS

They consider an aggressor who needs to get familiar with the client's PIN tapped on a delicate console of a cell phone through side channel data. We consider (digit-just) PINs since they are well known accreditations utilized by clients for some reasons for example, opening telephone, SIM PIN, NFC installments, bank cards, other saving money administrations, gaming, and other customized applications, for example, social insurance, protection, and so forth. Not at all like comparative works which need to pick up the entrance through an introduced application their assault does not require any client consent. So as to reveal when the client enters his PIN, we need to arrange his touch activities, for example, snap, scroll, and zoom.

They have just appeared in TouchSignatures that with a similar sensor information and by applying characterization calculations, it is conceivable to adequately recognize client's contact activities. Here, they think about a situation after the touch activity characterization. As such, our assailant as of now realizes that the client is entering his PIN. Also, except if unequivocally noted, we consider a conventional assault situation which isn't client dependant. This implies we try not to need to prepare our machine learning calculation with indistinguishable client from the subject of the assault. Rather, they have a one-round preparing stage with information from different intentional clients, and utilize the got prepared calculation to yield other clients' PINs later. This methodology has the advantage of not expecting to trap singular clients to gather their information for preparing.

IV. WEB PROGRAM IMPLEMENTATION

M. Mehrnezhad, et. al. [7] have mentioned that they actualized a website page with implanted JavaScript code so as to gather the information from intentional clients. Our code registers two audience members on the window object to approach introduction and movement information independently. The occasion handlers characterized for these designs are named Device Orientation Event and Device Motion Event separately. On the customer side, we built up a GUI in HTML5 which demonstrates irregular 4-digit PINs to the clients and enacts a nummpad for them to enter the PINs as appeared alongside their related marks which are the digits of the entered PINs. They executed our server program utilizing Node.js (nodejs.org). Our code sends the introduction and movement sensor information of the cell phone to our NoSQL database utilizing MongoLab (mongolab.com, web based administration for MongoDB). At the point when the occasion audience fires, it sets up an attachment by utilizing (socket.io) between the customer and the server and always transmits the sensor information to the database. Both Node.js and MongoDB (as an archive situated database) are known for being fit for supporting information concentrated applications in continuous.

FIGURE 1. PIN Protection

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

They executed our server program utilizing Node.js (nodejs.org). Our code sends the introduction and movement sensor information of the cell phone to our NoSQL database utilizing MongoLab (mongolab.com, web based administration for MongoDB). At the point when the occasion audience fires, it sets up an attachment by utilizing (socket.io) between the customer and the server and always transmits the sensor information to the database. Both Node.js and MongoDB (as an archive situated database) are known for being fit for supporting information concentrated applications in continuous.

V. ANALYSIS

Sensitive information leaked without the user's consent is never revealed. The user is lured into a fake interface. In most cases, trojan applications are installed on the devices. These applications reveal sensitive data of the user to the third party applications. Access of the sensor's data is not provided to the applications residing on the device. Different applications have a different approach. Every pattern of the user's behavior is noted and studied minutely. The machine learning and deep learning algorithms are used to study and analyze the patterns of the user's inputs. Different parameters are observed and analyzed for password detection. The input parameters such as time taken by the user, light of the device, level of brightness, font, speed of typing, rotation, view mode, touch points, camera, and many more are taken into account and studied well. According to the view mode of the device, for example, horizontal mode, the keyboard displayed will vary from that of the vertical display. The position of the touch gestures on the screen while entering a PIN, password or drawing the pattern are studied and used for analyzing the input data. Most of the passwords and PINs are common and find a match easily, using a huge database. The passwords can be guessed or detected within 3 attempts with a great accuracy. Security or privacy of the user's data needs to be changed or altered with regular time intervals. Sensor based analysis of sensitive data overcomes the Shoulder tapping method.

VI. CONCLUSION

While the applications depending on devices detecting are blasting, the security and protection issues identified with such applications are not surely known yet. The extreme dependency of the smart devices on the on-board sensors tend to invoke high threat to the data and the user's privacy. Various techniques for training the models to detect the PIN and password within 5 attempts with a higher accuracy are applied numerously. Artificial Intelligence helps learn the patterns to study the approach of user's input. A more secure password would be relevant. Two factor authentication, biometric authentication and face detection can be used to enhance the security and protection of PIN and passwords.

REFERENCES

[1] C. Ronao, S. Cho, "Human activity recognition with smartphone sensors using deep learning neural networks", Expert Systems with Applications, 2016, pp 235-244.

[2] R. Spreitzer, "PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices", In Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices, 2014, pp 51-62.

[3] N. Zheng, K. Bai, H. Huang, "You Are How You Touch: User Verification on Smartphones via Tapping Behaviors", 14th Proceedings of IEEE 22nd International Conference on Network Protocols, 2014, pp 221-232.

[4] A. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, 2004, pp 4-20.

[5] Z. Xu, K. Bai, S. Zhu, "TapLogger: Inferring User Inputs on Smartphone Touchscreens Using On-board Motion Sensors", Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, 2012, pp 113-124.

[6] A. Aviv, B. Sapp, M. Blaze, J. Smith, "Practicality of Accelerometer Side Channels on Smartphones", Proceedings of the 28th Annual Computer Security Applications Conference, 2012, pp 41-50.

[7] M. Mehrnezhad, E. Toreini, S. Shahandashti, F. Hao, "Stealing PINs via Mobile Sensors: Actual Risk versus User Perception", International Journal of Information Security, 2018, pp. 291-313.