Security in Mobile Computing: Attack Vectors, Solutions, and Challenges

Sara Alwahedi, Mariam Al Ali, Fatimah Ishowo-Oloko, Wei Lee Woon, and Zeyar Aung(✉)

Department of Electrical Engineering and Computer Science,
Masdar Institute of Science and Technology, Abu Dhabi, UAE
{salwahedi,maralali,fishowooloko,wwoon,zaung}@masdar.ac.ae

Abstract. With the growth of the mobile industry, a smart phone has the ability to store large amounts of valuable data such as personal and bank information, the users' location, call logs and more. Thus, the security of data in the mobile world has become an important issue. The main objective of this survey paper is to review the state-of-the-art technologies for the security of mobile computing. It covers the modern mobile operating systems that are being widely used today. It also identifies the various types of attack vectors particularly designed to infect mobile devices and highlights the available security solution to counter each type of attack. Finally, it briefly discusses the outstanding limitations and challenges in the mobile computing world.

Keywords: Mobile computing · Smart phone · Security · Attack vectors

1 Introduction

Mobile Computing is an emerging technology that serves users at anytime and anywhere, it is a combination of mobile and wireless communication services. The increasing demand for mobility along with the features of wireless networks, which differ from those of traditional networks, makes mobile computing more susceptible to challenges and threats. For that reason, providing security for mobile computing technology is important and critical for developing safe applications.

Mobile Computing includes three main parts: the hardware which consists of the physical components like the processor chip, the software that facilitates the computing process which is the operating system (OS) and the infrastructure such as protocols, services, bandwidth etc. [4]. Most attacks in mobile computing affects the OS and so we start by reviewing the popular OS for mobiles.

1.1 Contributions

The main contributions of this survey paper are as follow:

1. Describing different platforms of mobile computing and comparing between the two most widely-used ones, namely, Google's Android and Apple's iOS.

R. Agüero et al. (Eds.): MONAMI 2016, LNICST 191, pp. 177–191, 2017.
DOI: 10.1007/978-3-319-52712-3_13

2. Exploring common security issues in mobile computing, such as confidentiality and integrity, and exploring different attack vectors on those issues.
3. Analyzing existing solutions to these attack vectors.
4. Identifying limitations in challenges for mobile security solutions.

2 Mobile Computing Platforms

The common mobile OS are Google's Android, Apple's iOS, Nokia's Symbian, RIM's BlackBerry OS, Samsung's Bada and Microsoft's Windows Phone [15]. Given that Android and iOS have the largest share of the market population, this survey focuses on these two operating systems and in this section, we review the architecture, advantages and disadvantages of the two of them.

Apple's iOS developed by Apple Inc. was first announced in 2007 and was developed only for Apple products. The operating system is coded in Objective-C and is known for being user-friendly. It is however very tightly guarded. iOS acts as an intermediary between the underlying hardware and the apps. Apps do not talk to the underlying hardware directly. Instead, they communicate with the hardware through a set of well-defined system interfaces. The iOS SDK allows developers to make applications for the iPhone and test them in an "iPhone simulator". Apple approves apps by signing with encryption keys after which, such an app can be downloaded from the App store. This is to ensure that only apps satisfying Apple's security policy can be distributed to iPhones [8].

Currently, the most popular OS is Android owned by Open Handset Alliance. Android applications are open-source, written in Java and compiled by the Android SDK tools along with any data and resource files into an Android package (APK) file. Each Android application runs in its own space called a sandbox and can't access data from other applications without user permission [7]. This helps to ensure a certain level of security in Android phones. On the other hand, this feature is also detrimental as it prevents antivirus applications from accessing other applications too in order to scan them or update its virus database.

2.1 iOS vs. Andriod

Apple iOS has a major advantage over Android in terms of security due to the closed nature of the Apple store whereby all apps are vetted by Apple before release. This helps to reduce the number of malware apps found in the store. This is an advantage over Android that runs an open market and thus allowing a proliferation of malicious apps in its market. Yajin et al. collected over 1,200 malware samples of existing Android malware families within a period of 14 months [31].

However, once an app has been installed on to the phone, Android has the advantage with the sandbox system which confines each app to its directory alone. It is thus separated not only from every other app but from the main OS's files and folders [7]. This is unlike iOS applications that can access many system resources by default.

The openness of the Android market does offer a significant advantage over iOS which is the ease of development. The fact that Android is open sourced and development is done in Java and supports cross platform has led to a lot of apps being developed for the Android market which in turn has led to its growing popularity. In terms of similarities, both iOS and Android offer a public marketplace, however android users also have the option of downloading non-market apps.

Given the differences in their architecture, it's not surprising that there are differences in the vulnerabilities of each OS. Some attacks are more frequent and successful on the Android platform than on the iOS platform. Having introduced the common OS in mobile computing, the rest of the survey is organized as follows: Sect. 3 discusses in detail the security issues in mobile computing, this section is divided into a number of sub sections each focused on a specific kind of attack along with the existing solutions in the literature. Sometimes an attack might cut across more than one security issue. Then, Sect. 4 mentions the limitations in the solutions. Finally, we conclude our survey with a discussion in Sect. 5.

3 Security in Mobile Computing

Security issues in mobile computing are generally divided into three main categories, Confidentiality, Integrity, and Availability (CIA). An attack usually targets one or more of these categories and can render great damage to a system. CIA can be defined briefly as follows:

1. Confidentiality: It is the prevention of unauthorized access to the file or system by attackers. It deals with the privacy of the data [4].
2. Integrity: It prevents editing the data in any way, by modifying, creating or deleting data within the system or file [11].
3. Availability: It ensures that the data is accessible to the authorized user [20].

Other important categories that are related to mobile computing and that may be targets of attacks are:

1. Authentication: It has to do with verifying and validating the systems. Authentication seeks to make sure that the user is indeed who he says he is by proving his identity using certain means and credentials that the system requests for. This also is related to confidentiality since it helps in preventing unauthorized access [11].
2. Authorization: It verifies that the user is only viewing the data that he has the right to access. It has to do with availability and confidentiality in which it makes sure the appropriate user is authorized to access the data and whether or not he is able to [4].
3. Accountability: The user is held responsible for the actions he may take. This is arranged such that the link between both systems and users cannot be denied, as in the user is accountable for what he or she does, it can also be called non-repudiation [20].

Figure 1 shows the taxonomy of attack vector types specifically applicable to the mobile computing platform.

Although most of these attacks have solutions, the solutions also have some limitations. In the following sections, we explore different attacks on specific areas of security. Each attack is immediately followed by its solutions. General weaknesses and limitations to these solutions are discussed in a later session.

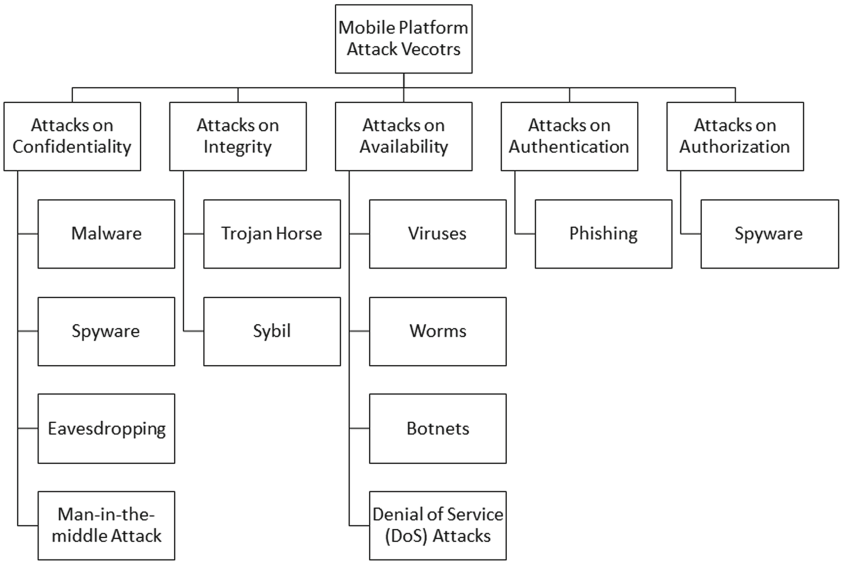

Fig. 1. Taxonomy of attack vector types in mobile computing.

3.1 Attacks on Confidentiality

A breach in confidentiality takes place when an attacker is able to read the data stored on the mobile phone. This is a very common form of attack because of the value of the information stored on the phones. One way in which this attack is usually carried out is by the use of malware.

Malware: Malware or malicious software is a piece of software that is used to attack the operating system of a victim to perform a series of harmful operations. These includes disrupting the system's operations, deleting or altering data, gathering sensitive data and information, gaining unauthorized access into the computer system, or clandestinely controlling the system to carry out illegal operations. Malware tends to target all the three categories of CIA depending on the type of malware used. There are different types which include viruses, worms, Trojans, and spyware. The type of malware that is typically used to breach confidentiality is called spyware.

Solutions: Malware detection programs can be used to detect and remove types of malware from a device including Trojans, viruses and worms which will be discussed in the upcoming sections. Android has several anti-virus applications available in its play store which are recommended to install on one's device. Early detection is the most important thing to mitigate the harmful effects of malware. Throughout the years, a number of malware detection methods have been proposed. These can be broadly categorized into: Signature-based, Change-based, and Anomaly-based methods.

- Signature-based methods: A signature based intrusion method detects a malware based on its signature. First, it gathers data and analyzes it, then any program or file with a similar signature to an already existing malware (compares to a database) is detected. This method is often used for detecting popular malware signatures, but it can be quite slow since it would have to compare the signatures to a large database, meaning it cannot be instant [28]. Data mining techniques are used in these applications for malware classification and it has been proven to be very effective. These include: Rain Forest Neural network, decision tree, Bayesian, Naive Bayes, Classification-based Multiple Association Rule (CMAR) [1].
- Change-based methods: Change based detection is a method that identifies when changes occurs in the system. It relies on probability distribution to detect the changes. These techniques include online and offline change detection techniques.
- Anomaly-based methods: Anomaly based systems look for abnormal behavior in the system tagged as anomalies. These anomalies are detected by first estimating or modeling the normal behavior of the system. Then, any changes or deviations from the estimated normal behavior (usually above a pre-defined threshold) are flagged as possible attacks [9,28].

While malware attacks can be prevented by installing anti-malware software on the mobile devices, one may consider using personal firewall software to restrict access. Since all types of data from and into the device passes through the firewall, the system is able deny access to unwanted intruders [15]. Although this solution seems appropriate, it has two main weaknesses. First, such software tends to consume a lot of power when installed in mobile devices. As a result, most users find themselves uninstalling them in order to conserve power. Alternatively, users are forced to purchase very expensive batteries in order to achieve the desired battery life [14]. Second, they also interfere with website links, access to certain internet updates, and other applications.

Spyware: Spyware is a type of malware that collects data from the system it infects, more accurately it spies on the mobile system. These days, smartphones can store huge amounts of data on the device, most users store important information on their devices such as bank account information. In regards to security issues, spyware is viewed to be a great threat to the confidentiality of the system though it can also affect authorization [10]. A phone infected by

spyware can have the user's location, messages, emails and calls tracked, spied on as well as recorded. An example of android spyware is Android Tapsnake which is a game software that actually steals user's information. Though, most spyware on android require the device to be rooted in order to successfully infect it, some of them can access information using standard permissions in an unrooted android device [3]. Similarly, jailbroken iOS devices are more prone to malware and spyware attacks.

Solutions: The defense methods for spyware are the same as those for malware as discussed above.

Eavesdropping: Another attack on mobile computing is eavesdropping (also known as disclosure attacks), which is considered to be the most known form of attack that affect data privacy. In this type of attack, the attacker will try however possible to access confidential information by observing and analyzing messages which go through the network [18]. Those information are transmitted through communication and could include passwords, location, private keys, etc., which should be secured and protected from any unauthorized access. This is where data is usually intercepted by an attacker who tends to observe communication that is being transmitted from a mobile device or being sent to it. The messages need to be protected and secured by using cryptographic mechanisms. The eavesdropping attack is divided into two parts:

- Passive Eavesdropping: The attacker will monitor and listen to the transmitted messages via network to detect useful information.
- Active Eavesdropping: It includes detecting information by appearing to the transmitters as friendly and known nodes.

Solutions: There are several measures that can be taken to address the above threats. However, such measures are sometimes inadequate since they also have their own weaknesses. One of such measures by which eavesdropping can be avoided is securing the communication channel. Here, the messages being sent are encrypted once they leave the source and are only decrypted after they are received by the intended recipient [5]. Since the message is usually in a coded form during the transit, even if the attacker intercepts it, it might not make much sense to him. Encryption also offers a solution to the message modification attack. However, encryption is not foolproof. This is because depending on the attacker's sophistication level; the message can be decrypted while in transit. To lower chances of such an eventuality, the encryption should be as strong as possible.

Man-in-the-middle Attack: Smart phones are prone to man-in-the-middle (MitM) attacks. This is when "an adversarial computer comes between two computers pretending to one to be the other" [17]. Here, the attacker positions himself between the receiver and the sender. He then sniffs information that is

being transmitted between the two nodes. Such an attack renders the confidentiality of mobile computing useless. MitM attack can be used to gain access to a smart phone and perform a financial malware attack (FMA). An FMA is an attack whose main objective is to steal important data from the user, such as the user's credentials, through the mobile device [10].

An FMA attacker can attack a phone by impersonating a bank or the attacker can use the MitM attack for banking transactions in which he will be able to steal the user's information. Android.Sniffer is a program that was used to steal bank information by using the MitM [3]. MitM attacks are also achieved by the setting up a fake Wi-Fi hotspot via a wireless router. The mobile phone will automatically detect the signal and request access, thus allowing the attacker to access all of the user's information through the router. Both Android phones and iPhones are prone to this attack [2].

Solutions: The certificates for verification and validation that a device has embedded in it or the applications it uses can help in preventing or mitigating MitM attacks. Often times, these are disabled by rooting or jailbreaking the smart phone, making it less secure. Additionally, certificate authority private keys should be used and are also pre-installed in the device. Android for example has over 100 of them [26].

3.2 Attacks on Integrity

Encryption is a common way of protecting the integrity of data as mentioned in the previous section. Thus, to attack the integrity of the data, attacks can attack the encryption system itself. Once, the encryption system is corrupted, then the integrity of the data is easily compromised. This kind of attack is usually disguised as a utility, essential third-party software application, or a game. Once it attacks a mobile device, it launches several attacks on the system as it continues to spread to any other devices sharing common connection [5].

Trojan Horse: A Trojan horse is a type of malware that "claims" to be legitimate. It often presents itself as a form of software update. It then sabotages the system by providing a backdoor for other illegitimate activities. It is different from viruses and worms because it does not replicate itself. An example of a Trojan horse for iPhones is iPhone firmware 1.1.3 prep that presented itself to users as an important software upgrade. Upon installation however, it corrupted other tools on the phone e.g. OpenSSH that were essential for data encryption [12].

Zeus Trojan horse is another malware that has infected personal computers using Windows OS, it is used to collect data while posing as an online banking service. Recently, a Trojan horse called Zitmo (Zeus in the mobile) collaborates with Zeus in order to hijack a user's android device by prompting the user (using Zeus) to install a security application on the mobile through an HTTP link. The application is Zitmo posing as "Trusteer Rapport" to fool the user and infect the android device thus gaining access to the user's data [26]. Since, Trojans

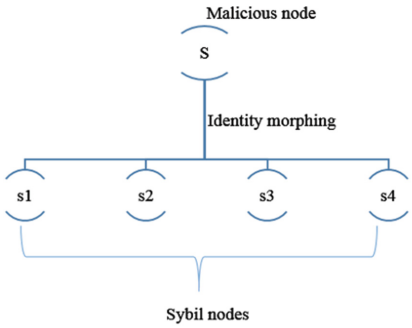

Fig. 2. Sybil attack.

such as Zitmo are able to access user information they are also an attack on confidentiality and authorization.

Solutions: The solution to the Trojan horse attack are the same as those explained in detail for preventing malware attacks.

Sybil: Another attack on the integrity of a system is Sybil attack (Fig. 2). This attack targets mobile networks and it affects the integrity of the data by introducing large amounts of false data into the network. In this attack, one malicious entity presents many fake identities to dominate an essential portion of the system [24]. This is a serious and severe challenge in many areas. For instance, an attacker can rig internet polls by submitting many votes through using many IP addresses [22]. In Sybil attack each node imitates multiple several other linked nodes and try as possible to create confidence by using different malicious methods [22]. The main effects of Sybil attacks in mobile computing include: data aggregation, fair resource allocation and routing [26].

- Fair Resource Allocation: Sybil attack can affect this scheme by giving a malicious node benefit from any network resource allocated to a node by presenting many different identities to that node.
- Data Aggregation: The Sybil attacker can change the result of data gathering or data aggregation by participating in the aggregation with multiple spoofed and fake identities.
- Routing: The performance and function of routing protocol on a path from initial node to destination node can be affected by Sybil attack. By presenting multiple, fake and spoofed identities for each malicious node, the routing process will be disrupted as a result of evolving into multiple paths. When the legitimate node wants to send message to a malicious node, the message will be sent to different paths because many nodes will have the same identity, while it is actually sent to one malicious node.

Solutions: There are existing solutions to prevent the effects of Sybil attack. One of these solutions of this attack is by stopping Sybil attacker from creating

fake identities [21]. This can be done by adopting additional infrastructures that build relationship between identities and cryptographic keys. Some examples of these infrastructures include admission control and public key servers. The problem or weakness with this solution is that implementing these infrastructures in any network is very expensive and not easy.

Another solution is by the installation of SybilGuard [30], which is disclosure technique that focus on peer-to-peer users' social media. This mechanism works by identifying Sybils by exchanging keys between a user and limited number of his trusted friends. By combining these social networks, the user or observer can see that Sybil attackers have a small number of friends, so it will be easy to identify him. The problem with SybilGuard is that it suffers from high misclassifications or false negatives. For example, in some cases honest users are unfairly classified as Sybil attackers.

3.3 Attacks on Availability

Viruses: Viruses are a type of malware that were commonly used until recently. They are known to self-replicate by means of another system or person in order to circulate. There are many types of computer viruses, categorized according to the objects they infect.

- File infectors: which are divided into two subparts, direct infectors and memory-resident viruses. Direct infectors are viruses that are usually in an executable (.exe) file format and they instantly infect the system as soon as they are executed, and from there, they start to infect other files. Memory-resident viruses, as their name implies waits in the memory of the device for a host to execute it. WinCE.Duts.A is a virus that infected mobile devices that run Windows OS in 2004. The user receives a message prompting him to download a software, which turns out to be a virus. Then, the virus proceeds to infect the system [13].
- Boot-sector viruses: These types of viruses reside in the boot of the system and try to gain control of the system before the operating system. Dust also affected Windows devices, it resides in the kernel of the device and its main purpose is deleting all the data on the phone and resetting it to its factory settings [19].
- Multipartite viruses: are a combination of both file infectors and boot-sector viruses in which they have the abilities of both. It can be said that Dust can be an example of a multipartite virus since it also infects files.

Solutions: Several commercial and free-ware anti-virus software for mobile platform are available nowadays. The internal working of those software are similar to those of anti-malware, which is explained in detail in the above Sect. 3.1 on preventing malware attacks.

Worms: Worms are almost identical to viruses except for one major difference, they do not require "outside assistance", meaning they self-replicate within the

network and do not require the interference of a user [25]. The first mobile worm to have been created is the Cabir Worm, it is a cross-platform worm meaning it can infect a number of OSs, these include Motorola, Nokia, Panasonic, and Sony Ericsson that support the Nokia-licensed Symbian Series 60 platform [13].

Both viruses and worms are a threat to mobile systems since they can spread very easily. They therefore threaten the availability of the mobile phone because of their replication property and thus denying the legitimate owner access to the functionality of his/her phone. Also, an expected increase in worm attacks is predicted with the "network function virtualization" that is expected to be released for new generation mobile networks [10]. Network function virtualization is a method involving running "multiple concurrent virtual networks over a common physical network infrastructure". It uses Bluetooth and other wireless technologies to infect the devices [6].

Solutions: Like other malware threats, virus and worm infections in mobile phones can be prevented or at least limited by installing anti-malware, mentioned previously, and firewalls.

Botnets: A botnet is a network of machines which are under the control of a botmaster who uses them to conduct malicious attacks [25]. A computer or system being controlled by a botmaster is called a bot or zombie. Smart phones are prone to being turned into bots, and the device can be greatly affected by this issue. The signs of being infected include:

- Slowing down of the system, the phone will be much slower than usual and have lags more often, in other words the performance of the system will be lower.
- The device will freeze from time to time and may reboot by itself.
- The smart phone will send and receive data regularly even when there are no applications that would require it to do so.
- Strange behavior of the system.

Solutions: Botnets are quite dangerous and detecting them is obviously important, recent research for detection include behavioral detection approach, which checks the messages of the phone and detects which messages have been sent by or include malware by identifying the signature.

Denial of Service (DoS) Attacks: In addition, another type of attack is the denial of service attack. It occurs when the attacker attempts to render a system or device inaccessible by flooding it with data which will force the device to use its resources and make it unavailable [11]. In this case, the attacker ensures that the users of certain services are not able to use them. This kind of an attack is usually worse in the wireless networks. It enables the attacker to remain anonymous when launching his attacks.

Normally, the attacker floods the access point or the communication server with many requests in a manner that keeps the server busy trying to respond to these requests instead of connecting what the legitimate user wants [11].

Solutions: In order to deal with this kind of attack, the user deploys highly dedicated DoS mitigation systems. These systems are essential in filtering any malicious traffic. Normally, they are installed in front of the routers and the servers. Alternatively, one can use cloud computing mitigation providers, who are usually experts in DoS mitigation [29].

3.4 Attacks on Authentication

Authentication seeks to make sure that the user is indeed who he says he is by proving his identity using certain means and credentials that the system requests for. To defeat the system, hackers steel the identifying information and then use it to carry out unauthorized tasks.

Phishing: An typical attack on authentication is phishing. This is where criminals and fraudsters trick the mobile users in a manner that makes them share highly personal information with certain illegitimate websites. This usually occurs when mobile users are online and a pop-up appears. By clicking on such pop-ups, the criminals are able to obtain the information they want about the individual. They then use this information to commit fraud or other criminal offenses. Some of these frauds end up risking an individual's good name and good standing with his clients or other organizations that he deals with [27].

Solutions: There are many ways of dealing with phishing. The first solution to phishing is to try and avoid it at all costs. In order to do so, one must be careful to ensure they guard against all spams. In doing so, one should be careful when dealing with emails that seem to come from unrecognized senders. One should also be very suspicious with any email that ask for confirmation on their financial information or personal information. Such requests are usually made in urgency and sometimes they can appear when one is connected to internet doing something that may or may not be connected to the kind of information the email is requesting [27]. In some cases, such mails even tend to threaten the users with any frightening information in order to compel them to act swiftly.

Secondly, one should only ensure that they communicate personal information only when their mobile devices are secure. In doing so, they should also ensure they are also using secure websites. One of the best ways to distinguish between a secure website and an insecure website is by confirming that the website's URL begins with "https" and not simply "http". The URLs that have "s" tend to be more secure as the "s" stands for secure. Besides this, users can also avoid phishing by ensuring that they do not end up divulging personal information whenever they receive phone calls from numbers they have not saved in their mobile devices. This should be the case especially where the user is not the one who has initiated the call [27].

3.5 Attacks on Authorization

Authorization is similar to authentication in terms of granting access to users. It however differs from authentication as it has to do with the levels of rights and privileges given to each legal user [25]. In mobile computing, when a user downloads an app, he is usually asked to grant certain permissions that the app needs for its operation. This permissions determine the level of authorization or access control given to that particular app. For example, Android apps can query the APIs for user information like IMEI, location, contacts or call history and download history. A popular attack on authorization is whereby an app makes use of a covert channel to send out information to hackers.

Spyware: As mentioned previously, spyware is a type of malware that collects data from the infected system. A recent example of a spyware that exploits an app's privileges is Zitmo [10]. This spyware intercepts confirmation SMS sent by banks and thus it gains access to the user's confidential banking information like password, biodata. This information is then passed to the hacker for carrying out fraudulent activities.

Another example of a spyware that sends out users' information covertly is JackeeyWallpaper [23]. The collected data such as phone history, IMEI can then be sold to other illegal parties like scammers and phishers.

Solutions: The solutions are as discussed above in Sect. 3.1.

4 Limitations and Challenges

There exists challenges to security in mobile computing some of which have been addressed by the solutions in the previous section. These challenges exist due to the limitations in the mobile computing infrastructure itself and due to lack of compliance on the part of the users.

Lack of centralized management in mobile networks remains one of the challenges facing mobile computing security along with inadequate security standard [15]. Also, power constraints limit the ability to use and the effectiveness of anti-malware solutions in mobile devices. Often times, such anti-malware need to search through huge databases which deplete the power of the devices making them unattractive to the users.

On the part of the users, most users are incentivized to un-root their phones in other to have more control and to increase the functionalities of their devices. This however makes the devices easily susceptible to attacks. Another limitation is due to human error. Even with all the information, people tend to forget or genuinely make mistakes and they end up being affected by attacks. Therefore all mobile computing users are encouraged to ensure their devices are protected with an anti-virus, spam filters, anti-spyware software, and a secure firewall [27].

User education for security and privacy plays an essential role when it comes to mobile phone usage in personal as well as in business settings. Users' security education requires a holistic approach encompassing four aspects [16]:

- **Legal and Reputation:** Safeguarding, health and safety, data protection, intellectual property rights and copyright.
- **Organizational:** Learner recruitment, learner and employer relationship management, financial risk management, and staff development.
- **Technical and Operational:** Device management, network management, data management, and content management.
- **Teaching, Learning, and Assessment:** Materials and activities authoring, behavior management assessment, exams and marking, and candidate identity authentication, and plagiarism detection.

5 Conclusion

The security of mobile computing continues to face threats from attackers who gain access into the communication channel. Such attacks could include Sybil attack, phishing, denial of service attack (DoS), eavesdropping, and spoofing, malware, and message modifications among others. They can be prevented by using respective software such as personal firewall, anti-malware software, and encryption. Although all these solutions have certain weaknesses, extra measures are necessary to overcome such limitations. It is in our opinion that the user should also be knowledgeable of security issues and should not just download any application on his smart phone. Research should be made before downloading apps, and the user should be wary of emails, messages and wireless networks that he is not sure of. Moreover, users should not ignore security warnings that the system may issue. In conclusion, many security measures exist to prevent attacks from occurring however because of the continuous evolvement of the malicious software world, it is necessary for users to be made aware of this issue in order to be protected.

References

1. Adebayo, O.S., AbdulAziz, N.: Android malware classification using static code analysis and apriori algorithm improved with particle swarm optimization. In: Proceedings of 2014 4th World Congress on Information and Communication Technologies (WICT), pp. 123–128 (2014)
2. Bergman, N., Stanfield, M., Rouse, J., Scambray, J.: Hacking Exposed: Mobile Security Secrets and Solutions. McGraw-Hill Education, New York (2013)
3. Chien, E.: Motivations of recent Android malware. Technical report, Symantec Security Response (2011)
4. Deepak, G., Pradeep, B.: Challenging issues and limitations of mobile computing. Int. J. Comput. Technol. Appl. **3**, 177–181 (2012)
5. Desmedt, Y.: Man-in-the-middle attack. In: van Tilborg, H.C.A., Jajodia, S. (eds.) Encyclopedia of Cryptography and Security, p. 759. Springer, Heidelberg (2011)
6. Esposito, F., Matta, I., Ishakian, V.: Slice embedding solutions for distributed service architectures. ACM Comput. Surv. **46**, 6:1–6:29 (2013)
7. Fedler, R., Kulicke, M., Schutte, J.: An antivirus API for Android malware recognition. In: Proceedings of 2013 8th International Conference on Malicious and Unwanted Software: "The Americas" (MALWARE), pp. 77–84 (2013)

8. Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D.: A survey of mobile malware in the wild. In: Proceedings of 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), pp. 3–14 (2011)
9. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E.: Anomaly-based network intrusion detection: techniques, systems and challenges. Comput. Secur. **28**, 18–28 (2009)
10. He, D., Chan, S., Guizani, M.: Mobile application security: malware threats and defenses. IEEE Wirel. Commun. **22**, 138–144 (2015)
11. Ladan, M.I.: Mobile computing: security issues. In: Proceedings of 2013 International Conference on Wireless Networks (ICWN), pp. 1–6 (2013)
12. Lawton, G.: Is it finally time to worry about mobile malware? Computer **41**, 12–14 (2008)
13. Leavitt, N.: Mobile phones: the next frontier for hackers? Computer **38**, 20–23 (2005)
14. Li, W., Joshi, A.: Security issues in mobile ad hoc networks - a survey. Technical report, University of Maryland, USA (2008)
15. Masoud, N., Karimi, R., Hasanvand, H.A.: Mobile computing: principles, devices and operating systems. World Appl. Program. **2**, 399–408 (2012)
16. mEducation: safeguarding, security and privacy in mobile education. Technical report, GSMA Connected Living Programme: mEducation (2012)
17. Miller, C., Honoroff, J., Mason, J.: Security evaluation of Apple's iPhone. Technical report, Independent Security Evaluators (2007)
18. Nassar, M.: Wireless and mobile computing security challenges and their possible solutions. Am. Sci. Res. J. Eng. Technol. Sci. **3**, 66–74 (2015)
19. Peikari, C.: Protecting embedded devices with integrated permission control (2006). US patent number US20060026687 A1, http://www.google.com/patents/US20060026687
20. Pullela, S.: Security issues in mobile computing. Technical report, University of Texas at Arlington, USA (2002)
21. Quercia, D., Hailes, S.: Sybil attacks against mobile users: friends and foes to the rescue. In: Proceedings of 2010 IEEE International Conference on Computer Communications (INFOCOM), pp. 1–5 (2010)
22. Saha, H.N., Bhattacharyya, D., Banerjee, P.K.: Semi-centralized multi-authenticated RSSI based solution to Sybil attack. Int. J. Netw. Secur. Appl. **1**, 338–341 (2010)
23. Seo, S.H., Gupta, A., Sallam, A.M., Bertino, E., Yim, K.: Detecting mobile malware threats to homeland security through static analysis. J. Netw. Comput. Appl. **38**, 43–53 (2014)
24. Shields, C., Levine, B.N., Margolin, N.B.: A survey of solutions to the Sybil attack. Technical report, University of Massachusetts Amherst, USA (2006)
25. Stamp, M.: Information Security Principles and Practice. Wiley, New York (2011)
26. Vasudeva, A., Sood, M.: Sybil attack on lowest ID clustering algorithm in the mobile ad hoc network. Int. J. Netw. Secur. Appl. **4**, 135–147 (2012)
27. Verton, D.: Critical Threads 2006: IT*Security. Lulu.com, Raleigh (2006)
28. Wu, H., Schwab, S., Peckhams, R.L.: Signature based network intrusion detection system and method (2008). US patent number US7424744 B1, https://www.google.com/patents/US7424744
29. Xiao, Y.: Security in Distributed, Grid, Mobile, and Pervasive Computing. Auerbach Publications, Boston (2007)

30. Yu, H., Kaminsky, M., Gibbons, P.B., Flaxman, A.: SybilGuard: defending against Sybil attacks via social networks. In: Proceedings of 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM), pp. 267–278 (2006)
31. Zhou, Y., Jiang, X.: Dissecting Android malware: characterization and evolution. In: Proceedings of 2012 IEEE Symposium on Security and Privacy (S&P), pp. 95–109 (2012)