EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.126-132
SANA ACADEMIC PRESS

Interaction Approach to Curb Emerging Smartphone Malware

K. Hemavathi[1], N. Muthulakshmi[2], S. Brindha[3]
[1]Research Scholar, St.Peter's University, Chennai.
[2]Asst.Prof., Dept. of Computer Applications, St.Peter's University, Chennai
[3]Asst.Prof., Dept. of Computer Applications, St.Peter's University, Chennai
hemavathibhavani@gmail.com

Abstract–*TWR is based on simple cyber-physical human interaction i.e., human gestures, that are very quick and intuitive but less like to be exhibited in users daily activities .Presence or absence of such gestures, prior to accessing an application can effectively inform the OS whether the access request is benign or malicious. Specifically, we present the design of a acceleration-based phone tapping detection mechanism The mechanism is geared for NFC applications, which usually require the user to tap her Phone with another device. In practice, to protect mobile phones from malware attack, the Android platform uses permission models to prevent malware from being installed at the first place. Our results suggest the proposed approach could be very effective for malware detection/prevention, with quite low false positive and false ne gat many smart phones are beginning to incorporate Near Field Communication (NFC)chips [23], which allow short, paired transactions with other NFC devices in close proximity. The use of NFC-equipped smart phone as payment token(such as Google Wallet) is considered to be the next generation payment system.*

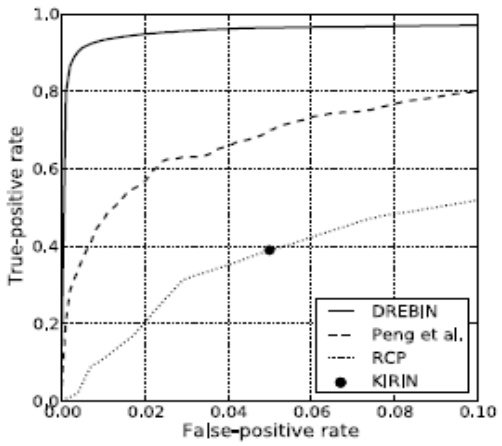
Keywords: *WAD, NFC, File Communication, crash severit. Human Gestures.*

I.INTRODUCTION

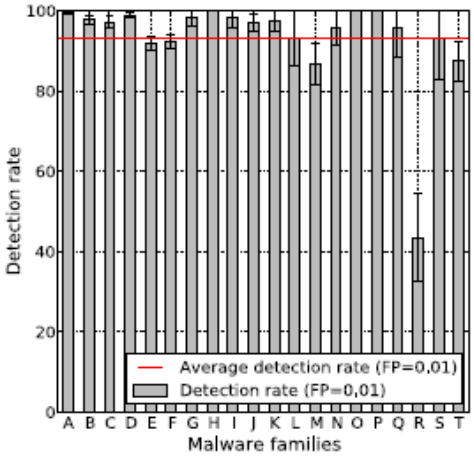
Manual Detection Model (MDM) which is different from the traditional signature scanning methods. Firstly, we monitor the path and files, and touch the scan option. After decoding MDM model, abnormal process can be detected using the matching extension files with empty spaces, the experimental results demonstrate that the proposed method can effectively detect mobile malware. In recent year, smart phone technology is becoming increasingly popular. The dangers of mobile phone malware are becoming more and more serious. In this paper we present a new mobile Smartphone malware detection scheme based on Manual Detection Model (MDM) which is different from the traditional signature scanning methods Firstly. We monitor the path and files, and touch the scan option. After decoding MDM model, abnormal process can be detected using the matching extension files with empty spaces, the experimental results demonstrate that the proposed method can effectively detect mobile malwares.

II.MATERIALS AND METHODS

Since 2014 A Specification Based Instruction Detection Framework For Mobile Phones (Ashw in Chaugule, Zhi Xu, and Sencun Zhu)With the fast growth of mobile market, we are now seeing more and more malware on mobile phones. One common pattern of many common found malware on mobile phones is that: the malware always attempts to access sensitive system service on the mobile phone in an unobtrusive and stealthy fashion. For example, the malware may send messages automatically interface with the audio peripherals on the device without the user's awareness and authorization. To detect the unauthorized malicious behaviour, we present (SBIDF) Specification Based Instruction Detection Framework which utilizes the keypad or touch screen interrupt to differentiate between malware and human activity. Specifically, in the proposed framework, we can use an application independent specification, written in Temporal Logic of Causal Knowledge (TLCK) to describe the normal behaviour pattern, and enforce this specification to all third party applications on the mobile phone during run time by monitor the inter-component communication pattern among critical components The results of this experiments are shown in Figure 4(a) as ROC curve, that is, the detection rate (true-positive rate) is plotted against the false-positive rate for different thresholds of the detection methods.



(a) Detection performance as ROC curve.



(b) Detection per malware family.

Detection of malware families: Another important aspect that should be considered when testing the detection performance of a method is the balance of malware families in the dataset [32]. If the number of samples of certain malware families is much larger than of other families the detection result mainly depends on these families. To address this problem one can use the same number of samples for each family. However, this leads to a distribution that significantly differs from reality. Instead we evaluate the detection performance for each of the 20 largest malware families separately. The family names and the number of samples for each family can be found in Table (c) and the detection performance of DREBIN for each family is illustrated in Figure (b).

Id	Family	#	*Id*	Family	#
A	FakeInstaller	925	*K*	Adrd	91
B	DroidKungFu	667	*L*	DroidDream	81
C	Plankton	625	*M*	LinuxLotoor	70
D	Opfake	613	*N*	GoldDream	69
E	GingerMaster	339	*O*	MobileTx	69
F	BaseBridge	330	*P*	FakeRun	61
G	Iconosys	152	*Q*	SendPay	59
H	Kmin	147	*R*	Gappusin	58
I	FakeDoc	132	*S*	Imlog	43
J	Geinimi	92	*T*	SMSreg	41

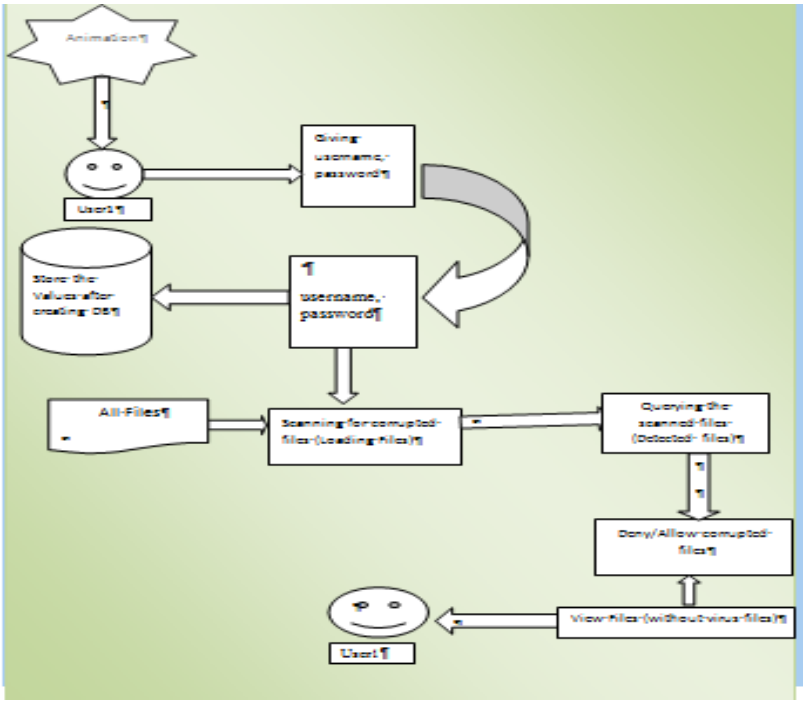
(c) Top malware families in our dataset.

Apposcopy: Semantic-Based Detection of Android Malware through Static Analysis(YuFeng,SaswatAnand,Isil Dillig 2015) We present Apposcopy, a new semantics-based approach for identifying a prevalent class of Android malware that steal private user information. Apposcopy incorporates a high level language for specifying signature that describe semantic characteristics of malware family and astatic analysis for deciding if a given application match a malware signature. signature matching algorithm of Apposcopy uses a combination of static taint analysis and a new form of program representation is called Inter-Component Call Graph In response to the rapid dissemination of Android malware, there is a real need for tools that can be automatically detect malicious applications that steal private user information. Two prevalent approach for detecting such Android malware are taint analyzer and signature EXISTING SYSTEM: We argue that existing malware defences, without considering the special characteristics of smartphone malware and that of smart phone themselves, might not be sufficient to sophisticated malware.

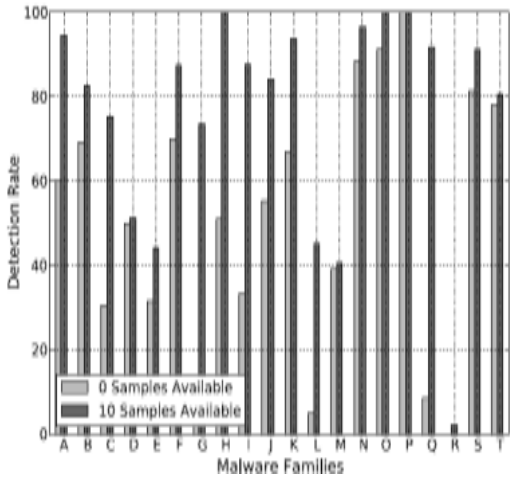
DRAWBACKS IN EXISTING SYSTEM:

Detecting some files only. Not easily get deleted. PROPOSED SYSTEM: We propose abnormal process can be detected using the matching extension files with empty spaces, the experimental results demonstrate that the proposed method can effectively detect mobile malwares. If files extension in abnormal process or empty files with abnormal process ca and corrupted files listed ADVANTAGES IN PROPOSED SYSTEM: Detecting and deleting every file in abnormal conditions Accurately detect the malware files. Better Accuracy than existing.

III. ARCHITECTURE DIAGRAM



IV. DETECTION OF UNKNOWN MALWARE FAMILIES:

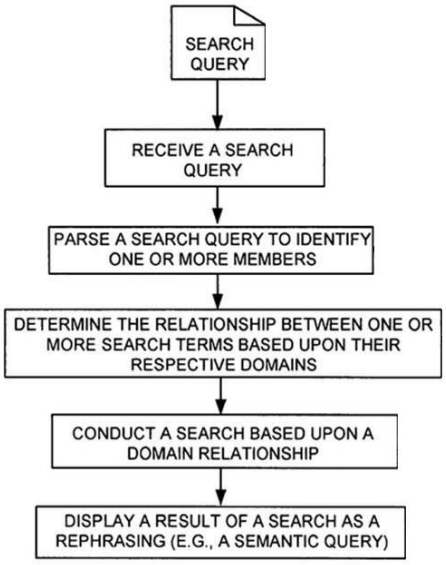


DREBIN uses known malware for learning its detection model. It is thus important to assess how many samples of a family need to be known to reliably detect this family. To study this issue, we conduct two additional experiments where we limit the number of samples for a particular family in the training set. In the first experiment we provide no samples of the family, corresponding to a totally

unknown malware strain. In the second experiment, we put 10 randomly chosen samples of the family back into the training set, thus simulating the starting spread of a new family. The results of the two experiments are shown in Figure 5, where the detection rate is shown for 0 and 10 available samples in the training set for each family. If no samples are available for learning, it is difficult for DREBIN to detect a family, as no discriminative patterns can be discovered by the SVM. However, only very few samples are necessary to generalize the behavior of most malware families. With only 10 samples in the training set, the average detection performance increases by more than 25 percent. Three families can even be detected perfectly in this setting.

A.RESULTS:

ALGORITHM: Semantics - aware malware detection techniques.



LOGIN & REGISTRATION

In this module both users can perform the login and the registration process. When the new user will register the User name, Password, and Confirm Password into the registration page. After registration the process, the next stage is login into the process, when the login page contains the user name and password field. When the users will give the correct data to login into the given application. For most of the feature sets, the construction of sentences from the templates in Table I is straightforward. For example, for the hardware features we make use of their naming scheme to construct meaningful sentences. If an application for instance uses the android .hardware. Camera feature, DREBIN presents the sentence ”App uses hardware feature camera.” to the user.

DATABASE CREATION.

Once the user will create the particular data's into this application, the data's will store int database. In this process we use the SQLite, it is an in-process library that implements a self transactional SQL database engine SQLite engine is not a stand alone process like other databases, you can link it statically or dynamically as requirement with your application. The SQLite access its storage files directly.

SCANNING FOR CORRUPTED FILES (LOADING FILES)

In this module , choose the path to scan for malware or any threads.

QUERYING THE SCANNED FILES (DETECTED FILES)

In this module, scan for malwares/threads in the selected folders/file DENY/ALLOW CORRUPTED FILES After finding the malwares in the scanned path remove the corrupted files/folders hen into the self-contained per your files.

V. DISCUSSION

It is used for smartphone malware detection and prevention In future effort will be focused on realizing this approach in practice and further evaluate it with a wide range of smartphones and internet users. Detect all files affected.
ALGORITHM**:** Semantics - aware malware detection techniques.

VI .CONCLUSION

In this paper, introduce a light weight permission enforcement approaches Tap-Wave-Rub (TWR) for smartphone malware detection and prevention. TWR is based on simple human gesture that are very intuitive but less likely to be exhibited in users' daily activities. Presence or absence of such gesture, prior to accessing a service, can effectively inform the OS whether the access request is benign or malicious.

REFERENCES

[1]Proximity Sensors. A description available at Wikipedia: http://en. wikipedia.org/wiki/Proximity sensor.
[2]Tap, Wave and Rub Magic. A description and video available at: http: //www.vinnymarini.com/download/tapwave.html.
[3]R.Amadeo. Exclusive: Android 4.2 alpha teardown, part 2: SELinux, VPN lockdown, and premium SMS confirmation. Available online at http://www.androidpolice.com/2012/10/17/exclusive-android-4-2-alpha-teardown-part-2-selinux-vpn-lockdown-and-premiumsmsconfirmation/, Oct. 2012.

[4]D.Arp, M. Spreitzenbarth, M. H¨ubner, H. Gascon, K. Rieck, and C. Siemens. Drebin: Effective and explainable detection of android malware in your pocket. In Proc. of NDSS, 2014.
[5]W.Augustinowicz. Trojan horse electronic pickpocket demo by identity stronghold. Available online at http://www.youtube.com/watch?v= eEcz0XszEic, June 2011.
[6]T.Baudel and B.-L. Michel. Charade: remote control of objects using free-hand gestures. Communication of ACM, 36:28–35, 1993.
[7]A.Bose, X. Hu, K. Shin, and T. Park. Behavioral detection of malware on mobile handsets. In MobiSys'08, 2008.
[8]I.Burguera, U. Zurutuza, and S. Nadjm-Tehrani. Crowdroid: Behavior based malware detection systems for Android. In ACM CCSW 2011.
[9]M.Calamia. Mobile payments to surge to $670 billion by 2015. Available online at http://www.mobiledia.com/news/96900.html, Jul. 2011.
[10]X.Cao and R. Balakrishnan. VisionWand: interaction techniques for large display using a passive wand tracked in 3D. In ACM UIST'03, 2003.