A Survey on Security for Smartphone Device

Syed Farhan Alam Zaidi
Department of Computer Science
COMSATS Institute of Information Technology,
Islamabad, Pakistan

Munam Ali Shah
Department of Computer Science
COMSATS Institute of Information Technology,
Islamabad, Pakistan

Muhammad Kamran
Department of Distance Continuing & Computer Education
University of Sindh, Hyderabad,
Pakistan

Qaisar Javaid
Department of Computer Science & Software Engineering,
International Islamic University,
Islamabad, Pakistan

Sijing Zhang
Department of Computer Science & Technology
University of Bedfordshire,
Luton, UK

***Abstract*—The technological advancements in mobile connectivity services such as GPRS, GSM, 3G, 4G, Blue-tooth, WiMAX, and Wi-Fi made mobile phones a necessary component of our daily lives. Also, mobile phones have become smart which let the users perform routine tasks on the go. However, this rapid increase in technology and tremendous usage of the smartphones make them vulnerable to malware and other security breaching attacks. This diverse range of mobile connectivity services, device software platforms, and standards make it critical to look at the holistic picture of the current developments in smartphone security research. In this paper, our contribution is twofold. Firstly, we review the threats, vulnerabilities, attacks and their solutions over the period of 2010-2015 with a special focus on smartphones. Attacks are categorized into two types, i.e., old attack and new attacks. With this categorization, we aim to provide an easy and concise view of different attacks and the possible solutions to improve smartphone security. Secondly, we critically analyze our findings and estimate the market growth of different operating systems for the smartphone in coming years. Furthermore, we estimate the malware growth and forecast the world in 2020.**

Keywords*—Smartphone Security; Vulnerabilities; Attacks; Malware

I. INTRODUCTION

The smartphone usage raised significantly in recent years, as smartphones provide users with several services like phone calls, Internet services, sharing data, keeping data, off-line games, online games, and some entertaining online/ off-line applications. As smartphone provides the vast services, thus are saddled with some challenges like security and privacy as well. Since most of the operations smartphones perform are on the Internet, so it is necessary to ensure security and safety of data and information. For smartphone authentication, a pattern like password, code password, PIN password, and face unlock can be used [1]. But these authentication methods are not secured at high ratio because with brute forcing and guessing such measures could be penetrated.

Critically, a lot of Malware, Viruses and Trojans have been developed which are based on smartphones APIs (application program interface) and most of them look like safe software; some reliable applications (Gmail, Facebook, etc.) collect user's information such as geolocation without user's knowledge with GPS service in smartphone [2]. There are many smartphone operating systems available, such as Android, iOS, Microsoft Window Phones, Symbian and BlackBerry [1]. Android is the widely used smartphone operating system with better performance as compared to other smartphone operating systems. Android OS is based on Linux operating system architecture. The desktop OS and the smartphone versions of such operating systems are very different, especially in user interfaces and system architecture. Using smartphones one can connect to the Internet and instantly communicate with friends, partners and browse data/information from the world wide web [3].

Now, smartphones pair mobile phones with other devices such as PDAs (personal data assistants), high definition camera, media player, GPS navigation units and other data storage and processing devices. Even the earlier mobile devices came with 3G and 4G compatibilities; but in the last decade, such devices transformed into mobile computers with the options of touch screen and laptop capabilities and can browse the Internet using wireless network and 3rd party applications. In the 3rd quarter of 2012, more than one million smartphones were in use [2]. According to Gartner Inc., the worldwide sales of mobile phones declined 3%, and smartphones sales were increased by 47 % in the 3rd quarter of the year 2012 [4]. In November 2012, 821 million smart devices were purchased in 2012 and 1.2 billons were sold in 2013 [5]. In August 2013, the smartphones sales were increased, and the growth was 46.5 % [6]. Some reports state that China with the highest number of smartphone users (519 million in 2014) [7]. The United States comes to the 2nd position with 165.3 million users and India to 3rd on the rank with 123.3 million users.

A. General Architecture of Smartphones

Smart devices are grouping of mobile phones and platform with rich connectivity and powerful computing proficiency. Therefore, a smartphone has the necessary modules of computing platforms, operating systems, third-party applications and smartphone hardware architectures, as shown in [8]. Unlike Android, the iOS operating system works only on iPad, iPhone, and iPod devices. To manage all operating

systems and devices, the OS provide necessary technology and interface and support to implement the new application to meet a variety of smartphone user needs.

The applications allow smartphone users to control their devices by interacting with the operating system, by such interaction users can access and control data communication interfaces and services. On another hand, the operating system can access user data and communicate directly with other services as well as devices. In general operating system can only access hardware directly, but the access to user's data might result in compromising user information and the information from the smartphone can be maltreated by attackers just like attacks on the computer such as viruses, Trojans, etc. The user data or information is the most valued property of smartphones. As discussed earlier, besides communication, smartphones connect to several other electronic devices such as computer and even servers through the Internet. The data without user's knowledge is usually retrieved through the applications infested by malicious codes or programs [8].

B. Structure of Smartphones Operating System

There are many operating systems for smartphones. In this part, we discuss Android, iOS, Windows Phone and Symbian operating system.

Android: Android is an open source mobile operating system which is based on Linux OS kernel and launched by Google. Android contains four layers including kernel, libraries, Android Runtime and Application framework. Application layer consists of all Android applications including email, SMS program, instant messaging, browsers, contacts and other various applications their names list is longer than few pages [9][10]. According to the authors in [11] and [12], application framework layer recognizes all Android applications. Libraries layer is divided into two parts: Android and Android runtime library. Android runtime combines the assets of the Java Virtual Machine and machine Dalvik. Android library consists of C / C ++ language.

iOS: The iOS is an operating system for Apple devices developed by Apple Inc. One obvious example is iPhone which was released in 2007. Now, iPhone is one of the larger competitors to the smartphone market shares. Application of Apple phone will need computer running MAC OS [13]. Like Android, new iOS has been developed for third party to overcome the capability limitations of platform [14].

Windows Phone: Microsoft Corporation has developed Windows phone operating system. In November 2011 [15], many devices has been built up for this OS including Nokia Lumia 800 and HTC Titan. After one year, Windows became the fourth most widely used operating system on the smartphone. Windows uses Android operating system like security model.

Symbian: PSION was established in 1980 before the Symbian. In 1990 [16], Symbian was created by Psion, Nokia, and Motorola. After that, some other vendors joined this corporation like Sony Erickson, Siemens in 2002. First, Symbian mobile platform was released in 2000 (EricksonR380) then Nokia announcement couple of versions (like Nokia N series). Symbian was developed with C++.

Almost all the smartphone OS provide mechanisms for users to enhance the security of their devices by certain login mechanisms. However, more than 30%, Mobile phone users do not use the PIN on their Phones. On the other hand, the amount of high valued contents stored on the phone is rapidly increasing, with mobile payment and money transfer application as well as enterprise data becoming available on mobile devices [17]. The statistical data obtained from sources [18] & [19] have been computed and represented in Table 1.

TABLE I. SMARTPHONE ESTIMATION BY OS 2014 SHIPMENT AND MARKET SHARE 2018

Vendor	2014 Shipment Values (Million)	2014 market % share	2018 Shipment values (Million)	2018 market % Share	Growth
Android	950.5	78.9 %	1321.1	76.0 %	10.7 %
iOS	179.5	14.9 %	249.6	14.4 %	10.2 %
Windows Phone	47.0	3.9 %	121.8	7.0 %	29.5 %
Black-Berry	11.9	1.0 %	5.3	0.3 %	-22%
Others	15.1	1.3 %	40.7	2.3 %	32.7 %
Total	1204.4	100.0 %	1738.5	100.0 %	11.5 %

To understand the existing security problems that distress smartphones, we examined the threats, vulnerabilities, targeted attacks on smartphone and study security solutions to protect them. Attention has also been paid to authentication issues, data protection and privacy issues. In this study, the review of related literature is made over the period of 2010-2015, by concentrating on smartphones vulnerabilities (issues that cause the attacks) and attacks (old and new attacks).

The paper is organized as, Section II introduces some background ideas and previous studies regarding the authentication problem, data protection and privacy, smartphone vulnerabilities, and attacks. The smartphone attacks are divided into two categories: Old attacks and new attacks. Section III evaluates the related works discussed in Section II. In this section, we summarize the old and new attacks, causes of attacks (vulnerabilities) their impact and solution to protect the smartphones. Section IV is a discussion; we discussed some open issues and possible future problems of smartphones in IoT (Internet of things). Finally, Section V draws some conclusion.

II. SMARTPHONE PROBLEMS

Powerful hardware, advanced operating system, latest applications, increasing capabilities of smartphone and functionality are enough, but an increase in present security threats in smartphones became a prominent issue. Other features of the smartphone such as broad bandwidth accelerators of the Internet, multiple peripheral interfaces also spreading viruses over the network. The multi-connectivity

gains high risk and make it easier to transmit viruses those may be aggravate threats [20][21]. The security challenges in the mobile environment are similar to the problems encountered in the personal computer world. Threat means possible destructions of smartphone security. Considering that the smartphone problems can be categorized into four categories: Authentication, Data Protection and Privacy, Vulnerabilities and Attacks. Fig.1 shows such categorization of smartphone security problems.

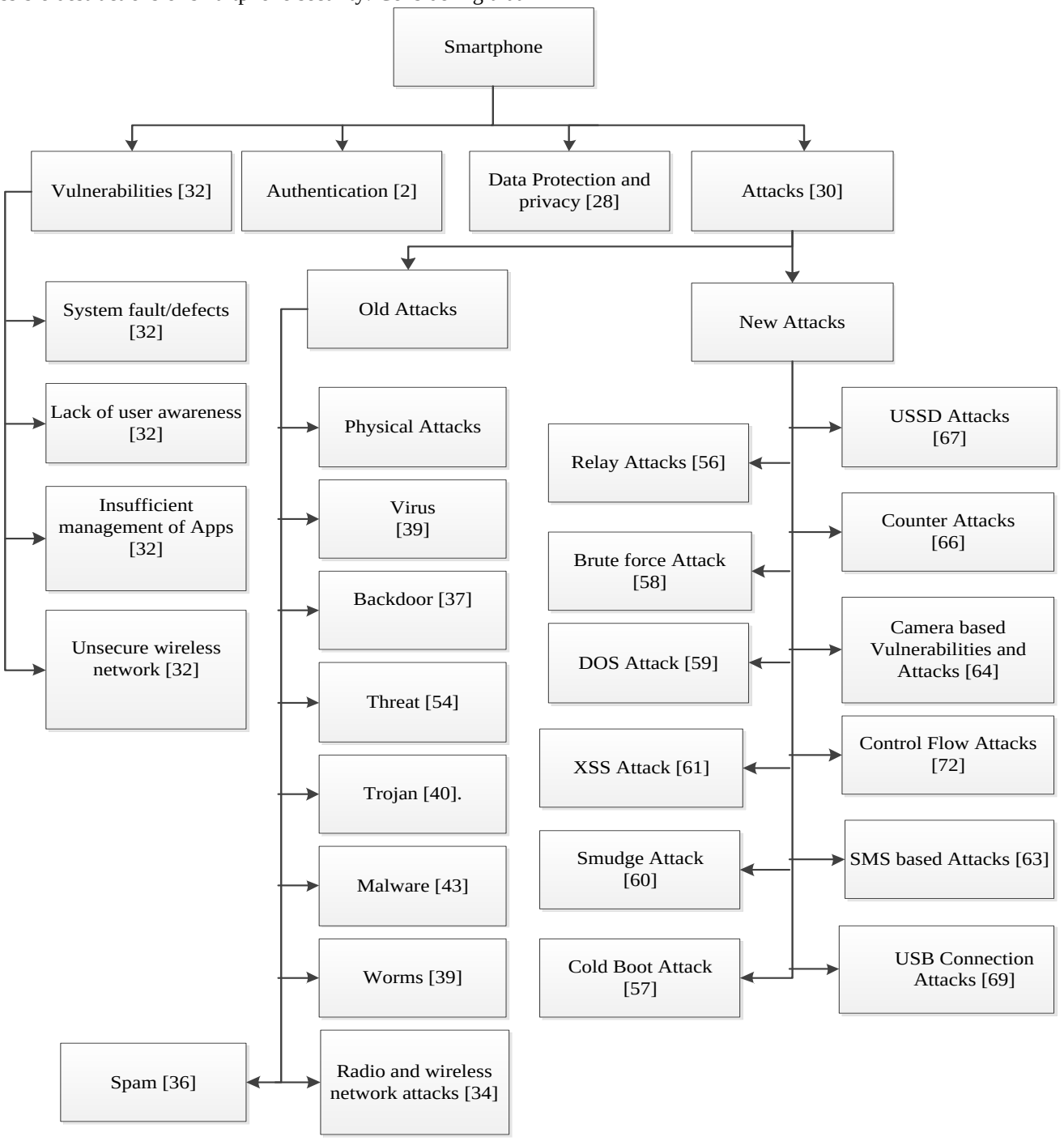


Fig. 1. Categorization of Smartphone Problems

A. Authentication in Smartphones

Authentication could be achieved using one of the following three methods. The first one is to use what users knows such as PIN or password. The second method is which users have certain code such as a token. The third method is commonly known as biometric. After introducing the general architecture of smartphone and its main parts or assets, we classify smartphone's security threats and vulnerabilities. In the study [2] the authors proposed a hierarchy of security

framework, consists of hardware, operating system application user data, communication as security.

Wei-Han proposed a multi-sensors-based system for smartphones to achieve the implicit authentication. The system incessantly learns the user's behavior patterns and setting by allowing the user to use a phone without disturbing the user's actions. This approach also has the capability to update user model. The experiment shows that the efficiency of this model only requires 10 seconds to run the model, 20 seconds to detect abnormal or fake request. In this model, the level of accuracy achieved can reach up to 90-95% [22].

Zahid *et al.* [23], proposed the user identification system to monitor the mobile phone key users to distinguish authentic consumers from quacks dynamically. The authors used custom data set of 25 users to point out the suggested system. That gives the fault rate lesser than 2% after detection mode, and the election of nearly zero after PIN authentication. They also connected their approach with five state-of-the-art procedures existing to identify basic user keystroke.

Authors in [24], suggested TAP *(Typing authentication and protection),* a virtual key based on a typing system for smart devices. There are two steps to improve the security of mobile by TAP, first is the login stage and second is the post login stage. In the first phase, TAP controls biometric information and hand morphology to secure the user's identity. In the second phase, TAP controls the dynamic behavior of the TAP Virtual user key. The experiments demonstrated that TAP preserves security and usability for the smartphone devices.

Chine-Cheng *et al.* have suggested the non-intrusive authentication method that uses the collected information from the orientation sensor of mobile devices. It is a new tactic that is operated by user's smartphone in its own unique way, and orientation sensor captures this type of behavioral biometrics. They use stepwise linear regression to select the feature set for each user. For classification, they used the k-nearest neighbor algorithm. The experimental results show equal error rate about 6.85% in method suggested. Their authentication model satisfies the performance that varies 3 to 8 different end users. The authors conclude that the non-intrusive mechanism can be used with the intrusive mechanism. For example, PIN or Password can be used with the biometric (finger-prints) to increase the security of smartphones [25].

Morris worked on combining traits from three different methods, i.e., biometrics, hand-written signature, face, and modalities of speech. He reported the authentication accuracy of a mobile device that would have been acceptable with a wide range of applications [26]. According to Gobbo *et al.* [27], SIM allows the user to access the network; make the user registration and authentication devices. Without a valid SIM module and a successful verification, mobile devices do not have access, so all the traffic on mobile infrastructure cannot inject. Firstly, SIM that enables the collection of resources is needed to launch an attack without disrupting users and risk found; secondly, the use of devices that are not in ownership of naive users can take part in the attacks as a botnet network nodes.

B. Data Protection and Privacy

Boshmaf *et al.* [28], address the problem of data protection from user-centered perspective and analyzed the user's need for data protection for smartphones systems. The authors outlined the types of data that users want to protect; they also investigated the practices of current users in the protection of such data and show how the security requirements vary across different types of data. They report the results of an exploratory study of the user in which 22 participants were interviewed. Overall, it was found that users want to protect the data on their smartphones, but find it inconvenient to do it in practice, by using the available solutions today.

Muslokhlove presents the problems of data protection against physical threats and possibility to overcome weak authentication. In that study, user's requirements to data protection are highlighted after interviews and survey studies. Finally, the author concludes that detection malicious data access approaches are not covering enough security although there remain several vulnerabilities but for data traffics these approaches are good. Upgrading the lock screen system for supporting authentication and user's accessibility and provide suitable security will increase the confidence of user and safety of smartphones [29].

Ghosh *et al.* worked in the context of privacy, protection and user data regarding semantic reasoning and user context modeling. In this work, the authors state that the privacy of users and smartphone under this framework are protected using embedded semantic policies that are based on the user's privacy and settings [30]. Kodeswaran *et al.* [31] have shown a framework to execute the privacy policies on smartphones, and to protect the enterprise data. The authors have defined their privacy policies of acceptable information flow on mobile devices. This flow of information depends on the object involved in conforming IPC (Inter-Process Communication) and its data. They have described their framework design which is based on policies for Android platform and have shown the results measuring executed by the framework.

C. Vulnerabilities

There are many several attacks and vulnerabilities in smartphones as shown in Fig. 1. According to [32] Smartphones have many vulnerabilities that can lead to insecurity or be victimized by malicious attackers to create attacks. Smartphones vulnerabilities include the following: System fault/defects, insufficient management of applications, insecure wireless network and lack of user awareness.

- System Fault / Defects

It is inconceivable for a smartphone to avoid both hardware and software defects. Such defects are only reveals after the device usage. Some defects can be observed / identified sooner and some later. The software defect can easily be corrected but the hardware faults may cause irregularities, and can be rectified by changing the hardware or by changing the device architecture. Such defects can be exploited by the attackers to initiate the attacks on smartphones.

- Insufficient Management of Apps

Most distinctive feature of the smart devices is their flexible APIs which are mostly used for application development. However, deficient API management is responsible for many malicious code infections. Thus, the API mismanagement is a main reason for malicious code attacks. APIs are classified into Open APIs, third party application development and control APIs; used to remote maintenance. Controlled APIs have particular higher privileges for updating system, file destruction, and information fetching. If attackers gain the APIs control, could easily initiate attacks and exploit the privileges of the APIs [32] [33].

- Unsecure Wireless Network

In wireless network, we use Wi-Fi technology, Bluetooth, cellular network and GPS to connect with any network or Internet. On any network device hacker can retrieve or fetch the packets on the network. So it is a vulnerability, and we can overcome it by using the encryption/decryption method in communication.

- Lack of User Awareness

User awareness to the security is important all the times especially when the smartphone is connected to the Internet for installing an unknown application or downloading data from insecure sources. There are many application available online that look like a legitimate source, but their save button is linked to some malicious codes. Also, activating wireless and Bluetooth interfaces can be executed secretly. Using protected access 2(WPA2) based on IEEE 802.11i is a new security protocol ensuring that only authorized users can access the network [32].

D. Attacks of Smartphone

Attacks are common in all computing devices and smart devices such as smartphones, tablets, etc., in the coming lines we will explain important attacks to the smartphones. The attacks are classified into two categories:

- *Old Attacks*

In this category, the most common attacks have been discussed. It includes physical attacks, viruses, worms, Trojans, malware, etc.

Physical Attacks: Smartphones and tablets are easily lost or stolen. Then, Sensitive data can be accessed and manipulated directly. Physical attacks also damage fallen or covering harmful disposals.

Radio and Wireless Network Attacks: Because the accessibility of wireless communication intruders can create wireless network attacks, they could be grouped into active attacks (Spoofing, corrupting, blocking and modifying) and passive attacks (sniffing and eavesdropping). Passive eavesdropping, the information is detected by listening to the message communication in the broadcasting wireless medium using malicious nodes. In wireless attackers create a fake Wi-Fi network to connect other users, thus, a common advice for smartphone users is to beware of what networks they are connecting to and using if it appears a fake wireless network; immediately disconnect and it is also a good practice to Switch off Wi-Fi sensors [34].

Jermyn and Zonunz,[35] studied the DoS attacks on the LTE and MAC uplink scheduler that cause several attacks. They state that such attacks depend on the QoSs (Quality of Services) requested by the clients. The authors proved the feasibility of suggested attacks on the Android-based simulator. C. Guo *et al.* [36], warm about the dangers of potential smartphone attacks to telecommunication infrastructure, the damage that can range from invasion of privacy and identity theft to emergency harassment centers that can result in a state of crisis. The authors outline various defensive strategies, many of which require a lot of research. It is also suggested to the system architect to concentrate on Internet insecurity in bringing new hardware to the Internet.

Backdoor: Backdoor accepts attackers to establish a connection with their network while evading detection [37]. Research has revealed many backdoor uses in target attacks. Backdoors result mainly from a system, bug, and revelation of controlled APIs. Some of smartphones come with insufficient authentications, based on these vulnerabilities. Backdoor bypass access to the attacker in a normal security [38]. Example Netcat and Virtual network security.

Virus: Virus infects executable files, boot sectors and normal files such as word processing documents, PDF, etc. The virus makes replication to the file with consuming the capacity of the system. Viruses also give a link to an unknown source like installation software without a request from a user [39]. Cheng and Lu [40], introduce a *virus detection system* and alert system for smartphones. This system detects viruses from the information of communication actions. They study the unusual behavior of the smart device, and develop a *SmartSiren* system and grab the result to show that the developed system avoids viruses effectively with reasonable overhead.

Worms: Worms are the programs that transport their copies from one device to another device with the help of different transport mechanism throughout the network without user interference [39] [41] [42].

Malware: Malware attacks harm smartphones by creating an application and provide it to a user to download that application, but that application is a malware. Malware constitutes a serious security threat that slows down the large scale wireless application development. Sometimes your data can crash once you accept or install malware software [43][44] [45].

Shabtai *et al.* suggested a framework (Host-based Malware detection system) that observes features and events acquired from smartphones and then apply a machine learning anomaly detectors to categorize the normal or abnormal data [46]. Peng [44] provides a study of malware, including the advancement of mobile malware, correlated concepts, and the risk of infection vectors. This article shows that the multiplicity and complication of mobile malware poses a major challenge in containing malicious software modeling.

In this paper, the authors suggested assessment criteria to evaluate the development of smart phone malware. They

provide a comparative analysis of case studies in which the progress malware detection and distribution concept of location data is attempted in the current smartphone platform [47]. E. Gelenbe and R. Lent [48], propose taxonomic malware attack vectors studies to better understand the Android malware; the attacker ways to infect smartphones, and a component of the project responsible for the detailed examination and finding of malware Android that NEMESYS structure. Infrastructure intended understanding and network attacks and smartphones detection.

To examine existing development of malware on smartphone platform and average programmer those have access functionary tools and library of smartphone, research [26][49] suggest specific evaluation criteria measuring the level of security of common OS such as Android, Apple iOS, BlackBerry, Windows phone and Symbian in the term of development of malware, and give comparative analysis and based on the proof of the study. However, this proof would not stop the easiness developing of malware attacks in all smartphone. Finally, they suggested solution against that malware, (a) users to be aware, (b) giving or using saves applications.

Trojan: Trojan is a program which is mostly useful, but it has hidden malicious functionality. The purpose is sneaked into the system without the knowledge of the administrations [43] [50]. Smartphones are becoming more complex and more dominant in providing more functions; growing concern about the opposite of smartphone users security threats. Same software architecture is used by smartphones just like a personal computer; they are susceptible to the same class of security hazards such as viruses, Trojans and worms [51]. Houmansadr *et al.* [51], suggest a *cloud-based smartphone-specific intrusion detection and response engine*, which unceasingly accomplishes a detailed forensics examination on the smartphone to notice any misbehavior. Misbehavior is detected; the suggested engine decides upon and takes optimal response actions to avoid the current attacks.

Spam: Spam is kind of malware attachments can be appended to electronic mail and MMS messages reach to smartphones. Sometime a user opens an attachment at this time smartphone can be infected by malicious codes such as Trojan, worms, etc. which appears as a normal attachment. Attackers manipulate smartphones zombies by sending junk messages and those message used as a door by the attackers to compromise smartphone [36] [52].

Xu and Zhu have studied the possibility of launching attacks and spam with Trojan applications installed by abuse customized notification service. The experimental results are presented and the fact of attacks in four major smartphone platform. Also, the authors present an approach to stealth spam content delivery that can help in identifying application Trojan that ignores the review process of the application in app stores. To maintain the proposed strikes propose design principles Semi-OS-controlled to see notifications, see a safe framework for public view and authentication services to log notifications review notification [53].

Threat: Delac *et al.* [54], show the threats and deeply study the threat mitigation mechanism. They show the attacker centric threat model for smartphones. They evaluated the vectors of attack and strategies and give a security model for two main smartphone Operating system; Android and iOS.

- *New Attacks*

In this category new types of network or system attacks have been discussed. It includes Brute force, DoS, smudge attacks, etc.

Relay Attacks: It involves only future applications on mobile phones. Elements and application access security relays APDU command interface / response network (GSM, UMTS, and Wi-Fi). Attackers can use victims' secured as if they have their physical possession. Relay application can access additional resources (address book, keyboard, etc.) [55]. In article [56], Peer-to-Peer communications in NFC (Near field communication) are being deliberated for a variety of applications with payment. Relay attacks are a threat and can circumvent security measures and encryption/decryption using temporary contracts. The author's contributions in this work include the implementation of practical demonstrations of the first relay attack using NFC mobile platform technology. They show that the attacker using NFC can create a proxy for the development and introduction of the software (without hardware change) of the MID let appropriate for mobile devices. The attack does not involve any code validation and software to be installed on the insurance program. It also uses ordinary, readily accessible APIs such *as JSR 257 and JSR 82*, need for action measures. Such attacks can be controlled intensely using location-based solutions discussed in [56].

Cold Boot Attack: Smartphones and tablets are easily stolen or lost. In paper [57], it is discussed that, this makes them vulnerable to low-grade memory attacks such as *cold-boot* attack using a bus, monitor to keep an eye on the memory bus and *DMA* attacks. The article further describes the *Sentry*, a system that permits applications and operating system modules to stock their code and data on the *System-on-Chip (SoC)* instead of DRAM. They propose the use a special mechanism of ARM-specific was specially intended for embedded systems, but it is still in existing mobile phones, to defend applications and OS in contradiction to a memory subsystem.

Brute Force Attack: Kim [58], proposed a keypad to make the brute force and smudge attacks difficult. This type of keypad increases the time that is required by both brute force and smudge attacks. Keypad time is increased by the formation of random buttons and display delay time.

Denial of Service Attack: Dondyk and Zou [59], proposed a new denial of service oriented attack for the smartphones used by ordinary operators who are not tech savvy. This type of attack which they call the DoS attack, does not prevent future technical perception to use the service through the operation of data management protocol connection to find your smartphone with Wi-Fi antenna. By creating a false eye Internet access Wi-Fi (using devices such as a laptop), the attacker can ask for a smartphone with a Wi-Fi enabled to dismiss the supply of mobile broadband connections that is authorized automatically and link to a bogus Wi-Fi

connection. As a result, it avoids the target smartphone to have any Internet link, unless the dupe can identify the attack and manually disable the Wi-Fi capabilities. They have shown that the most popular smartphones, with iPhone and Android mobiles susceptible to denial of accessibility. To counter these attacks, they propose a new enactment of Internet access authentication protocol to send secret passphrase from authentication server to Internet using a cellular network. Then you try to recover the secret key phrases via Wi-Fi channel that you created to verify the Wi-Fi access point. They have fully evaluated the attack, and defense prototype that runs on Android phones.

Smudge Attack: Gibson [60], explored smudge attacks using oil on the mobile touch screen and captured the smudges. They emphasized on the effect on password pattern of smartphone. They provide a primary study of applying the information learned in a smudge attack to predicting a pattern password.

Cross-Site Scripting (XSS) Attacks: Jin and Hu run the risk of systematic reviews in HTML5 - based mobile application, discovered a new injection code attack, which inherited a cross-site scripting (XSS) attacks (basic cause), but several channels used to insert XSS code. These channels exclusively for mobile devices, including contacts, SMS, bar codes, and MP3 to assess the occurrence of addition code susceptibility in mobile application based on HTML5. They developed a screening tool to analyze the weaknesses of 15,510 applications in Google Play, Phone Gap, 478 applications likely the rate of 2.30% error-positive rate and developed a model called No injection as a cover for the Android hone GAP to protect it from attack [61].

The problem is that HTML5-based malicious code can be inserted into any automated software or application and run. This is the cause of cross-site scripting (XSS) attacks are one of the most common attacks on Web-based applications or programs. Cross-site scripting can only target web application [62].

SMS Based Attack: Attacker can advertise and distribute phishing links via SMS attacks. Text messages can also be used by attackers to feat vulnerabilities [63][64]. Rieck and Stewin [62], study the security of SMS OTP (One-Time password) system architecture and attacks that present a hazard to service learning authentication through the Internet and authorization. They resolute two basic SMS OTP erected on wireless networks and mobile devices have totally dissimilar when SMS OTP is intended and introduced. During this exertion, which showed why SMS OTP system is not safe again? Their results based on proposed mechanisms to ensure SMS OTP against collective attacks and precisely against Trojan.

Hamandi *et al.* [65], examine some of the messaging design verdicts that cause a set of vulnerabilities in the Android operating system, and they show how applications can be built for malware detection to avoid abuse by this vulnerability. These applications appear as a normal application SMS messages and use them fundamental truths to send/receive short messages. Since many operators around the world offer a service that allows users to transfer credit/unit via SMS, cause the misuse of this service to transfer credit illegally. Subsystem “permission”, subsystem "broadcasting receiver," and ordering mechanism to contribute to the establishment of a haven for SMS malware, giving them total control over the sending, receiving and hiding SMS messages. Therefore, the application hides the malicious confirmation from telecom operators that can arise after the transaction for credit transfer. Such subsystems allow users to stream and balance malware attacks that have the potential to cause damage to a large number of users and telecommunications operators. The application has been shown in local control and successfully passed the standard inspection procedure aimed to catch malware. A set of possible solutions is also presented to decrease the risk of such attacks.

Counter Attacks / Escalation Attack: In [66], authors proposed a scheme for detection and prevention that protects Android with features like counter-attacks or escalation attack that attempt to gain full access to all data. These systems monitor the proposed scheme essentially used to call for the application process. If the call system is called by special components of the Android system in normal operation, the regime prevented it from performing. The scheme can detect and block new and unknown malware.

USSD Attacks: USSD (Unstructured Supplementary Service Data) is a protocol used by operators of www(world wide web) to run specific functionality between users and operators [67], examples such as functions including credit check and credit of USSD, USSD can send a prepaid callback, Mobile-Money services. The USSD contains following components: Main Activity, USSD interceptor Service, Boot service and Permission testing.

Hamdani, and Elhajj [68] identified and evaluated two types of Android smartphone based attacks. The first is done by sending an SMS in the background and push notifications network to steal customer credit. Also, they show how the SPM security structure in Android has grown, but they showed how the attack can still be performed. The second attack using the mobile dialler application using the USSD protocol on the target user background.

USB Connection Attacks: Decker and Zúquete [69], exposed serious weaknesses in some private provider’s Android operating system. They described the proof-of-concept to them, which can be used to explore the implications of vulnerability, such as root access. For advanced features are intended for use by suppliers of computer applications to configure and control the device, developed on purpose and with the intention stated. In their observation, the installation of such "features" must be at least possible released to the user, so they recognize the risks of an unprotected USB connection.

Camera based Vulnerabilities and Attacks: Currently, almost all smartphones have features like camera and touchscreen. These functions can lead to attacks on smartphones. Users change device through third party applications from the "app stores" or traditional websites. Source application is a problem, so users are constantly at risk of installing malicious programs that steal personal information or gain root access to their device [64][70].

In article [71], it is figured out the weaknesses associated with Android phones are also for those versatile and sound applications. The authors talked about pieces of spy cam (use of smartphone as spy cam), can play for their attack or gain customers. The authors argue that they found some spy camera forward attacks, including attacks related to continuous monitoring, remote control and two pass-code once led to the raid. Meanwhile, they suggested a plan to ensure a strong guard mobile phone spy cam all this aggression. They explore the possibility of conducting espionage attack (grab information used to launch a successful attack).

Control Flow Attacks: Runtime attacks and control flow (such as code injection or return-oriented programming) is one of the biggest threats to software programs [72] [73]. These attacks are common and have been recently applied to smartphone applications that are downloaded by many users. Davi *et al.* presents a mobile CFI (MoCFI) framework that provides a general countermeasure in contradiction of control flow attacks on smartphone platform by CFI. A typical smartphone that is involved because of two different architectures ARM and Intel. The authors prove that MoCFI is efficient for all smartphone OSes excluding iOS [74].

III. Performance Comparison

In this section, we review present solutions, settled to avoid different types of smartphone threats, attacks and vulnerabilities. To respond to the increasing number of attacks and malware with the vulnerabilities on smartphones, we have several solutions for the problems. So, we show all attacks and their solutions in tabular form. Table 2 shows the old attacks, causes of old attacks and their suggested solutions. Similarly, Table 3 shows a new form of attacks, the cause of these type of attacks and their solutions.

In article [28], 22 participants were interviewed and it was found that each participant wanted to protect data. For data protection and privacy many of the researchers proposed various solutions some of them are discussed here; In Musklokhlove *et al.* [29] authors gave solution for data protection and authentication. They purpose detection malicious data access approach for data protection and upgrade the lock screen system for smartphone authentication. The [30] and [31], articles provide a framework to execute privacy policies to protect user data and enterprise data.

In [18] and [19], it is discussed that the growth of selling smartphone is increasing gradually. In 2014, the shipment values were as the following with respect to Mobile Phone Operating System, Android phone: 950.5 million, iOS: 179.5 million, Windows Phone: 47 million, BlackBerry: 11.9 million, and other (Symbian, etc.): 15.1 million. And in 2018, their market share will increase 11.5%. Fig. 2 show the estimated market share and shipment values of 2018 with the help of 2014's data of shipment and market share.

According to report [75], they said that by the end of 2015, there will probably be more smartphones than people and in 2016 there could be 10 billion smartphones. So, it can be true if sale or shipment of smartphones could gradually increase. Because many peoples may has more than one device.

Table 4 shows the distribution of new mobile malware by their types (first is Installation program and the second is new mobile malicious programs) from the Quarter 4 (Q4) 2014 to Quarter 3 (Q3) 2015. The statistical data obtained from sources (Kaspersky Lab) [76] & [77] have been computed and represented in Table 4.

TABLE I. Distribution of New Mobile Malware (Q4 2014 to Q3 2015) [76] and [77]

Time Period	Mobile Malware Type	
	Installation Package	New mobile malicious program
Q4 2014	65443	30849
Q1 2015	147835	103072
Q2 2015	1048129	291887
Q3 2015	1583094	323374

The Q denotes quarter at x-axis in Fig. 3. Q4 2014 to Q3 2015, the mobile malware increase gradually. This shows in Q4 of 2015 the malware will increase. So, we can say that mobile malware will increase gradually till Q4 2020 shown in Fig. 3. But it is possible that the graph is stable or decrease if any control mechanism will introduce. This estimation is shown in Fig. 3. The middle line shows the stability of the malware and the bottom line is showing the decreasing in malware if a control mechanism is introduced.

These estimations show that due to increasing growth of selling smartphones, malware writers develop a lot of malware software that causes the security threats in smartphones.

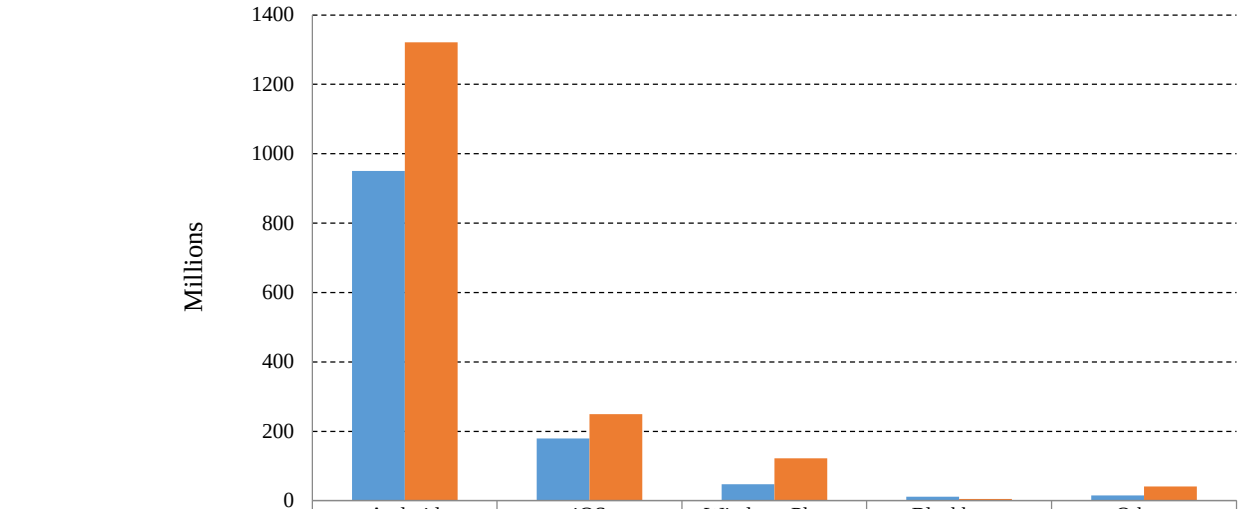
TABLE II. OLD ATTACKS, THEIR VULNERABILITIES AND SOLUTIONS

Attack Name	Vulnerabilities	Solution	Impact	Ref.
Physical Attack	System defects / fault.	Re-manufacturing whether is software or hardware.	Weak the security of mobile phone. Abnormal behavior.	
	Insufficient APIS Management.	Use trusted application from sources.	Malicious code can infect user's data or files.	[33]
Radio Wireless attack	Eavesdropping sniffing and spoof computing blocking.	Suddenly disconnect from the wireless network.	Data can be hacked easily. Weaken computer security.	[34]
	Insecure Wireless network.	Only use trusted network. Using encryption / decryption method to secure communication.	Information can be hacked during communication.	[34]
Backdoor	System bugs and disclosure.	Update your device and install strong antivirus.	Security of smartphone can weak. A backdoor for viruses can be made.	[38]
Virus	Target finding, replication file with unknown source.	Install update Antivirus in your system.	Abnormal behavior of application. Information or applications may be corrupted.	[39], [40]
Worms	Transferring information. Transfer malicious program.	Use updated Antivirus.	Can create the backdoor for hacker. Intertwined with the system files.	[39]
Malware	Downloading file from interested resources.	Use updated anti-virus, install malware prevent software. Use host-based malware detection system, use safe application.	Disturb computer operations. Gather sensitive information.	[43], [44], [46], [26]
Trojan	Downloading Apps from untrusted resources. Hidden malicious functionality.	Smart phone specific intrusion detection system. Use anti-virus.	Disturb computer operations. Gather sensitive information.	[78],[51]
Spam	Any attachment with malicious code transfer via E-mail or MMS. Attacker can advertise phishing links.	Avoid opening these types of emails and MMS. Only taking authentic services and using authentic application. Avoiding responding to any emails that you never asked for.	Fills your Inbox with number of ridiculous emails. Degrades your Internet speed to a great extent. Steals useful information like your details on you Contact list. Alters your search results on any search engine.	[53]
Threat	Spoofing, Information disclosure.	Use CTM (Cyber threat management) software.	Corrupt data. Weaken computer security. Provide back doors into protected networked.	[79]

TABLE III. NEW ATTACKS, THEIR VULNERABILITIES AND SOLUTIONS

Attack Name	Vulnerabilities	Solution	Impact	Ref.
Relay Attack	Insecure network environment. Use of unauthentic proxy service.	Use secure network and trusted proxy application.	Information hacked during communication.	[56]

Cold Boot Attack	Unauthorized access to RAM and encryption / decryption key of system	Use a system that store code and data on the SOC (System on chip) instead of RAM i.e. Sentry. Use powerful encryption decryption method	Encryption key may be hacked. Weak data security.	[57]
Brute Force Attack	Try again and again to unlock phone using many combination and no limit to prevent from hacking.	Set a limit for try again and again to unlock device and display time delay.	Password cracked. Slowing the CPU speed.	[58]
Smudge Attack	By keep touch screen dirty or using oily hands.	Keep clean and clear screen and use clean hand to operate device.	Easily guess the pattern password. Data unsecure.	[60]
Denial of Service Attack	By using other device dismiss the supply of mobile broadband connection. Link to bogus Wi-Fi connection	Use internet access authentication protocol.	Busy the network. Busy smartphone and block other services.	[59]
XSS Attack	HTML 5 based malicious code inserted into an application or software.	Use popular and authentic apps. Use screening tool to check the weakness of the apps.	Smartphone infected by inject malicious code via HTML page or any other untrusted script. Cause of hacking information or provide backdoor.	[62], [61]
SMS based Attack	Attacker can advertise phishing links.	Device can protect by setting up the Message settings, or to dis-allow auto receiving MMS or text.	Sensitive information can be fetch.	[63], [64], [80]
USSD Attack	Blue Jacking, Bluesnarfing and unknown coming calls.	Use Anomaly based Intrusion detection system	Personal data can be fetched. Cause the damage on the cell phones.	[68]
USB Connection Attack	Root access, enable ADB(open command tool and avail both developer and attacker)	Use apparently inoffensive smartphone charging station	Sensitive information can be fetch easily. Any malware can be injected easily.	[69]
ABD Attack	Open command tool and avail both developer and attacker	Backward slicing. Static analyzer and string analyzer.	Sensitive information can be fetch easily.	.[2]
Camera based attacks	Malicious program, unauthentic source and etc. Use camera of smart phone as spy cam by malicious program	Spy camera could support. Implement effective fine Grained access	Weak the smartphone security. Can fetch data or information.	[64], [71]
Control Flow attacks	Code injection, data over flow in Memory	Use Mobile control flow integrity framework	Can be exploited to snip the user's SMS or contacts database, to open a remote reverse shell. Exploiting memory corruption.	[74]



	Android	iOS	Windows Phone	Blackberry	Others
2014 Shipment Values (Million)	950.5	179.5	47	11.9	15.1
2018 Shipment values (Million)	1321.1	249.6	121.8	5.3	40.7

Fig. 2. Smartphone market share and shipment by OS in 2014 and its estimation for 2018 [18] & [19]

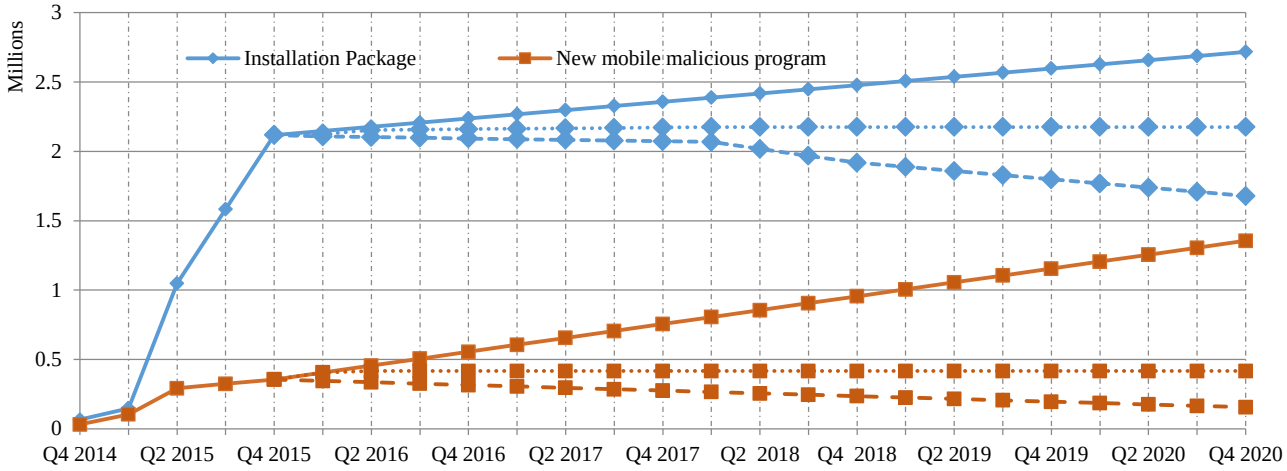


Fig. 3. Estimated Mobile malware from Q4 2014 - Q4 2020

IV. Discussion

Authentication, data privacy, vulnerabilities (which cause the attacks) and attacks are the major open issues of security. Authentication problem is the major part of security breach. An appropriate solution to authentication problem can overcome many authentication problems and saves smartphones from security breach. All users want to protect their data. So, Data Privacy is one of the biggest concerns to the smart phone users. Thus, the data privacy issues, can most of times could be addressed by using trusted sites and applications. Most of the smartphone attacks occur due to vulnerabilities. If the vulnerabilities are minimized, it can save the smartphones from most of the attacks. But in rapidly growing field where development occurs at large scale it is hard to achive100% security, but the careful design and development processes lead to more secure smartphones.

Number of smartphones is increasing rapidly. The reason behind this increment is the frequent technological changes and evolution. But with this technological evolution, more malware attacks are being launched. If we look upon the Kaspersky Laboratories reports regarding these attacks, we come to know that number of malware attacks is increasing every year, which is also included in this review paper. So, we should neither be satisfied upon the increasing in number of smartphone sales, nor it should be merely lookup for solution by the developer against the malware attacks being launched. But manufacturers as well as developers have to look around the reason behind these attacks, launched for smartphones which are obviously because of the loophole present in the architecture and software of the smartphone being provided by the manufacturer and the software developer.

The future belongs to IoT (Internet of Things); technology where all the devices remain online and interconnected. So, almost each routine gadget would be controlled by smartphone

via IoT. Which includes electronic devices, machines, vehicles, security based entrances, etc. So, this will cause a lot of issues regarding smartphones such as battery drainage issue, performance issue and security issues regarding not only data privacy but also illegal access to the personal devices via IoT. So, it is required to have a smartphone that used for IoT, must have best battery consumption, efficient processing and maximum security. So that we would be able to achieve maximum benefits from IoT. As we know that we don't have a mechanism for complete security regarding smartphone. We can't say that our data privacy and access is completely safe and sound. So that manufacturers as well as developers require building and presenting a mechanism that provides maximum security.

The purpose for writing this review is to provide a holistic account of smartphone vulnerabilities and problems and to look at various possible solutions suggested in the literature. These solutions and problems have been collected from review of previous researches.

V. Conclusion

Smartphones are the multipurpose handheld devices that contain a lot of third-party applications that extend the functionality of the device. With the quick production of smartphones prepared with many features such as several connectivity links and sensors, the mobile malware are growing. The smartphone environment is different from the PC environment. Similarly, the solutions to prevent the infections and diffusion of malicious code in smartphone are different from PC or other computer devices. Smartphones have insufficient resources, including power (battery) and processing unit. Increasing the capabilities of the smartphone, these features can be misused by attackers, as different types of links, sensors, services and user's secrecy.

In this work, at first, we discussed the current authentication problems, data protection and privacy problems. We investigated the vulnerabilities in smartphones and attacks that can occur in smartphones. Secondly, we have characterized identified attacks in contradiction of smartphones, concentrating on why attacks occur and what are their effects on smartphones. Finally, we have studied existing security results to prevent smartphones from infections, malicious codes and intruder's attacks.

References

[1] N. Yildirim, R. Das, and A. Varol, "A Research on Software Security Vulnerabilities of New Generation Smart Mobile Phones," in 2nd International Symposium on Digital Forensics and Security (ISDFS'14), 2014, pp. 6–16.

[2] A. Agrawal and A. Patidar, "Smart Authentication for Smart Phones," Citeseer, vol. 5 (4), pp. 4839–4843, 2014.

[3] P. Schulz and D. Plohmann, "Android security-common attack vectors," in Rheinische Friedrich-Wilhelms-Universitat Bönn, Germany, Tech. Rep, 2012.

[4] C. Pettey and R. van der Meulen, "Gartner says worldwide sales of mobile phones declined 3 percent in third quarter of 2012; smartphone sales increased 47 percent," Gartner),[Online], 2012.

[5] R. van der Meulen, "Gartner says 821 million smart devices will be purchased worldwide in 2012; sales to rise to 1.2 billion in 2013," 2012.

[6] R. van der Meulen and J. Rivera, "Gartner Says Smartphone Sales Grew 46.5 Per Cent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First Time," 2013.

[7] "Global Smartphone Use Continues to Climb, Studies Show." [Online]. Available: http://www.eweek.com/mobile/global-smartphone-use-continues-to-climb-studies-show.html. [Accessed: 30-Oct-2015].

[8] H. Luo, G. He, X. Lin, and X. Shen, "Towards hierarchical security framework for smartphones," in Communications in China (ICCC), 2012 1st IEEE International Conference on. IEEE, 2012, pp. 69–72.

[9] M. Ahmad and N. Musa, "Comparison between android and iOS Operating System in terms of security," in Information Technology in Asia (CITA), 2013 8th International Conference on. IEEE, 2013, pp. 1–4.

[10] M. Goadrich and M. Rogers, "Smart smartphone development: iOS versus Android," in Proceedings of the 42nd ACM technical symposium on Computer science education. ACM, 2011, pp. 607–612.

[11] L. Ma, L. Gu, and J. Wang, "Research and Development of Mobile Application for Android Platform," Int. J. Multimed. Ubiquitous Eng., vol. 9, no. 4, pp. 187–198, 2014.

[12] J. Liu and J. Yu, "Research on Development of Android Applications," in Fourth International Conference on Intelligent Networks and Intelligent Systems. IEEE, 2011, pp. 69–72.

[13] T. Grønli and J. Hansen, "Mobile application platform heterogeneity: Android vs Windows Phone vs iOS vs Firefox OS," in Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on. IEEE, 2014, pp. 635–641.

[14] D. Tilson, C. Sørensen, and K. Lyytinen, "Change and control paradoxes in mobile infrastructure innovation: the Android and iOS mobile operating systems cases," in System Science (HICSS), 2012 45th Hawaii International Conference on. IEEE, 2012, pp. 1324–1333.

[15] V. Remenar, S. Husnjak, and D. Peraković, "Research of Security Threats in the Use of Modern Terminal Devices," in 23rd International DAAAM Symposium Intelligent Manufacturing & Automation: Focus on Sustainability, 2012.

[16] A. Maji and K. Hao, "Characterizing failures in mobile oses: A case study with android and symbian," in Software Reliability Engineering (ISSRE), 2010 IEEE 21st International Symposium on. IEEE, 2010, pp. 249–258.

[17] O. Riva and C. Qin, "Progressive Authentication: Deciding When to Authenticate on Mobile Phones.," in Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)., 2012, pp. 301–316.

[18] F. Al-Qershi, "Android vs. iOS: The security battle," in Computer Applications and Information Systems (WCCAIS), 2014 World Congress on. IEEE, 2013, pp. 1–8.

[19] D. Padmavathi and M. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," arXiv Prepr. arXiv0909.0576, vol. 4, pp. 1–9, 2009.

[20] M. A. Dar and J. Parvez, "Smartphone operating systems: Evaluation & enhancements," in 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014, pp. 734–738.

[21] J. H. Choi and H.-J. Lee, "Facets of simplicity for the smartphone interface: A structural model," Int. J. Hum. Comput. Stud., vol. 70, no. 2, pp. 129–142, Feb. 2012.

[22] W. Lee and R. Lee, "Multi-sensor authentication to improve smartphone security," in Conference on Information Systems Security and Privacy., 2015, pp. 1–11.

[23] S. Zahid, M. Shahzad, S. Khayam, and M. Farooq, "Keystroke-based user identification on smart phones," in Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2009, pp. 224–243.

[24] T. Feng, X. Zhao, B. Carbunar, and W. Shi, "Continuous Mobile Authentication Using Virtual Key Typing Biometrics," in 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013, pp. 1547–1552.

[25] C.-C. Lin, C.-C. Chang, D. Liang, and C.-H. Yang, "A New Non-Intrusive Authentication Method Based on the Orientation Sensor for

Smartphone Users," in 2012 IEEE Sixth International Conference on Software Security and Reliability, 2012, pp. 245–252.

[26] A. Morris, "Multimodal person authentication on a smartphone under realistic conditions," in Defense and Security Symposium. International Society for Optics and Photonics, 2006, p. 62500D–62500D.

[27] N. Gobbo, A. Merlo, and M. Migliardi, "A denial of service attack to GSM networks via attach procedure," Secur. Eng. Intell. Informatics. Springer Berlin Heidelb., vol. 8128, pp. 361–376, 2013.

[28] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Understanding Users' Requirements for Data Protection in Smartphones," in 2012 IEEE 28th International Conference on Data Engineering Workshops, 2012, pp. 228–235.

[29] I. Muslukhov, "Survey: Data Protection in Smartphones Against Physical Threats," in Term Project Papers on Mobile Security. University of British Columbia., 2012.

[30] D. Ghosh, A. Joshi, T. Finin, and P. Jagtap, "Privacy Control in Smart Phones Using Semantically Rich Reasoning and Context Modeling," in 2012 IEEE Symposium on Security and Privacy Workshops, 2012, pp. 82–85.

[31] P. Kodeswaran, V. Nandakumar, S. Kapoor, P. Kamaraju, A. Joshi, and S. Mukherjea, "Securing Enterprise Data on Smartphones Using Run Time Information Flow Control," in 2012 IEEE 13th International Conference on Mobile Data Management, 2012, pp. 300–305.

[32] R. Prodanovic and D. Simic, "A Survey of Wireless Security," J. Comput. Inf. Technol., vol. 15, no. 3, p. 237, Sep. 2007.

[33] A. Kataria, T. Anjali, and R. Venkat, "Quantifying smartphone vulnerabilities," in 2014 International Conference on Signal Processing and Integrated Networks (SPIN), 2014, pp. 645–649.

[34] K. Mandke, H. Nam, and L. Yerramneni, "The evolution of ultra wide band radio for wireless personal area networks," Spectrum, vol. 3, pp. 22–32, 2003.

[35] J. Jermyn, G. Salles-Loustau, and S. Zonouz, "An Analysis of DoS Attack Strategies Against the LTE RAN," J. Cyber Secur., vol. 3, pp. 159–180, 2014.

[36] C. Guo, H. Wang, and W. Zhu, "Smart-Phone Attacks and Defenses," Citeseer HotNets III., 2004.

[37] O. Ugus, D. Westhoff, and H. Rajasekaran, "A leaky bucket called smartphone," in 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, 2012, pp. 374–380.

[38] M. Durairaj and A. Manimaran, "A Study on Security Issues in Cloud Based E-Learning," Indian Journal of Science and Technology, vol. 8, no. 8. pp. 757–765, 01-Apr-2015.

[39] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," IEEE Commun. Surv. Tutorials, vol. 15, no. 1, pp. 446–471, 2013.

[40] J. Cheng, S. H. Y. Wong, H. Yang, and S. Lu, "SmartSiren," in Proceedings of the 5th international conference on Mobile systems, applications and services - MobiSys '07, 2007, p. 258.

[41] S. Peng, M. Wu, G. Wang, and S. Yu, "Propagation model of smartphone worms based on semi-Markov process and social relationship graph," Comput. Secur., vol. 44, pp. 92–103, Jul. 2014.

[42] D. Liu, N. Zhang, and K. Hu, "A Survey on Smartphone Security," Appl. Mech. Mater., vol. 347–350, pp. 3861–3865, Aug. 2013.

[43] M. H. R. Khouzani, S. Sarkar, and E. Altman, "Maximum Damage Malware Attack in Mobile Wireless Networks," IEEE/ACM Trans. Netw., vol. 20, no. 5, pp. 1347–1360, Oct. 2012.

[44] S. C. Peng, "A Survey on Malware Containment Models in Smartphones," Appl. Mech. Mater., vol. 263–266, pp. 3005–3011, Dec. 2012.

[45] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, "Crowdroid: behavior-based malware detection system for Android," in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices - SPSM '11, 2011, p. 15.

[46] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "'Andromaly': a behavioral malware detection framework for android devices," J. Intell. Inf. Syst., vol. 38, no. 1, pp. 161–190, Jan. 2011.

[47] A. Mylonas, S. Dritsas, B. Tsoumas, and D. Gritzalis, "Smartphone security evaluation The malware attack case," in Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on, 2011, pp. 25–36.

[48] E. Gelenbe and R. Lent, Eds., Information Sciences and Systems 2013, vol. 264. Cham: Springer International Publishing, 2013.

[49] A. Mylonas and S. Dritsas, "Smartphone security evaluation The malware attack case," in Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on. IEEE, 2011, pp. 25–36.

[50] Z. Xu, K. Bai, and S. Zhu, "inferring user inputs on smartphone touchscreens using on-board motion sensors," in Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks - WISEC '12, 2012, p. 113.

[51] A. Houmansadr, S. A. Zonouz, and R. Berthier, "A cloud-based intrusion detection and response system for mobile phones," in 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), 2011, pp. 31–32.

[52] M. J. Smith and G. Salvendy, Eds., "A Practical Analysis of Smartphone Security," in Symposium on Human Interface 2011, Held as Part of HCI International 2011, Orlando, FL, USA, July 9-14, 2011, Proceedings, Part I, 2011, pp. 311–320.

[53] Z. Xu and S. Zhu, "Abusing notification services on smartphones for phishing and spamming," in Proceedings of the 6th USENIX conference on Offensive Technologies. USENIX Association, 2012, pp. 1–1.

[54] G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in MIPRO, 2011 Proceedings of the 34th International Convention. IEEE, 2011, pp. 1468–1473.

[55] M. Roland, J. Langer, and J. Scharinger, "Relay attacks on secure element-enabled mobile devices," in Information Security and Privacy Research. Springer Berlin Heidelberg, 2012, pp. 1–12.

[56] S. B. Ors Yalcin, Ed., Radio Frequency Identification: Security and Privacy Issues, vol. 6370. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[57] P. Colp, J. Zhang, J. Gleeson, S. Suneja, E. de Lara, H. Raj, S. Saroiu, and A. Wolman, "Protecting Data on Smartphones and Tablets from Memory Attacks," ACM SIGARCH Comput. Archit. News, vol. 43, no. 1, pp. 177–189, Mar. 2015.

[58] I. Kim, "Keypad against brute force attacks on smartphones," IET Inf. Secur., vol. 6, no. 2, p. 71, Jun. 2012.

[59] E. Dondyk and C. C. Zou, "Denial of convenience attack to smartphones using a fake Wi-Fi access point," in 2013 IEEE 10th Consumer Communications and Networking Conference (CCNC), 2013, pp. 164–170.

[60] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," pp. 1–7, Aug. 2010.

[61] X. Jin, X. Hu, K. Ying, W. Du, H. Yin, and G. Peri, "Code injection attacks on HTML5-based mobile apps: Characterization, detection and mitigation," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014, pp. 66–77.

[62] K. Rieck, P. Stewin, and J.-P. Seifert, Eds., Detection of Intrusions and Malware, and Vulnerability Assessment, vol. 7967. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013.

[63] "A Survey Of Mobile Device Security: Threats, Vulnerabilities and Defenses | A Few Guys Coding Blog," in University of Colorado at Colorado Springs, 2011.

[64] M. E. S. Amravati, "A Review on Camera Based Attacks on Android Smart Phones," Int. J. Comput. Sci. Technol., vol. 6, no. 1, pp. 88–92, 2015.

[65] K. Hamandi, A. Chehab, I. H. Elhajj, and A. Kayssi, "Android SMS Malware: Vulnerability and Mitigation," in 2013 27th International Conference on Advanced Information Networking and Applications Workshops, 2013, pp. 1004–1009.

[66] H. Lee, D. Kim, M. Park, and S. Cho, "Protecting data on android platform against privilege escalation attack," in International Journal of Computer Mathematics, 2014, pp. 1–14.

[67] S. Arzt, S. Huber, S. Rasthofer, and E. Bodden, "Denial-of-App Attack: Inhibiting the Installation of Android Apps on Stock Phones," in

Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices - SPSM '14, 2014, pp. 21–26.

[68] K. Hamandi, A. Salman, and I. Elhajj, "Messaging Attacks on Android: Vulnerabilities and Intrusion Detection," in Mobile Information Systems 2015, 2015.

[69] B. De Decker and A. Zúquete, Eds., Communications and Multimedia Security, vol. 8735. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[70] M. Bartere and M. Pore, "Preventions and Features of Camera Based Attacks on Smart Phones," Int. J. Innov. Res. Comput. Commun. Eng., vol. 3, no. 5, pp. 4846–4853, 2015.

[71] R. Mayavan and A. Selvan, "Security Dangers to Versatile Interactive Media Applications: Cam Based Assaults on Versatile Telephones," 2015.

[72] "Control-Flow Integrity." [Online]. Available: https://www.trust.informatik.tu-darmstadt.de/research/projects/current-projects/control-flow-integrity/. [Accessed: 20-Feb-2016].

[73] "Control Flow Integrity: Talks." [Online]. Available: https://talks.cs.umd.edu/talks/71. [Accessed: 20-Feb-2016].

[74] L. Davi, A. Dmitrienko, M. Egele, and T. Fischer, "MoCFI: A Framework to Mitigate Control-Flow Attacks on Smartphones.," in 19th Annual Network & Distributed System Security Symposium (NDSS), 2012.

[75] "2015 Mobile Threat Report - The Rise of Mobile Malware." [Online]. Available: https://securityintelligence.com/events/the-current-state-of-mobile-threats/. [Accessed: 11-Dec-2015].

[76] "IT threat evolution in Q1 2015 - Securelist." [Online]. Available: https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/. [Accessed: 11-Dec-2015].

[77] "IT threat evolution in Q3 2015." [Online]. Available: http://www.tsecurity.de/it-security-sicherheit/malware-trojaner-viren/28810-it-threat-evolution-in-q3-2015. [Accessed: 11-Dec-2015].

[78] J. Jamaluddin, N. Zotou, R. Edwards, and P. Coulton, "Mobile phone vulnerabilities: a new generation of malware," in IEEE International Symposium on Consumer Electronics, 2004, 2004, pp. 199–202.

[79] "Threats in computer security." [Online]. Available: https://en.wikipedia.org/wiki/Threat_(computer). [Accessed: 04-Dec-2015].

[80] A. Pore and M. Bartere, "A Review on Camera Based Attacks on Android Smart Phones Anushree Pore," vol. 6, no. 1, Feb. 2015.