SECURE VIOLENT DELETION IN ANDROID APPLICATION WITH TRUST ANALYSIS IN GOOGLE PLAY

K. UMAMAHESWARI

Assi. Prof. Mr. K. NIRMAL

Department of Computer Applications, Krishnasamy College of Engineering and Technology, Cuddalore, Tamil Nadu, India

ABSTRACT - The Android Application model is becoming a viable communication alternative to the traditional infrastructural model for modern mobile consumer electronics equipped with short-range communication technologies such as Bluetooth, NFC, and Wi-Fi Direct. Proximity violence is a class of violence that exploits the opportunistic contacts and distributed nature of application for propagation. Behavioral characterization of violence is an effective alternative to pattern matching in detecting violence, especially when dealing with polymorphic or obfuscated violence. In this paper, first propose a general behavioral characterization of proximity violence which based on naive Bayesian model, which has been successfully applied in non-apps setting such as filtering email spams and detecting botnets. Identify two unique challenges for extending Bayesian violence detection to apps ("insufficient evidence versus evidence collection risk" and "filtering false evidence sequentially and distributedly"), and propose a simple yet effective method, look ahead, to address the challenges. Furthermore, proposed two extensions to look ahead, dogmatic filtering, and adaptive look ahead, to address the challenge of "malicious nodes sharing false evidence." Real mobile network traces are used to verify the effectiveness of the proposed methods.

Key Terms: Naive Bayesian model, detecting violence, dogmatic filtering, adaptive look ahead.

I. INTRODUCTION

The Android application model is an alternative to the traditional infrastructure model. The widespread adoption of these devices, coupled with strong economic incentives, induces a class of violence that specifically targets apps. In this paper, consider a general behavioral characterization of proximity violence. Behavioral characterization, in terms of system call and program flow, it has been previously proposed as an effective alternative to pattern matching for violence detection. In this model, violence-infected nodes" behaviors are observed by others during their multiple opportunistic encounters: Individual observations may be imperfect, but abnormal behaviors of infected nodes are identifiable in the long-run. This paper focus on how individual nodes shall make such cutoff decisions against potentially violence-infected nodes, based on direct and indirect observations. Essentially, it extend the naive Bayesian model, which has been applied in filtering email spams, detecting botnets, and designing IDSs, and address two application specific, violence-related, problems:

1. Insufficient evidence versus evidence collection risk. In applications, evidence (such as Bluetooth connection or

SSH session requests) is collected only when nodes come into contact. But contacting violence-infected nodes carries the risk of being infected. Thus, nodes must make decisions (such as whether to cut off other nodes and, if yes, when) online based on potentially insufficient evidence.

2. Filtering false evidence sequentially and distributed. Sharing evidence among opportunistic acquaintances helps alleviating the aforementioned insufficient evidence problem; however, false evidence shared by malicious nodes (the liars) may negate the benefits of sharing.

In applications, nodes must decide whether to accept received evidence sequentially and distributed. This paper presents a general behavioral characterization of proximity violence, under the behavioral violence characterization, and with a simple cut-off violence containment strategy, it formulate the violence detection process as a distributed decision problem. It analyze the risk associated with the decision, and design a simple, yet effective, strategy, look ahead , which naturally reflects individual nodes‟ intrinsic risk inclinations against violence infection. Look ahead extends the naive Bayesian model, and addresses the application-specific, violence-related, “insufficient evidence versus evidence collection risk” problem. It considers the benefits of sharing assessments among nodes, and address challenges derived from the application model: liars (i.e., bad-mouthing and false-praising malicious nodes) and defectors (i.e., good nodes that have turned rogue due to violence infections). It will present two alternative techniques, dogmatic filtering and adaptive look ahead, that naturally extend look ahead to consolidate evidence provided by others, while containing the negative effect of false evidence.

A nice property of the proposed evidence consolidation methods is that the results will not worsen even if liars are the majority in the neighborhood. Real contact traces are used to verify the effectiveness of the methods.

II. LITERATURE VIEW

1. The research paper Droid Mat: Android Violent Detection through Manifest and API Calls Tracing written by author “D.J.Wu, C.H.Mao, T.E.Wei, H.M.Lee” in the year of 2012 explains that android violent detection in Api calls tracing.
DISADVANTAGE**:** Functional Calls.

2. The research paper Behavioral detection of Violent on mobile handsets written by author “A. Bose,X.Hu, K.G.Shin, T.Park” in the year of described as novel behavioral detection framework is proposed to detect mobile worms Security, Mobile Handsets, Worm Detection, used to Machine Learning.
DISADVANTAGE: Cannot Access the Mobile Access Points.

3. The research paper Detecting Symbion OS Violent through Static Function Call Analysis written by A.D.Schmidt, J.H.Clausen, S.H.Camtepe, S.Albayrak and described as Supporting Vector Machine.
DISADVANTAGE: Power Consumption.

III. PROPOSED METHODOLOGY

Behavioral characterization, in terms of system call and program flow, has been previously proposed as an effective alternative to pattern matching for violence detection. In our model, violence-infected nodes’ behaviors are observed by others during their multiple opportunistic encounters:

Individual observations may be imperfect, but abnormal behaviors of infected nodes are identifiable in the long-run. Identify the challenges for extending Bayesian violence detection to Applications, and propose a simple

yet effective method, look-ahead, to address the challenges. Furthermore, proposed two extensions to look-ahead, dogmatic filtering and adaptive look-ahead, to address the challenge of "malicious nodes sharing false evidence".

Assessments come from two models. 1. Household watch 2. Neighborhood watch. The Household watch Violence Detector node's own assessments only. The Neighborhood watch Violence Detector node own assessments with its neighbors'. In Household watch: Pg(A) >= Pe(A) Evidence A is favorable to j. Pg(A) < Pe(A) Evidence A is unfavorable to j. Instead of making the cut-j-off decision right away when Pg(A) < Pe(A), Violence Detector node looks ahead to confirm its decision.

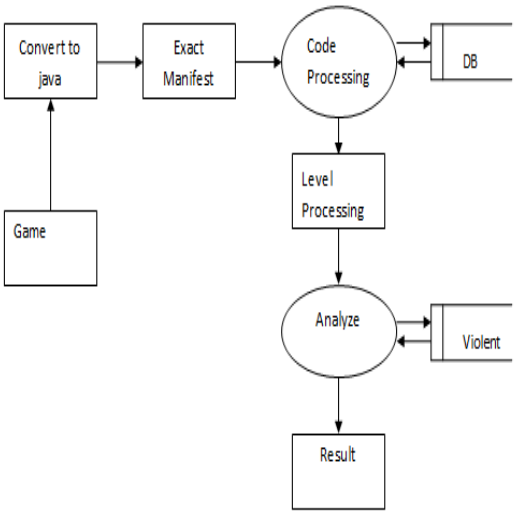

Figure1: Architecture of the proposed system

IV. MODULES

Determining components of interest

The first step in the analysis of an app is identifying components of interest, i.e. if it does not fit a model defined for all components of type. In current version of ALTERDROID, models measure statistical features only, such as for example the expected entropy, the byte distribution, or the average size. Such features are computed from a dataset of components of the same type, such as text files, pictures, code, etc.

Producing Fault Injected Apps

Components of interests identified in the previous stage are injected with faults and reassembled, together with the remaining app components, to generate a faulty app. This process can generate several fault-injected apps, as there are multiple ways of applying different FIOs to different components in the set of component interest. In ALTERDROID, fault-injected apps are generated one at a time and sent for differential analysis. If no evidence of malicious behavior is found in the differential analysis, the fault injection process is invoked again to generate a different faulty app, and so on.

Determining Differential Analysis

Differential analysis between a candidate fault-injected app and the original app is carried out following the model. The process comprises the following steps: Generate an appropriate usage pattern and context, to feed both apps and extract their behavioral signatures. Both the original and the fault-injected app is tested under the same conditions and using the same inputs. Note that this assumes that the execution of an app is completely deterministic.

Prototype Implementation

ALTERDROID is implemented using Java and relies on a number of Android open source tools for specific tasks. App components are extracted using Android. After fault injection, components are repackaged into a modified app using apk Tools. These events should be generated specifically for each test to intelligently drive the GUI exploration, i.e., to test code implementing different functionalities of the app.

V. CONCLUSION

Behavioral characterization of violence is an effective alternative to pattern matching in detecting violence, especially when dealing with polymorphic or obfuscated violence. Naive Bayesian model has been successfully applied in non- application settings, such as filtering email spam sand detecting botnets. Proposed behavioral characterization of application-based proximity violence. To address two unique challenging in extending Bayesian filtering to applications: insufficient evidence versus evidence collection risk and filtering false evidence sequentially and distributed.

VI. REFERENCES

[1] J. Su, K. Chan, A. Miklas, K. Po, A. Akhavan, S. Saroiu, E. de Lara, and A. Goel, "A Preliminary Investigation of Worm Infections in a Bluetooth Environment," Proc. Fourth ACM Workshop Recurring Malcode (WORM), 2006

[2] S. Cheng, W. Ao, P. Chen, and K. Chen, "On Modeling Violence Propagation in Generalized Social Networks," IEEE Comm. Letters, vol. 15, no. 1, pp. 25-27, Jan. 2011

[3] C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, and X.Wang, "Effective and Efficient Violence Detection at the End Host," Proc. 18th Conf. USENIX Security Symp., 2009

[4] Chao Gao and Jiming Liu, "Modeling and Restraining Mobile Violent Propagation," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.12, NO.3, MARCH 2013

[5] C. Gao, J. Liu, and N. Zhong, "Network Immunization with Distributed Autonomy-Oriented Entities," IEEE Trans. Parallel and Distributed Systems, vol. 22, no.7, pp. 1222-1229, July 2011.

[6] C,Gao and J.Liu, " Modeling and Predicting the Dynamics of Mobile Violent Spread Affected by Human Behavior", Proc. IEEE 12th Int'l Symp. A World of Wireless, Mobile and Multimedia Networks (WoWMoM '11), pp, 1-9, 2011.

[7] D.-H. Shi, B. Lin, H.-S. Chiang, and M.-H. Shih, "Security Aspects of Mobile Phone Violent: A Critical Survey," Industrial Management and Data System, vol. 108, no. 4, pp. 478-494, 2008.