Drive Now, Text Later: Nonintrusive Texting while Driving Detection using Smartphones

Ms. Pawar Darshana[1] Ms. Yadav Pranjali[2] Ms.Inamdar Firdose[3] Ms. Bhange Sonam[4] Ms. Jadhav Manali[5]
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]Dr. D. Y. Patil Polytechnic, Akurdi, Pune, India

Abstract— The system proposes a security system, named the Internal Intrusion Detection and Protection System (IIDPS for short) at system call level, which creates personal profiles for users to keep track of their usage habits as the forensic features. The IIDPS uses a local computational grid to detect malicious behaviors in a real-time manner the proposed work is regarded with Digital forensics technique and intrusion detection mechanism. The number of hacking incidents are increasing day by day as new technology rolls out. The system designed Intrusion Detection System (IDS) that implements predefined algorithms for identifying the attacks over a network. Therefore, in this project, a security system, named the Internal Intrusion Detection and Protection System (IIDPS), is proposed to detect insider attacks at SC level by using data mining and forensic techniques. The system can identify users forensic features by analyzing the corresponding SCs to enhance the accuracy of attack detection, and able to port the IIDPS to a parallel system further shorten its detection response time.

Key words: Smartphones, Vehicles, Accelerometer, Global Positioning System

I. Introduction

From last decade, computer systems have been largely employed to provide users with easier and more perfect lives. However, securities are the most serious issue in computer domain when users take advantages of powerful capabilities since attackers try to enter in the computer systems and behave harmfully, e.g. corrupt data can make systems out of work or destroying the systems. Pharming attack, distributed denial-of-service (DDoS), eavesdropping attack, and spear-phishing attack generally all this attack are well known attacks inside attack is most difficult for the detection because firewalls and intrusion detection systems (IDSs) fights against outside attacks. Now a days, to authenticate a user, most systems check ID and passwords as a login token. However, attackers may install Trojan virus to hack the password and may then log in to the system, access users' private files, or modify or destroy system settings. Fortunately, systems can now detect a known intrusion in a real time manner. Attack packets are often issued with forged IPs or attackers may enter a system with valid login patterns that's why it's very difficult to identify who is attacker. However in Operating System level system calls (SCs) is more helpful to find out attacker and identify the exact attack, processing a large volume of SCs, detecting harmful behaviors from them, and detecting possible attackers for an intrusion are still engineering challenges Therefore, in this paper, we propose a security system, at SC level which detects harmful behaviors launched toward a system named Internal Intrusion Detection and Protection System (IIDPS). To mine system call patterns (SC-patterns) defined as the longest system call sequence (SC-sequence) that has repeatedly appeared several times in a user's log file for the user the IIDPS uses data mining and forensic profiling techniques.The user's forensic features, define is as an SC Pattern find out in submitted by users SC sequences but normally used by other users computer usage history. The contributions of this paper are: 1) identify a user's forensic features by analyzing the corresponding SCs to enhance the accuracy of attack detection; 2) able to port the IIDPS to a parallel system to further shorten its detection response time; and 3) effectively resist insider attack. Technique is crucial requirement.

II. Modules

A. *T & D System*

We investigate a new point for user's input detection: we utilize smart phone embedded sensors to log touch strokes, which are directly associated with user's input. We have carried out extensive experiments which show that each touch stroke will cause a tiny, but discernable and distinctive rotation change of the smart phone, which can be captured by its gyroscope sensors. In this way, the time of occurrence of each input of mobile users can then be identified. In addition, using touch stroke induced rotation to infer touch screen input does not need to access contents of the messages, thus the privacy of smart phone users can be preserved.

B. *Touch Stroke Detection*

Here the touch strokes are identified by using the gyroscope data. Using the training data set a touch stroke template is constructed. On this gyroscope data the template is utilized as wavelet basis and they carry out wavelet transform. According to the occurrence of touch strokes the significant peaks and the location of the peaks are selected.

III. Proposed System

The proposed system allows the user attend calls that are urgent and are in the emergency list. The system doesn't blindly block all the calls. The system detects the usage of phone while driving without any external hardware such as cameras or motion sensors. It uses the inbuilt mobile phone sensors like, Accelerometer, Gyroscope to detect the usage of phone considering the velocity at which the phone is moving, thus it is a cost effective approach to reduce the accident percentage involving usage of cellphones

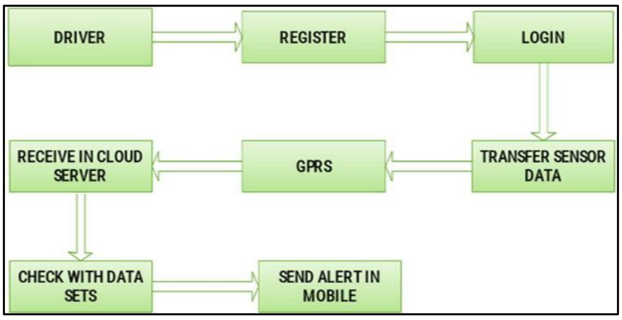

Fig. 2: System Architecture

A. *Correlating Touch Strokes Information from Vehicles*

We correlate touch strokes with the information of vehicle to test the first two patterns of T&D. In particular, the decrease of vehicle speed before and during touch strokes will be utilized to test pattern

1) A driver prefers to compose messages after the car speed is decreased, and the change of vehicle direction will be used to test pattern.
2) A driver usually stops editing messages when the car is taking turns

IV. ADVANTAGES

It doesn’t require frequent manual activation.

Once started it will track all actions performed on the smartphone so that malicious behavior of users can be tracked.

Cost effective solution as no external devices are used.

V. CONCLUSION

In this paper, we propose a method which is able to detect T&D. Instead of using any extra devices, the method leverages some patterns associated with how smart phones are used in moving vehicles. Sensors in smart phones collect the information and analyze, to see whether these T&D patterns exist. Extensive experiments have been conducted by different persons at different driving locatoins. Results show that this method can achieve good detection accuracy with. The outcome of this approach will achieve good detection accuracy.

REFERENCES

[1] Doo Seop Yun, Jeong-Woo Lee, Shin-Kyung Lee, and Oh-Cheon Kwon, “Development Of the Eco-Driving and Safe-Driving Components using Vehicle Information,” 2012 International Conference on ICT Convergence (ICTC), pp. 561-562, Oct. 2012.

[2] J. Almazán, L. M. Bergasa, J. Yebes, R. Barea, and R. Arroyo, “Full auto-calibration of a smartphone on board a vehicle using IMU and GPS embedded sensors,” in Proc. IEEE Intell. Vehicles Symp. (IV), Jun. 2013, pp. 1374– 1380.

[3] Cheng Bo, Xuesi Jian, Taeho Jung, Junze Han, and Xiang-Yang Li, “Detecting Driver’s Smartphone Usage via Nonintrusively Sensing Driving Dynamics,” IEEE Internet of Things Journal., vol. 4, no. 2, pp. 340-350, April. 2017.

[4] L. M. Bergasa, D. Almería, J. Almazán, J. J. Yebes, and R. Arroyo, “DriveSafe: an App for Alerting Inattentive Drivers and Scoring Driving Behaviors,” in IEEE Intelligent Vehicles Symposium (IV), Detroit, USA, June 2014, pp. 240–245.

[5] Doo Seop Yun, Jeong-Woo Lee, Shin-Kyung Lee, and Oh-Cheon Kwon, “Development Of the Eco-Driving and Safe-Driving Components using Vehicle Information,” 2012 International Conference on ICT Convergence (ICTC), pp. 561-562, Oct. 2012

[6] National survey on distracted driving attitudes and behaviors. 2012.

[7] F. Pukelsheim, "The three sigma rule", The American Statistician, vol. 48, no. 2, pp. 88-91, 1994.

[8] H. L. Chu, V. Raman et al., "Poster: You driving? Talk to you later", Proc. 9th Int. Conf. Mobile Syst. Appl. Serv., pp. 397-398, 2011.

[9] http://www.who.int/violence_injury_prevention/publications/road_traffic/distracted_driving/en/index.html

[10] C.-W. You, M. Montes-de Oca, T. J. Bao, N. D. Lane, H. Lu, G. Cardone, L. Torresani, and A. T. Campbell. Carsafe demo: supporting driver safety using dual-cameras on smartphones. InProceedings of the 2012 ACM Conference on Ubiquitous Computing, pages 547–547. ACM, 2012