www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 11 Nov 2015, Page No. 15000-15004

Surveying Smartphone Security for Linux Powered Devices

Sharan Shetty,Nitin Ranjan, Aditya Sharma Aman Prakash Singh,Rahul Koti, Mrs. D.A. Phalke(Guide) & Mr. Rahul Pawar(Co-Guide)

Department of Computer Engineering D Y Patil College of Engineering Akurdi, Pune
Email: sharan.shetty0000@gmail.com
Email: nitinojha65@gmail.com Email: sharmaa210@gmail.com Email: amanprakash35@gmail.com Email: vip4499@gmail.com

Abstract : In this era of Globalization, the extensive use of SmartPhones in our day-to-day life has become a very important factor. According to surveys, nearly 0.8 of the SmartPhone industry is dominated by Android. Therefore, the issue of Security and Privacy of the User becomes a crucial factor to be taken care of. Since, Android is an Open-Source Platform, the scope of resolving issues like this becomes easy and effective with the help of applications designed by programmers around the globe. Smartphones running on Android OS have an in-built password detection mechanism (character/pattern/gesture) which helps in differentiating between real user from unknown user. Also, the proposed system are designed to work with their own perspective to meet the users demands and this done with the help of pre-defined sensors which are thoroughly elaborated after a lot of search. In this paper, A survey of the research done by the predecessors on related subject to provide better security and to overcome this breach of privacy. Now while discussing the security measures, The system can possibly assume that under a certain type of scenario an intruder may try to access valuable information of the user without his knowledge and when faced with a password barrier, the intruder may try to bypass it by entering another password, and if the password is wrong it may result in multiple failed attempts. So there has to be certain solution to detect this breach and if possible overcome it. Along with this, the proposed system should make sure that the application consumes least amount of battery and uses minimum amount of system memory.

Keywords–Mobile computing, password detection, location tracing, SOS Message, In-built Micro-Environment Sensors.

I. Introduction

In this era, where there is a total boom of smartphones being used it is very important that the users security is not compromised. Various attempts can be made by a malicious user who is trying to access the information of the user. One such attempt is when the unknown user tries to bypass password lock set by the real user. It is highly possible that he might not know the password, and so he would carry on multiple attempts to unlock it. Thus, finally he may or may not be able to access the phone, but the point is that the real user may never know that someone had tried to access his phone without his permission. Another concern from users perspective is that he may wanna try to contact his colleagues in case of emergency but it might not be possible to talk to them normally. Thus, it is very important to overcome these issues in order to provide the user better security and help them contact when in need and emergency. In this system, it proposes an Android application which consists of modules that help the user to carry out theft detection, tracing of location and allowing the user to send SOS message in case of emergency when contacting someone is very difficult. To implement such a platform, difficulties are triple. First, previous context-aware solution (especially if algorithms and metrics if any) are analyzed by human intuition. Second, the application must be tested on different versions of Android OS to determine its feasibility and compatibility and as the updates are made quickly and vary through different smart phones, it becomes very complicated. Third, distinguishing similar micro-environment relies on systematic collaboration among multi-modal sensors since the chances of the application of not distinguishing between a required task and its pre-defined task is very important for effective functioning. The proposed system is to build the framework of the application upon an investigation of phone usage and user habits. The framework covers the majority of phone states, and consists of three core modules: Theft Detection, User Security especially Women during emergency and Tracing location of phones using GPS GSM/text.

DOI: 10.18535/Ijecs/v4i11.23

II. Related Work

The proposed system present the design, implementation and evaluation of Sherlock, a simple yet practical platform for micro-environment sensing for smartphones. Via collaboration among built-in sensors. The platform automatically collects sensor hints and characterizes the immediate surroundings of smartphones at centimetre level accuracy, providing fine-grained environment information to upper layer applications. The system conducted comprehensive experiments to evaluate their system through a prototype implementation on android platform. Preliminary experiment results show that Sherlock achieves low energy cost, rapid system deployment, and competitive sensing accuracy[1].

The proposed system have developed an aid for locating missing or lost children. The solution proposed in their paper takes advantage of the rich features offered in Androids smart phones. The architecture of the system is built on two main component, GPS satellite, and GSM telephony services. Some of this work relies on internet connectivity or a server that has to be up running. The proposed service relies only on two main services, telephony and location, thus eliminating the need of internet connection or a dedicated server. Finally, like any software product or design, there is still room for enhancement and features such as Geo-fencing, emergency alerts can be added to the system[2].

The problem was solved by proposing an application Locating Friends and Family Using Mobile Phones with Global Positioning System (GPS). The architecture of the system is based on clientserver approach. The client phone registers and login into the server. Then, the client periodically sends his coordinate location updates to the server which stores it in a database. Thus, any client wishes to learn the location of another client will have to register and login to the server to request the location. This application was developed to helps locate family member and friends. The mobile application was implemented using J2ME. As for the server, it uses MySQL Database along with PHP to guarantees that the server would not be overloaded. This proposed solution makes each client has same control and command privileges as the other which is not convenient for use in child tracking application where only the parent should have the control and command privileges. A limitation of this solution is that in order for the system to work there must be internet connectivity in both client and server sides[3].

The system propose an online calibration and synchronization algorithm for cellphones that is able to estimate not only the camera projection parameters, but also the gyroscope bias, the relative orientation between the camera and gyroscope, and the delay between the timestamps of the two sensors. The proposed algorithm is based on the generalization of the coplanarity constraint of the cross products of matched features in a rolling shutter camera model. Experiment run on real data collected from cellphones show that the proposed algorithm can successfully estimate all of the needed parameters with different kinds of motion of the cellphones. This online calibration and synchronization of rolling shutter camera and gyroscope make it more convenient for high quality video recording, gyro-aided feature tracking, and visual-inertial navigation[4].

A three level security approachhas been applied on the system, which apparently makes it highly secure along with being more user friendly. This system will definitely help thwarting Shoulder attack, Tempest attack and brute-force attack at the client side. 3-Level Security system is definitely a time consuming approach, as the user has to traverse through the three levels of security, and will need to refer to his mobile number for the one-time automated generated password. Therefore, this system cannot be a suitable solution for general security purposes, where time complexity will be an issue. But will definitely be a boon in areas where high security is the main issue, and time complexity is secondary, as an example take the case of a firm where this system will be accessible only to some higher designation holding people, who need to store and maintain their crucial and confidential data secure [6].

The system describes that while the Android message passing system promotes the creation of rich, collaborative applications, it also introduces the potential for attack if developers do not take precautions. The system examine inter-application communication in Android and present several classes of potential attacks on applications. Outgoing communication can put an application at risk of Broadcast theft (including eavesdropping and denial of service), data theft, result modification, and Activity and Service hijacking. Incoming communication can put an application at risk of malicious Activity and Service launches and Broadcast injection. There is a tool, ComDroid, that developers can use to find these kinds of vulnerabilities. Their tool relies on DEX code, so third parties or reviewers for the Android Market can use it to evaluate applications whose source code is un- available. It analyzed 100 applications and verified their findings manually with 20 of those applications. Of the 20 applications, 12 applications with at least one vulnerability. This shows that applications can be vulnerable to attack and that developers should take precautions to protect themselves from these attacks[8].

The proposed system have reported the design, development and performance evaluation of a smartphone app that performs live detection of physical activities. This app differentiates itself from previous works on activity recognition in the following: 1) It requires no user interaction post-setup, 2) It requires no additional sensing hardware and relies solely on the physical sensors that are standard on even low-end smartphones, 3) It requires no calibration, 4) It supports the detection of 7 different physical activities, including walking, running, climbing stairs, descending stairs, cycling, driving and remaining inactive, and 5)The Decision Tree classifier used by the Activity Diary app is accurate. The average area under the ROC curve exceeds 0.99. This application lets users monitor their daily physical activity and enables them to make healthier and more informed choices that can lead to healthier habits and lifestyle. Live updates are specifically targeted to encourage decisions based on a healthier lifestyle.The propsoed system are currently field testing the Activity Diary app and are working to make it available to the public through the Google Android marketplace. In the future, the system would like to extend this app further to: 1) Support more physical activities, 2) Infer modes of transportation and provide users with feedback in terms of their estimated carbon footprint, and 3) Develop an app function that uses historical information about physical activities and contextual information to gives users pro-active suggestions for lifestyle choices[9].

The system presents SenGuard, a mobile user identification management solution that can provide continuous and implicit user authentication service on a mobile system. SenGuard is implemented over an open source mobile operating sys- tem. It uses a novel virtualization based system architecture that drastically improves protection of its user identification mechanism by moving it into a privileged virtual domain. In addition, virtualization allows implicit and continuous capture of interactive inputs from multiple sensor modalities. An initial prototype of SenGuard was created using four sensor modalities, voice, location, multitouch, and locomotion. Preliminary empirical studies with a small set of human users indicate that those four modalities are suited as data sources for implicit mobile user identification. The preliminary results also suggest a number of interesting avenues for further research[10].

The system propose an application named AALTm -An Android Application to Locate and Track Mobile phones which is a unique & efficient application having a variety of features that enhances the existing mobile tracking system. AALTm stands different from the existing system as it is not only the GPS value it makes use of but it works on GSM/text messaging services which make it a simple and unique one. This application doesnt work if the phone is switched off. For future work, it is proposed to implement some algorithm where the phone itself identifies that it is being lost. Whenever, the phone is off for more than 48 hours it should make it switch on automatically[11].

III. System Architecture

The system involves three basic layers : Hardware layer at the bottom, Middleware Layer in the middle, and the topmost layer is the Application layer. The Hardware layer consists of sensors and actuators like Gyroscope, Proximity and Pressure sensor, GPS. Also, it involves activity generation using front- camera and touchscreen. The functionality of each module is defined separately in the Middleware layer. Each module, has a particular set of tasks to be carried out, and this is done with the help of additional information gathered from respective Hardware layer sensors. For eg: in order to determine whether or not to send an SOS message it is first checked whether the pressure is more than the threshold value and this value is determined by the timeframe for which pressure sensor was active due to users touch. All these modules are accessed and turned on/off using the interface of modules in the topmost layer i.e. Application layer. This entire application, as a whole, runs as a daemon process in the background, maintaining battery optimization, with no disturbance to user-interface with other applications and maintaining its secrecy of tracing the intruder or malicious user.

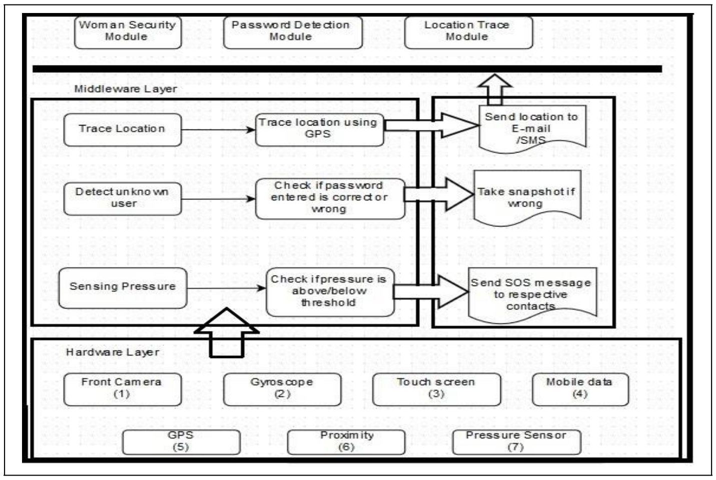

Fig. 1. System Architecture

IV. Conclusion

The proposed system carry out a thorough survey of different research related work which are directly or indirectly aimed at Smart phone security in Android. Basically, the approach was towards achieving security from an unknown or malicious user who is trying to access private or professional information of the real user using his phone. Although, it is most certain that the phone will be password protected, yet the unknown intruder might try to bypass it by attempting to guess password and it is least likely yet possible that he may unlock the phone and the real user might be stripped out of his bank details, credit card details, important and confidential media etc. Thus, on carrying out this survey, the system learned the predecessors acknowledged various kinds of similarly related threats and have suggested many effective and user-friendly methods to overcome such kind of breach of security and invasion of privacy. All the aforementioned papers, have contributed greatly to the proposed system and have helped to develop this application .

Acknowledgment

We express our sincere gratitude to Mrs. M. A. Potey, Head of Department, Computer Engineering, for her assistance, persuasion, and an incent to work better. Our deepest gratitude goes to our project guide, Mrs. D. A. Phalke, for her guidance, ideas, help, encouragement, interpretations and suggestions which helped us in the realization of our objective and coordinate as a team.

We wish to thank Ms. Disha Tiwari and Mr. Rahul Pawar for their constant support which helped bring the best out of our survey.

We are extremely thankful to our project incharge, Mrs Shanthi Guru for her comments, introspections and support which helped us throughout our work.

References

[1] [1] Zheng Yang, Member, IEEE, Weixi Gu, Student Member, IEEE, Zimu Zhou, Student Member, IEEE, Sherlock: Micro-Environment Sensing for Smartphones, Published by the IEEE Computer Society, December-
2014.

[2] [2]A. Al-Mazloum, E. Omer, M. F. A. Abdullah, GPS and SMS-Based Child Tracking System Using Smart Phone, Published by International Journal of Electrical, Computer, Energetic, Electronic and Communication En- gineering Vol:7, No:2, 2013.

[3] [3]Ghaith Bader Al-Suwaidi, Mohamed Jamal Zemerly, Locating friends and family using mobile phones with global positioning system (GPS), IEEE/ACS Interna- tional Conference on Computer Systems and Applica- tions, 2009.

[4] [4]Chao Jia and Brian L. Evans Department of Electrical and Computer Engineering, OnlineCalibration and Synchronization of Cellphone Camera and Gyroscope, Published by IJCSMC, ISSN 2320 088X, February 2014.

[5] [5] Narseo Vallina-Rodriguez and Jon Crowcroft, Fellow, IEEE, Energy Management Techniques in Modern Mo- bile Handsets, Published by IEEE COMMUNICATIONS SURVEYS TUTORIALS, 2013.

[6] [6] Nagesh.D Kamble,J.Dharani, Implementation of Security System Using 3-Level Authentication, Published by IJEDR, ISSN: 2321-9939, 2014.

[7] [7] Emiliano Miluzzo, Hong Lu, Daniel Peebles, Survey of Mobile Phone Sensing , Proc. 26th Annual ACM SIGCHI Conf. Human Factors Comp. Sys., 2008, pp.
17971806A.

[8] [8] Erika Chin, Analyzing Inter-Application Communi- cation in Android, pp. 117, 2004.

[9] [9]Alvina Anjum Muhammad Ilyas, Activity Recognition Using Smartphone Sensors, Pervasive Computing, IEEE, vol. 1, no. 3, pp. 2432, 2002.

[10] [10] Weidong Shi, Jun Yang, Yifei Jia, SenGuard: Passive User Identification on Smartphones Using Multiple Sensors, 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications.

[11] [11] Sonia C.V, Dr. Aswatha, AALTm: An Android Application to Locate and Track Mobile Phones, Published by International Journal of Engineering Trends and Technology (IJETT), May, 2013.