Activity Modeling and Threat Taxonomy for Context Aware Proactive System (CAPS) in Smart phones

Poonam N. Railkar, Parikshit N. Mahalle
Department of Computer Engineering
STES's Smt. Kashibai Navale College of Engineering
Pune - 411041, India

ABSTRACT

Mobile technology and Internet is becoming an integral part of our daily life. Widespread usage of smart phones and its greater in-built functionality have provided portability to perform transaction like shopping, ticket booking and banking transactions on the fly. In mobile computing, the characteristic like context awareness allows to provide proactively adapted services to user according to the context. Especially in combination with mobile devices, these mechanisms carries high value and are used to increase usability tremendously. Equally being an Android operating system as open source, it is prone to attack. In this view there is need to define new attack taxonomy and its modeling. This paper presents a novel taxonomy for Context Aware Proactive System (CAPS) in smart phone. This paper also presents activity modeling of proposed taxonomy to get an actual view of happening of attack like Cross Service attack, spyware and Battery Exhaustion attack. At the end this paper also discusses mitigation techniques to address few of the mentioned attacks.

General Terms

Security, Attacks.

Keywords

Threat, Taxonomy, Security Context, Context-Awareness, Mobile, Proactive system, Profile translation, Smartphone, Android, User profile.

1. INTRODUCTION

Advances in mobile technologies and internet access make users life very comfortable and convenient to do the work very intelligently. CAPS is android based context aware proactive system which manages user's whole profile information and gives abstract view of profile according to the current context requirements [1, 2, 3]. As whole profile information is stored at one place consistency of information will be maintained [4]. Profile of user will be in user's control and not of service provider. In this way it becomes convenient for user to update his profile. He can update his profile stored in the database and next time when he visits different websites, this updated information will be made available to that website proactively. Traditionally Internet uses client-server model. Client requests for some pages and server responds to client or client may give his information to server if required. This is a reactive model. To give more ease at the client end we can use concept of proactivity. Proactive service can be defined as giving response without explicit request. In proactive systems, user is provided with different suggestions according to the different situations. So proactivity means that the system pushes recommendations to the user when current situations seem appropriate [5]. To apply proactivity we should store user's information, situation or some rules (context) and to enhance proactivity, concept of context awareness is applied [6].

Context awareness is a potential mechanism for mobile devices as it can facilitate the device use in demanding situation by dynamically adapting the device behavior. Context awareness systems are also the component of ubiquitous environment and pervasive environment.

It has become common practice for retailers, banks, service providers, and just about everyone else to provide customers with a way of shopping on the Web. So every service is being computerized and made available to users online. Many users are using these online services through their desktops or through the Smart phones. Due to the emerging of centralized markets, we have seen an explosion in the number of applications for Smartphone. So here, concept of context aware proactive system is applied on android Smart phones to provide information of user proactively to the service provider [1, 2, 3].

Similarly, the open source nature of some of the leading Smartphone operating systems such as Android and Symbian are becoming the driving factor of attracting malware writers. Hence, the growing security problems of Smartphone's are becoming a real concern for users. The increasing popularity of Android is drawing the attention of more and more enterprises to deploy their custom applications and services for Android and allow employees to download data for viewing and/or editing on their mobile devices [7]. However, as mobile devices turn to be more business oriented, rather than simple devices to make and receive calls, their practicality is counterbalanced by an escalating number of security issues.

Due to this SMS Trojans are aggressively being developed. The number of threats for Android is growing extensively. Malicious users are violently exploiting vulnerabilities. Spyware is now causing a host of problems for mobile device users [8].

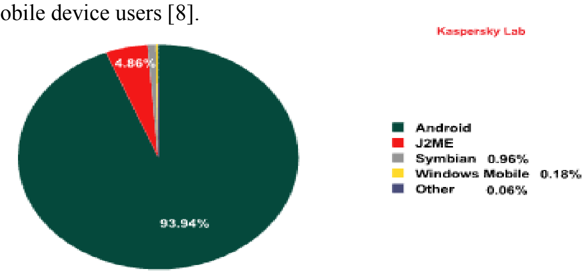

Fig 1: Distribution of mobile threats by platform, 2004 – 2012

According to Kaspersky Laboratory distribution of mobile threats by platform are shown in figure 1.

This paper is structured as follows. Section II presents detailed study of Android architecture and about its current security model. Section III presents the related work in attack modeling for smart phone and discusses the evaluation of related work. Section IV presents the proposed attack taxonomy for CAPS for smart phones. Section V presents the behavioral modeling using activity diagram by unified modeling language to get an actual view of how attack happens. Section VI presents mitigation techniques to address few of the attacks. Finally section VII concludes with the future work.

2. BACKGROUND

2.1 Android Architecture

The following diagram shows the major components of the Android operating system [9].

Android has become one of the most prominent open source platforms for handheld devices. It is not just an operating system rather a complete software stack consisting of operating system, middleware and a number of built-in applications.

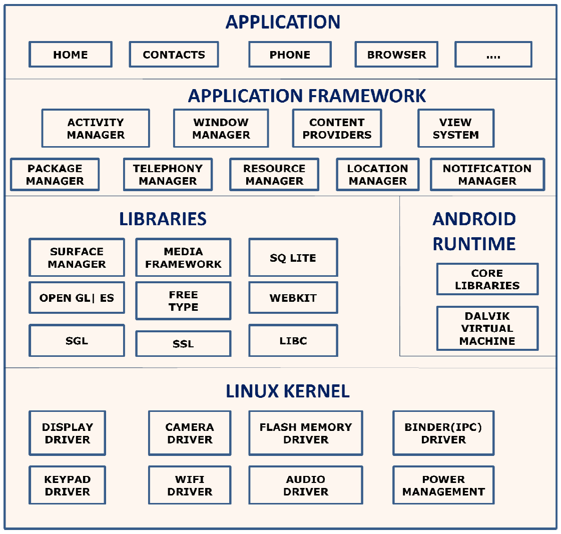

Fig 2: Component of Android Architecture

Its architecture is composed of different yet interacting layers (Figure 2). The lowest layer in the Android's architecture is the Linux Kernel that contains hardware drivers and performs low-level functionalities like memory management, threading and power management. This layer is include an Android specific component known as Binder, which is responsible for performing communication between different application components. The upper layer is composed of a set of C and C++ libraries that contains graphic libraries, an SQL engine, some customized C libraries, media codecs and web browser engine. The next layer is the Android runtime that contains Android specific virtual machine and some core libraries. The Dalvik virtual machine is designed specifically to run compact and memory efficient executables. It's an important design decision for battery powered and low memory devices. Next is the Android application framework layer that provides an API to allow applications interaction with each other and with the hardware. Above the framework layer the applications layer is present that contains a number of pre-build and user defined applications [7, 9].

2.2 Android Security Mechanism

Some of the core security features that help to build secure apps which include [7, 10]:

- The Android Application Sandbox, which isolates your app data and code execution from other apps. The underlying Linux kernel enforces process isolation and discretionary access control to resources (files, devices) by user ownership. To sandbox applications, every application instance in Android is assigned a unique user identifier (UID), while system resources are owned by either the system or root user. Applications can only access their own files, or files that are explicitly defined as world-wide readable [18].
- An application framework with robust implementations of common security functionality such as cryptography, permissions, and secure IPC.
- Technologies like ASLR, NX, ProPolice, safe_iop, OpenBSD dlmalloc, OpenBSD calloc, and Linux mmap_min_addr to mitigate risks associated with common memory management errors.
- An encrypted filesystem that can be enabled to protect data on lost or stolen devices.
- User-granted permissions to restrict access to system features and user data.
- Application-defined permissions to control application data on a per-app basis.

3. RELATED WORKS

A lot of work has been done in the area of smart phone security and context aware proactive system.

Schilit and Theimer [11] introduced the term 'context aware' first time. Context-aware computing was discussed by them in 1994 to be "software that adapts according to its location of use, the collection of nearby people and objects, as well as changes to those objects over time." This definition is more specific claimed by Dey. Dey defines more general definition of context as "Context is any information that can be used to characterize the situation of an entity [12]." An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves [13].

In [7] authors have analyzed the current security mechanism of one of the most anticipated open source smartphone platform – Android. They also discussed the vulnerabilities and limitations in the current security model in detail especially the application permission mechanism. Article [14] includes the list of best practices for Android; BlackBerry and iOS to mitigate and/or prevent unauthorized access, loss of information, and loss of confidentiality. In paper [15] author proposes a context-based remote security control scheme for Mobile Communication Device (MCD). Their proposed scheme consists of two systems: Context-based Mobile Security (CMS) client and server. The proposed scheme can automatically not only protect the MCD from cyber attacks, but also prevent the MCD from being used as an attack tool, by help of CMS server.

Smartphone's data protection problem in a user-centric way, and analyze the requirements of data protection systems from users' perspective are discussed in [16]. In [17] authors analysed Smartphone malware detection techniques literature. They have provided structured and comprehensive Smartphone malware detection techniques taxonomy.

In nutshell, evaluation of the related work shows that, Smartphone security and essentially in the context of CAPS needs more focus. In this view there is a need of attack classifications and activity modeling of these attacks.

4. ATTACK TAXONOMY FOR CAPS

4.1 Proposed Architecture of CAPS

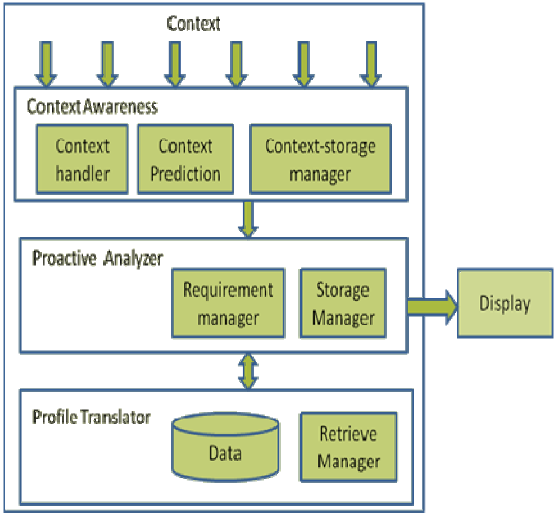

Figure 3: Proposed System Architecture for CAPS [1], [2], [3]

The Figure 3 summarizes layered architecture for the proposed system which incorporates interrelated functionalities. The detailed description of each layer is as follows.

- **Context Awareness Layer**

Context is taken as main input to the system. The basic task of context handler is to recognize the current context in which user is operating. Recognition of context can be done by checking stored context. Sometimes it may happen that the user is using that app first time or navigating the new web site. Now, if user is in new context then the whole data is passed to Context Predictor. Context Predictor checks if this current context needs the profile to be generated. If require then this context is passed to Context Storage Manager. Context Storage Manager stores new context or updates previous data according to the situation. This way, first layer recognizes the context that is nothing but the situation awareness and suggests if current context is appropriate for profile translation. And finally forwards this contextual information to the next layer.

- **Proactive Analyzer Layer**

It takes the contextual information which is provided by upper layer. The Requirement Manager in this layer will gather all the required information of the profile. This is done without user's request which is nothing but extracting the requirements from the context proactively. Here, best results can be achieved by properly examining the current context and gathering results accordingly. After this accumulation, the data is pushed to the next layer.

- **Profile Translation**

The layer takes the requirements from second layer via Retrieve Manager. It will check if those user requirements are fulfilled by the database. If the user requirements are satisfied then it creates the abstract view of profile. The layer will pass this abstract view to the Display Manager from Proactive Analyzer Layer. It will display the view proactively.

For secure profile translation authorized user can access this web app with authentication. And also cannot update profile without login to the system.

4.2 Proposed attack taxonomy for CAPS in smart phones

The proposed attack taxonomy for CAPS for smart phones is shown in figure 4.

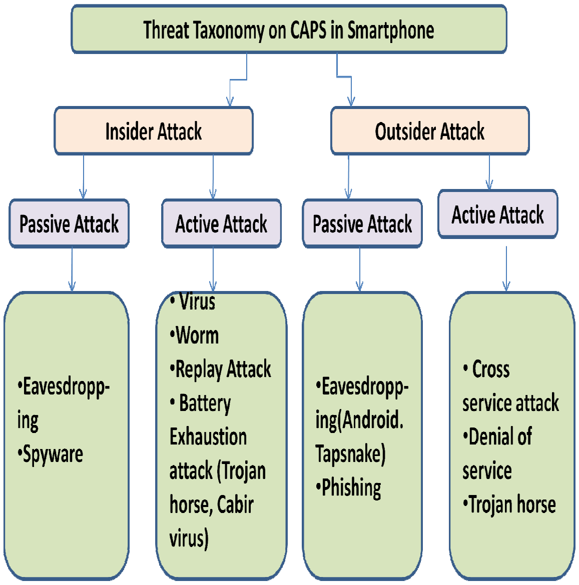

Figure 4: Proposed attack taxonomy for CAPS

These threats are classified into two types: Insider Attack & Outsider Attack. Again both of these are classified as Passive Attack & Active Attack.

Spyware gathers information about a user without their knowledge and that may send such information to another entity without the customers permission. Trojan and Worm target to popular Smartphone platforms with an objective to steal or damage users' data. Android.Tapsnake works as Eavesdropping which reports GPS location of the server to the phone. Because of the Trojan horse and Cabir virus, Battery Exhaustion attacks can occur. Phishing perform to acquire information such as Credit card details, Password etc. Denial of service attack is an attempt to make mobile unavailable to others. Over-charging, spam, phishing, and battery-consumption attacks occur because of Cross service attack.

5. PROPOSED ACTIVITY MODELING OF THREATS ON SMARTPHONE

In figure 5 below, the malignant attacks, in which a virus or Trojan horse is used to make the device consume significant power. The benign attacks, in which an unmodified program is given pathological data such that the program consumes excessive energy, and in service request attacks, a special form of the benign attack in which repeated requests are made to a network service provided by the device.

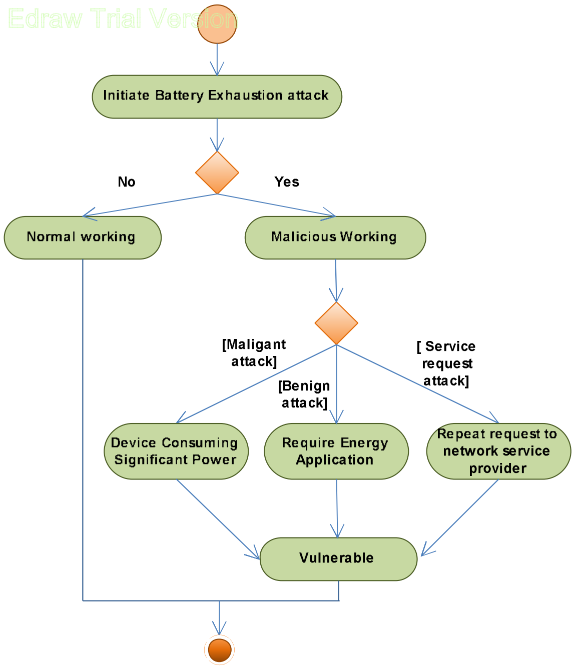
Edraw Trial Version
Initiate Battery Exhaustion attack
No
Yes
Normal working
Malicious Working
[Maligant attack]
[Benign attack]
[Service request attack]
Device Consuming Significant Power
Require Energy Application
Repeat request to network service provider
Vulnerable

Figure 5: Activity modeling of Battery Exhaustion attack

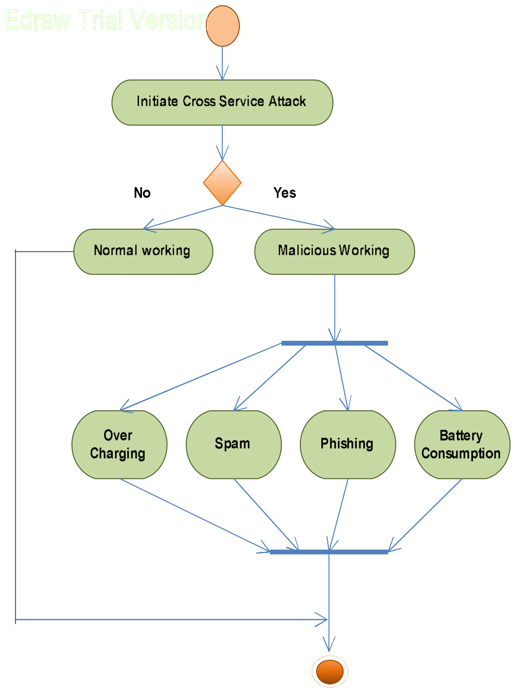

Figure 6: Activity modeling of Cross Service attack

As shown in figure 6, Cross-service attack occurs because the service architecture of Smartphone allows attacker to cross service boundaries. A cross-service attacker makes an intrusion on a Smartphone through the most vulnerable communication interface among the ones that it provides, and then exploits the other communication interfaces. This attack may result in over-charging, spam, phishing, and battery-consumption attacks.

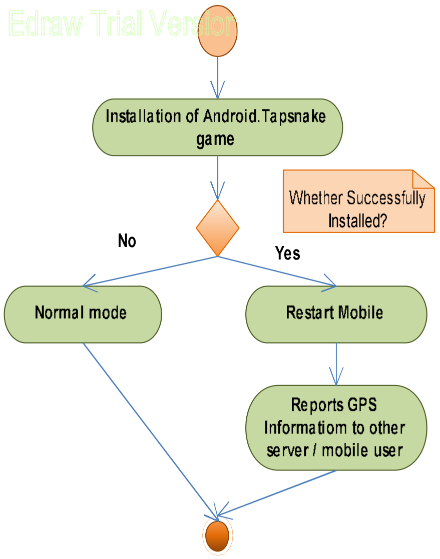
Edraw Trial Version
Installation of Android.Tapsnake game
Whether Successfully Installed?
No
Yes
Normal mode
Restart Mobile
Reports GPS Informatiom to other server / mobile user

Figure 7: Activity modeling of Installation of Android.Tapsnake

As shown in figure 7, if Android.Tapsnake game is installed properly on the mobile, then your friend or other users will get your GPS /location information. It also increases the user privacy issues.

6. MITIGATION TECHNIQUES

Following certain steps or practices will substantially reduce the probability of attacks.

- **Kirin:**

Enck, et al. [19] have proposed a framework knownas Kirin – install-time certification mechanism – that allows the mobile device to enforce a list of pre-defined security requirements prior to installation process of an application. During installation of an application the Android framework informs the user regarding the resources that can be accessed by the application but it cannot reflect the possibility of using different combinations of permission in a malicious manner. The Kirin framework is contacted when installation process for an application package is initiated. Kirin utilizes the application's manifest file where all the required permissions are listed and uses the action string along with the permissions to construct a set of Prolog facts. Kirin also modifies the Android application installer that can be used to prompt user with statements of risk rather than simply showing them the permission list at install time, it can also be used to deny installation of an application if certain conditions are met.

- **Data Encryption:**

Smartphone is also very vulnerable to loss, theft, and using by stealth attacks because it is a portable device, thereby being exposed to threats of important data leakage. To protect Smartphone from data leakage attacks, there must be some security functions such as a data encryption.

- **Authentication Methods:**

Use Authentication methods in your Smartphone such as, Fingerprint Authentication, Retina Scan, Recognition Based Authentication, Speaker Recognition, Face Recognition [20].

- **Disable Unknown Source for application installation:**

Being an open platform, any third party vendor can develop an application for the Android platform. Applications available outside the Play Store (previously called Android Market) are at a high risk of containing potentially unsafe programs that could cause serious threats. Best practice for a user is to avoid downloading applications from third party websites [14]

- **Install Anti-Virus protection:**

Anti-virus applications have been designed to prevent malicious applications from being installed and to detect installed malware.

- **Turn off wireless features (GPS, Bluetooth, Wi-Fi and Portable Hotspot) when not in use**

Connecting to unknown and unsecured networks or devices may lead to serious threats. Best practice is to turn-off these settings when they are not in use.

- **Backup data on the device**

Frequently back-up data on the device to prevent loss of information or in case of stealing of mobile. The 'Back up my data' features allow users to copy current application data to remote Google cloud storage. If a factory reset is performed on the device, application data can be automatically restored from the cloud backup. Sync all contacts, calendar and other information with the Gmail account, which will act as a data backup. Alternatively you can also use other applications from the Play Store to backup phone content [14].

7. CONCLUSIONS AND FUTURE WORK

As the use of smart of phones for M-commerce on the fly is increasing at faster rate, there is need making this amalgam context aware with proactivity introduced. Equally, it is also important to make this transaction secure due to less user intervention. This paper has proposed novel attack taxonomy for CAPS in smart phones. With the thorough analysis of the state of the art in smart phone security, conclusion is drawn in this paper that there is a need of behavioral modeling of few of the attacks. In this view, this paper has also presented activity modeling of these attacks with the activity diagrams using Unified Modeling language. Finally this paper has also presented mitigation techniques to address few of the aforementioned attacks like Cross Service attack, spyware and Battery Exhaustion attack

Future plan is to design efficient and lightweight protocols and schemes to address these attacks. Verification of these protocols using security protocol verification tool and its implementation is also another future outlook.

8. REFERENCES

[1] Poonam N. Railkar, Parikshit N.Mahalle, "Proposed secure context aware profile translation" IJITS, Vol. 1; No. 2: ISSN: 2277-9825

[2] Ketaki Shah, Anuja Raundal, Gouri Bhandari, Santwana Rathi, Poonam Railkar ,Parikshit Mahalle "Proposed profile translation In context aware proactive system" IJCSE ISSN : 0976-5166 Vol. 3 No.6 Dec 2012-Jan 2013

[3] Poonam N Railkar, Parikshit N Mahalle, "Proposed Profile Translation based Proactive Adaptation using Context Management (PTPACM) in Smartphones", pp 356-361 2013 3rd IEEE International Advance Computing Conference(IACC),Feb 2013

[4] Wuest, Bjoern; Droegehorn, Olaf; David,Klaus, "Architecture for profile translation", IST summit 2005, 12.

[5] Daniel Gallego Vico; Wolfgang Woerndl; Roland Bader "A Study on Proactive Delivery of Restaurant recommendations for Android Smartphones". In ACM Recsys Workshop on Personalization in Mobile Applications, Chicago, USA, October 2011

[6] Jaewoo Chang; Sora Na; Min Yoon; "Intelligent Context-Aware System Architecture in Pervasive Computing Environment", Parallel and Distributed Processing with Applications, 2008. ISPA '08. International Symposium on , vol., no., pp.745-750, 10-12 Dec. 2008

[7] Khan,S. ; Nauman,M. ; Othman,A.T. ; Musa,S. "How Secure is your Smartphone: An Analysis of Smartphone Security Mechanisms" IEEE, Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012

[8] Mobile Malware Evolution: Part 6 Available from: http://www.securelist.com/en/analysis/204792283/Mobile_Malware_Evolution_Part_6#8

[9] "Android Reference: Application Fundamentals-Components," available at: http://developer.android.com/guide/topics/fundamentals.html.

[10] "Android Reference: Security and Permissions," available at: http://developer.android.com/guide/topics/security/security.html.

[11] Dey, Anind K.; "Understanding and Using Context", Personal ubiquitous comput., Springer-verlag, vol. no., 5, pp.4-7,25 July.2007

[12] Dey, A.K. Abowd, G.D. "Towards a Better Understanding of Context and Context-Awareness", CHI 2000 Workshop on the What, Who, Where, When, and How of Context-Awareness (2000)

[13] Hofer T.; Schwinger W.; Pichler M.; Leonhartsberger G.; Altmann J.; Retschitzegger W.; "Context-awareness on mobile devices - the hydrogen approach", System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on , vol., no., pp. 10 pp., 6-9 Jan. 2003

[14] Tae Oh ; Stackpole, B. ; Cummins, E. ; Gonzalez, C. ;Ramachandran, R. ; Shinyoung Lim "Best Security Practices for Android, BlackBerry, and iOS", First IEEE Workshop on Enabling Technologies for Smartphone and Internet of Things (ETSIoT), 2012

[15] Gaeil An ; Daehee Seo ; Jonghyun Kim ; Kiyoung Kim ;Dongil Seo "Context-based Remote Security Control for Mobile Communication Device", IEEE, International Symposium on Communications and Information Technologies (ISCIT), 2010

[16] Muslukhov, I. ; Boshmaf, Y. ; Kuo, C. ; Lester,J. ; Beznosov, K. "Understanding Users' Requirements for Data Protection in Smartphones", IEEE 28th International Conference on Data Engineering Workshops (ICDEW), 2012

[17] Amamra, A. ; Talhi,___C. ; Robert,___J. " Smartphone Malware Detection: From a Survey Towards Taxonomy", IEEE 7th International Conference on Malicious and Unwanted Software (MALWARE), 2012

[18] Sven Bugiel, Lucas Davi, Alexandra Dmitrienko, Thomas Fischer, Ahmad-Reza Sadeghi, Bhargava Shastry, "Towards Taming Privilege-Escalation Attacks on Android", 19th Annual Network & Distributed System Security Symposium (NDSS) 2012.

[19] W. Enck, M. Ongtang, and P. McDaniel, "On lightweight mobile phone application certification," in Proceedings of the 16th ACM conference on Computer and Communications Security. ACM, 2009, pp. 235–245.

[20]Dorflinger,T. ; Voth, A. ; Kramer,J. ; Fromm,R. "MY SMARTPHONE IS A SAFE!" The User's Point of View Regarding Novel Authentication Methods and Gradual Security Levels on Smartphones", IEEE, Proceedings of the 2010 International Conference on Security and Cryptography (SECRYPT).