A Review of Android and iOS Operating System Security

Shahnawaz Khan[1]
Faculty of Engineering, Design and Information & Communications Technology
Bahrain Polytechnic,
Isa Town, Bahrain
shahnawaz.rs.cse@itbhu.ac.in

Ammar Yusuf
College of Arts and Science
Applied Science University, Bahrain
ammar.yousif@asu.edu.bh

Mohammad Haider
College of Computing and Informatics
Saudi Electronic University
Dammam, Saudi Arabia
m.haider@seu.edu.sa

Thirunavukkarasu K.
Department of Computer Science and Engineering
Galgotias University
Greater Noida, India
thiruk.me@gmail.com

Parma Nand
School of Engineering and Technology
Sharda University
Greater Noida, India
astya2005@gmail.com

Mohammad Khalid Imam Rahmani
College of Computing and Informatics,
Saudi Electronic University, Riyadh
11673, Saudi Arabia
m.rahmani@seu.edu.sa

***Abstract*— Mobile devices are an inseparable part of our lives. They have made it possible to access all the information and services anywhere at any time. Almost all of the organizations try to provide a mobile device-based solution to its users. However, this convenience has arisen the risk of losing personal information and has increased the threat to security. It has been observed recently that some of the mobile device manufacturers and mobile apps developers have lost the private information of their users to hackers. It has risen a great concern among mobile device users about their personal information. Android and iOS are the major operating systems for mobile devices and share over 99% of the mobile device market. This research aims to conduct a comparative analysis of the security of the components in the Android and iOS operating systems. It analyses the security from several perspectives such as memory randomization, application sandboxing, isolation, encryption, built-in antivirus, and data storage. From the analysis, it is evident that iOS is more secure than Android operating system. However, this security comes with a cost of losing the freedom.**

Keywords—Mobile device security, privacy threat, memory randomization, application sandboxing, isolation, encryption, iOS, Android

I. Introduction

Mobile devices have made our lives so easy and dependable. It is almost impossible to live without mobile devices for many of us. Technological advancements have increased the need for mobile devices multi-fold. The number of mobile devices currently in 2020 is 14.02 billion mobile devices and it is expected to increase to almost 17 billion mobile devices in the next 3 years (O'Dea, 2020b). Mobile devices use system software that enables the underlying hardware of the mobile device. This system software for mobile devices is known as a mobile operating system (MOS). Mobile operating systems is a self-explanatory term, that can be simply stated as the operating system embedded in mobile devices as a software to run applications and programs on mobile devices.

Based on research by O'Dea (O'Dea, 2020a), 99.42% of the mobile devices use either the Android or iOS mobile operating system. However, the increasing number and excess involvement of mobile devices in our daily routine have amplified the risk of security of private information. In the last couple of years only, a few cases of stealing the personal data of the users such as the Facebook data breach case (Chan, 2020), Canva data breach (Canva, 2020), and Dubsmash data breach (Dubsmash, 2019). Collectively, the personal data of almost billions of users were impacted by these incidents. However, there are several reasons for data breach and stealing but the fact, that mobile devices based apps collect several kinds of personal information, cannot be neglected. If this personal information is not secured than it might pose different threats (such as financial, life, and personal identity, etc.) to an individual. Therefore, having a secure platform while using a mobile device is a must. The security requirements for these operating systems include various technical aspects such as memory randomization, application sandboxing, encryption, built-in anti-virus, and data storage format. The threats against security would also be taken into consideration.

Mobile devices have given access to various kinds of applications and services on our fingertips. For example, if you are accessing some information that is in a different language then you can use machine translations (Shahnawaz, 2011; Shahnawaz & Mishra, 2015; Khan & Usman, 2019) to convert it to your language of choice. Capturing photographs is common using mobile devices, users can use some artificial intelligence-based apps and services to process the image and assess the quality (Bashir et al, 2017). Mobile devices also provide access to cloud services that can be used even for scientific applications such as big data processing (Khan & Kannapiran, 2019) or other machine learning applications (Shahnawaz & Mishra, 2013a, 2013b; Khan et al, 2018)

This research conducts a comprehensive comparative analysis of the Android and iOS operating systems' security. It provides an extensive study to understand how these MOSs work from the security perspective. Security is one of the most important features for consumers. So that, they can trust the mobile device with their insensitive information and data.

II. Mobile OS and Security Threats

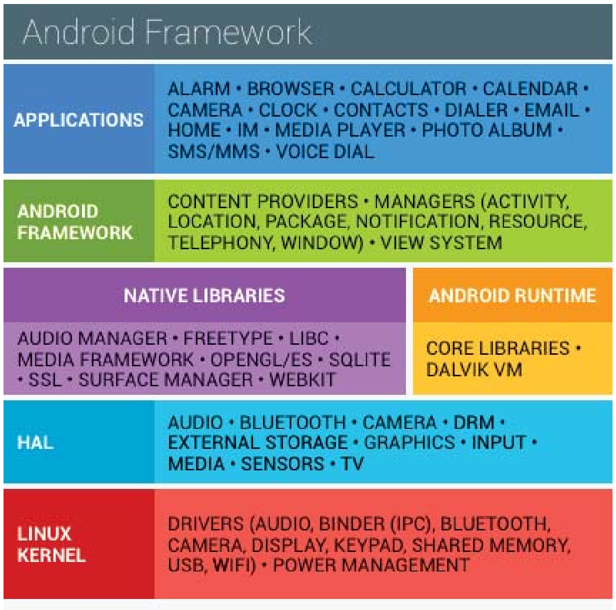
In 2005, Google acquired Android Inc. and in 2008, Android was launched for mobile devices (Morrill, 2008). Android has seen several versions of it, the latest android version is Android 11. Being open-source and flexible for the

2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS) | 978-1-6654-6919-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICETSIS55481.2022.9888847

978-1-6654-6919-7/22/$31.00 ©2022 IEEE

Authorized licensed use limited to: Vivekanand Education Society's Inst of Tech. Downloaded on August 26,2024 at 04:01:08 UTC from IEEE Xplore. Restrictions apply.

users to download anything they want and use it, Android has gained the 74.6% market share (O'Dea, 2020a). Google play store is the official market to download and install applications in android based mobile devices. The following figure (figure 1) illustrates the android framework. Android uses Dalvik Virtual Machines developed by them instead of Java virtual machines due to licensing issues. Not all Android devices get the same update at the same time. Different brands and different models get the latest version of Android at a different time this is due to the development of Android-based on the specific models. As all the devices do not get the latest security patches and upgrades, it makes the mobile device vulnerable against different types of security threats.



Android Framework

APPLICATIONS: ALARM • BROWSER • CALCULATOR • CALENDAR • CAMERA • CLOCK • CONTACTS • DIALER • EMAIL • HOME • IM • MEDIA PLAYER • PHOTO ALBUM • SMS/MMS • VOICE DIAL

ANDROID FRAMEWORK: CONTENT PROVIDERS • MANAGERS (ACTIVITY, LOCATION, PACKAGE, NOTIFICATION, RESOURCE, TELEPHONY, WINDOW) • VIEW SYSTEM

NATIVE LIBRARIES: AUDIO MANAGER • FREETYPE • LIBC • MEDIA FRAMEWORK • OPENGL/ES • SQLITE • SSL • SURFACE MANAGER • WEBKIT

ANDROID RUNTIME: CORE LIBRARIES • DALVIK VM

HAL: AUDIO • BLUETOOTH • CAMERA • DRM • EXTERNAL STORAGE • GRAPHICS • INPUT • MEDIA • SENSORS • TV

LINUX KERNEL: DRIVERS (AUDIO, BINDER (IPC), BLUETOOTH, CAMERA, DISPLAY, KEYPAD, SHARED MEMORY, USB, WIFI) • POWER MANAGEMENT

Fig.1: Android Software Stack, source: https://source.android.com/

iOS is a mobile operating system, developed by Apple in 2007. It supports only the mobile devices developed by Apple such as the iPhone, iPad, and iPod touch (Costello, 2020). It uses the XNU hybrid kernel of Darwin. Darwin is a Unix-like kernel developed by Apple. iOS just like Android has undergone several upgrades to keep up with its rival and to provide its users a better experience. The current version of iOS is version 14 and the official market for iOS applications is the App store. The figure (figure 2) illustrates the integrated secure subsystem in the Apple chips.

A. Security Threats

Several types of security threats can arise in various forms of mobile devices. Threats can be caused by applications that are installed in the device. These applications may contain malicious code that has specific targets to breach the security of the device. It has been most likely from third-party source downloaded apps (Bhuyan et al, 2017). Malware can enter the device and start changing the code of the system, get access to unauthorized user data, send emails or messages, get information about messages, phones, and contacts stored in the device without the user's knowledge (Hussain et al, 2018). There may be several loopholes in the security of different installed applications on the device. These loopholes make it easier for people with wrong intentions to manipulate and attack other people's data. This happens as developers are in hurry to launch their app and do not check the security functions of their applications.

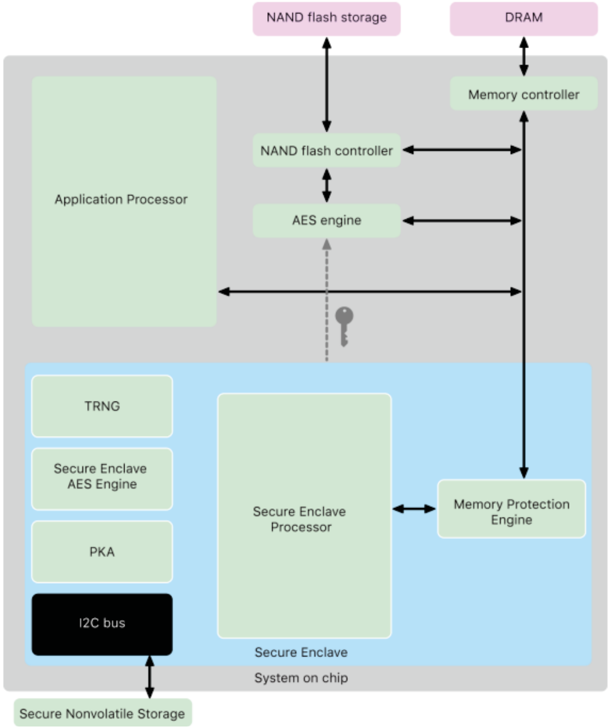


Fig.2: iOS Secure Enclave components, source: apple.com

It has been detected that location privacy has been leaked by several apps, giving away the exact coordinates and location of the users (Primault et al, 2018). This is mostly seen in social network apps. Web applications can also cause threats to a user's security. However, they might not be always as specific as mobile devices. But it does put the mobile device's security in danger. The most common web threat is phishing where links are sent to people to trick them thinking it's a real website and they give away their credentials. A physical level threat is where the physical mobile phone is lost or stolen. This is because mobile phones are small and portable, the chances of losing them are higher. The data in the mobile devices then become easily accessible to others. The need to protect the device from losing is a concern and many mobile devices come with a tracking option and locking the phone until a correct password or answer to a question is entered (Ali & Awad, 2018). The threats discussed in this section provide us a general idea of the worst possible scenarios of breaching security. The following section discusses the security requirements for mobile operating systems.

III. Analysis of Processes for Mobile OS Security

As discussed in the earlier section, the major cause of security threats to mobile devices comes from the mobile apps installed by third-party developers or in some cases from the mobile apps installed from the app stores. Android and iOS have released regulations, guidelines, and security requirements that must be followed by the app developers. However, some of the app developers don't follow these strictly. This section analyses the security requirements provided by Android and iOS, how they are similar and different from each other. It also describes how threats can

Authorized licensed use limited to: Vivekanand Education Society's Inst of Tech. Downloaded on August 26,2024 at 04:01:08 UTC from IEEE Xplore. Restrictions apply.

penetrate and cause damage to the device or user's information by exploiting these. The following figure 3 illustrates the security components for mobile operating systems.

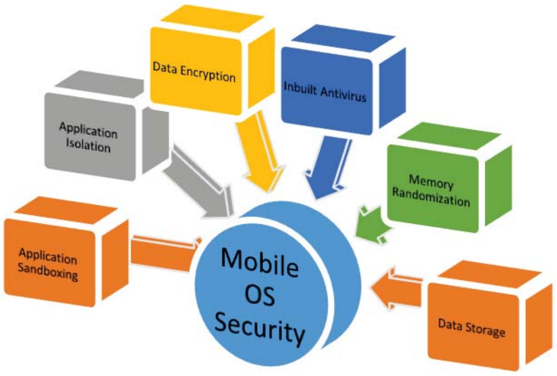


Fig.3: Security components for mobile operating systems.

A. Application Sandboxing

Application sandboxing is the process to limit the functionalities of a code that can execute due to certain entitlements or declarative permissions. These entitlements or permissions are assigned when an app is created. These entitlements or permissions are not dynamic and cannot change during runtime or by OS kernel. This is an important layer of protection for mobile OS and increases security. Application sandboxing acts as a container and prevents the applications from gaining access to the system or other applications that may contain the virus and malicious code (Ahmad et al, 2013; Novac et al, 2017). Unique ID (UID) is assigned to each application. When an application runs, it runs through a separate process. In iOS, the application sandboxing controls and limits the access of the application to just the file system, hardware, and network. It also has a special robust model for sandboxing applications that have similar sandbox model is more reliable and secure and reduces the access to the public crowd (Sehgal et al, 2018).

In Android, as it is based on Linux, sandboxing is also on Linux based kernel platform. Android sandboxing is robust and complex. Each application requires approval and permission to continue and access what the application requires and needs (Greene & Shilton, 2018). Each application exists in the sandbox's directory and the permissions directly depend on the application. This helps to improve the security better and tighter. Even though both have the same approach in sandboxing but iOS is better than Android in this context as iOS allows the users to access the system file in the root and not for each application as Android does during installation (Sehgal et al, 2018; Greene & Shilton, 2018). However, Android does allow the users to set the security as per their wish with the permissions. But it does not apply to every application. As a result, there are more chances of being exposed to threats in Android and more risk of loss of personal information.

B. Application Isolation

Applications are executed and isolated in the sandbox environments of their device. During execution, as applications are isolated in their environment, they are unable to make changes to other applications (Greene & Shilton, 2018). In iOS, isolation is done where the applications work in their environment and have no knowledge, privileges, and access to other applications in the kernel (Novac et al, 2017). In short, apps cannot abuse other apps. Third-party applications are controlled by iOS and they have very limited influence over the system (Ahmad et al, 2013). There are few things the apps can do without the user's permission that includes access to the camera, device ID, calendar, and Wi-Fi connectivity. On the other hand, iOS is strict with giving no access and isolating the apps from emails and SMSs of the user. Thus, isolation does not only involve in the kernel for security measures but also emails and messages as well. SMSs and emails can be sent by the Apps only after user's permission. Isolation does not give complete security even when it is isolating applications from each other in the kernel. Network-based and web-based attacks are prevented due to isolation (Sehgal et al, 2018).

Since some resources can still be accessed by the application, a malicious application can be used to steal sensitive information by the attackers. Like iOS, Android follows the same technique of isolation. It isolates the applications from each other in the kernel as well. But in Android, the user is asked for permission to be given for certain resources, and the isolation is done accordingly. Isolation of every app takes place from the system's kernel that makes sure there is no vulnerability and no probability of compromising the administrator level of control (Hussain et al, 2018). This disables the attacker's intention to compromise other applications using a malicious application on an Android device. But if specific permissions are given then a list of other applications can be generated. It can start an application in the background or even pop it up, for example, Google Music App opens automatically to the user. It can gain access to the application's code and check for logic. This includes the SD Card a user inserted in the device for additional usage. It can access, read, and modify the SD card without the user having any knowledge of it whatsoever. There are no restrictions on it and mostly downloaded files, music, and videos are stored on it. It all depends upon how the user allows different permissions that can cause different types of attacks and access to the device's subsystems.

C. Data Encryption

Encryption is the process of converting and translating data into code to prevent unauthorized access (Kenny et al, 2007). It is an eminent approach and well-known for being effective in data security. If the data is encrypted, then a password or special key is necessary to decrypt the file and gain access to retrieve the encrypted information. Data that is encrypted is called ciphered text and unencrypted data is simply called a plain text. Encryption is necessary for mobile devices, especially, in an unforeseen circumstance when the mobile device is stolen. It secures the product by encrypting it. However, the key may be removed remotely and once it is removed the device becomes vulnerable. Android introduced encryption from its 4.0 version onwards and it was device encryption API (Leung et al, 2016; Novac et al, 2017).

iOS has a fully functional mobile device management API available to use. Android encryption is based on disk encryption(dm-encrypt) (Greene & Shilton, 2018). In Android, to get access to the encrypted file, it is necessary to have a password or pin to decrypt it. For both Android and

Authorized licensed use limited to: Vivekanand Education Society's Inst of Tech. Downloaded on August 26,2024 at 04:01:08 UTC from IEEE Xplore. Restrictions apply.

iOS, the developers cannot access without encryption codes. It is also possible that all the data can be stored in plain text by the developers (Sehgal et al, 2018). Both MOSs allow storage of secrets as cipher-text on the disks. It depends upon the developers how they want to make use of it and most of the time while designing the developer does not necessarily always take the advantage of encryption.

D. Inbuilt Antivirus

The most common three types of malware that are known to affect the mobile devices are spyware, viruses, and trojans (Zhou & Jiang, 2012). A virus is a software containing malicious code. Spyware collects information from users without their consent and knowledge. A trojan is a misleading software that depicts some normal functionality but instead is harmful to malicious content. An antivirus usually protects against such type of attacks. Android and iOS provide their inbuilt antivirus support system (Ahmad et al, 2013). Some Android devices come with an extrinsic antivirus software provided by the device manufacturer as a bundle with the device. But within Android itself, only Google play store has antivirus detection for the applications being provided to the customers. Since Android provides the freedom to install applications from third-party sources, it increases the risk of installing some malicious content. Therefore, it poses a security risk to download applications outside the Google Play store as a result. Android does ask the user when they download applications from third-party sources whether they want to give the access and permissions or not, if given once then the mobile is in a vulnerable state (Sehgal et al, 2018).

Apple has worked on its app store more to make sure all the available applications are thoroughly tested and do not contain malicious codes. The code signing certificates also enhances security (Zhou & Jiang, 2012; Mohamed & Patel, 2015). The antivirus structure for iOS is an extreme one. As it carefully checks the virus without the need of having antivirus software on the mobile. Apple does not allow its mobile devices to download from any other source than its legit App store. This might make Apple more secure, but Android is an open-source that is the reason for them to allow more freedom to the users. Apple is more secure and less likely to virus attacks on the contrary Android is more vulnerable to virus attacks (Novac et al, 2017; Greene & Shilton, 2018).

E. Memory Randomization

To prevent malicious attack or virus from locating the exact position or memory region, memory is allocated randomly. This is done as the running application's memory allocation becomes hard to find for the malicious code. In memory allocation not only the memory of running application is allocated randomly but also the shared libraries and other as such things in regard to the device (Jang et al, 2016). Developers are extra careful even after the implementation of memory randomization. They add layers of programming techniques to create additional security from buffer overflow and memory corruption.

Both android and iOS didn't always have memory randomization (Mohamed & Patel, 2015). iOS implemented their memory randomization from version 4.1 whereas Android started it with the Jellybean release (Novac et al, 2017). Apple was the first one to embed it in iOS before Android. iOS are also ahead with their security by introducing code signing technology where the developer must have a certificate from Apple to be validated to post their application for other users to use. This is done mainly to prevent third-party harmful applications. Every unauthorized application must have this Apple certificate for them to share their applications. As a result, the operating system is kept secured and trusted with new apps. As a result, iOS is more secured than Android in terms of memory randomization with the extra factor they have code signing (Sehgal et al, 2018).

F. Storage Format

Data can be stored both internally and externally on mobile devices. This process is known as data storage. Mobile devices come with built-in storage space. The user must choose what kind of sensitive data they want to store on it as well as to make sure it is protected and secure. In Android devices, both internal and external (if necessary) storage device is provided. External storage can be stored on an SD card installed additionally. If an SD Card is inserted in the device, Android does not force the applications to ask for any permission. Applications get access to the SD card to use whenever required (Kim & Kim, 2012). Crypto libraries are used as a security measure to keep the stored data safe as it acts as a password policy. It is possible that with root access a malicious code can find the keys of encryption. As there are no permissions and restrictions for external storage, malware can be spread from both external storage to the device and vice versa (Ahmad et al, 2013).

iOS does not support its devices to have external storage, it only allows built-in storage. Even within the internal storage, it requires permission to make use or manipulate the data. This is a safety measure. As Android has its crypto libraries, iOS has complex passphrases that work with Data Protection (APIs) to protect the data (Daryabar et al, 2016). It makes iOS more difficult to manipulate and use data than Android. Hence, iOS devices have minimal chances of attracting malware or losing sensitive information and data to others than Android devices.

IV. Discussion

This research provides an analysis of different components and measures taken to ensure the security of the mobile devices and the user data by Android and iOS. It has been observed by several researchers that even though the techniques and methods for security are almost similar in Android and iOS operating systems, but iOS mobile devices are more secure (Zhou & Jiang, 2012; Kim & Kim, 2012; Ahmad et al, 2013; Mohamed & Patel, 2015; Daryabar et al, 2016; Leung et al, 2016; Novac et al, 2017; Sehgal et al, 2018; Greene & Shilton, 2018, etc.). This research study is in agreement with the existing researches. For example, the memory randomization in iOS is more secure because of code signing technology. However, it is also important to consider that Android is an open-source operating system and allows the installation of apps from third party sources. It is one of the major reasons for vulnerabilities. Another key consideration is the user's choice. Android allows the user to make some of the decisions such as for apps' permissions and installation of unverified apps. Sometimes, it leads to creating a security threat to the user's personal data. If the user is not being careful, then the personal information of the user is vulnerable. The following table 1 summarizes the security features for Android and iOS mobile operating systems. From the analysis, it is evident that iOS is more secure than Android operating system. However, this security comes with a cost of losing the freedom. The iOS applications and environment is

Authorized licensed use limited to: Vivekanand Education Society's Inst of Tech. Downloaded on August 26,2024 at 04:01:08 UTC from IEEE Xplore. Restrictions apply.

more secure as it has certain restrictions such as limitation of choosing the source of app installation or external storage etc, While Android users have more control over their devices and can make choices about the sources of installation of apps, storage systems and a number of other choices, this freedom develops security vulnerabilities if the user is not aware of the consequences of the choices he/she is making.

Table I: Comparison of Security components for mobile OS

Components	iOS	Android
Application Sandboxing	Shared sandboxing; more secure because of the resource access limitation	Individual app sandboxing; Each app requires approval and permission in order to continue and access
Application Isolation	Apps work in their environment and have no knowledge, privileges, and access to other apps in the kernel; Apps cannot abuse other apps.	Follows the same technique of isolation as in iOS; but user chooses the permissions for isolation that may cause security vulnerabilities
Data Encryption	Disk and other hardware level security such as custom CPU capabilities and dedicated silicon security functions	Disk encryption (dm-encrypt); a password or pin is required for decryption
Inbuilt Antivirus	Has inbuilt antivirus; an extreme antivirus structure; only Apple store apps can be downloaded; less freedom, more secure	Has inbuilt antivirus; Apps are scanned by play store and device manufacturers often provide an antivirus system; more freedom, less secure
Memory Randomization	Available; Unauthorized apps must have this Apple certificate; Code signing technology makes it more secure	Available; however, apps can be installed from untrusted source and absence of code signing technology makes it vulnerable to security attacks.
Storage Format	Does not support its devices to have external storage and uses complex passphrases that work with Data Protection (APIs) to protect the data	Supports external and internal storages; uses Crypto libraries are used as a security measure

V. Conclusion

Mobile devices have become an important part of everyone's lives. Android and iOS mobile devices are the most popularly owned throughout the world. Every mobile device user wants their personal data to be safe and private to themselves, only when necessary to share with others. It is evident based on the analysis of iOS and Android that iOS has better security measures than Android. Android devices are more likely to compromise users' data, but it also provides freedom to its user. But with this freedom, comes certain responsibilities as well. It requires certain knowledge on how to prevent any leakage of data. Consumers buy mobile devices for features but if security is the topic of concern and the user is not careful then iOS is more recommendable. iOS security features from the application's code signing certificates to the system's measures are commendable.

References

[1] Ahmad, M. S., Musa, N. E., Nadarajah, R., Hassan, R., & Othman, N. E. (2013). Comparison between android and iOS Operating System in terms of security. In 2013 8th International Conference on Information Technology in Asia (CITA) (pp. 1–4).

[2] Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. sensors, 18(3), 817.

[3] Bashir, T., Usman, I., Khan, S., & Rehman, J. U. (2017). Intelligent reorganized discrete cosine transform for reduced reference image quality assessment. Turkish Journal of Electrical Engineering & Computer Sciences, 25(4), 2660-2673.

[4] Bhuyan, S. S., Kim, H., Isehunwa, O. O., Kumar, N., Bhatt, J., Wyant, D. K., ... & Dasgupta, D. (2017). Privacy and security issues in mobile health: Current research and future directions. Health policy and technology, 6(2), 188-191.

[5] Canva. (2020). Canva Security Incident – May 24, https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/ Retrieved on September 10, 2020.

[6] Chan, R. (2020). "The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections". Business Insider. Retrieved September 10, 2020.

[7] Costello, S. (2020). The History of iOS, from Version 1.0 to 13.0, Lifewire, Updated on March 11, 2020https://www.lifewire.com/ios-versions-4147730, Retrieved September 11, 2020.

[8] Daryabar, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K.-K. R. (2016). Forensic investigation of OneDrive, Box, GoogleDrive and Dropbox applications on Android and iOS devices. Australian Journal of Forensic Sciences, 48(6), 615–642.

[9] Dubsmash. (2019). Notification of a Data Security Inciden, https://dubsmash.com/user-notice, Retrieved on September 10, 2020.

[10] Greene, D., & Shilton, K. (2018). Platform privacies: Governance, collaboration, and the different meanings of "privacy" in iOS and Android development. new media & society, 20(4), 1640-1657.

[11] Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., & Albahri, A. S. (2018). Conceptual framework for the security of mobile health applications on android platform. Telematics and Informatics, 35(5), 1335-1354.

[12] Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., & Albahri, A. S. (2018). Conceptual framework for the security of mobile health applications on android platform. Telematics and Informatics, 35(5), 1335-1354.

[13] Jang, Y., Lee, S., & Kim, T. (2016, October). Breaking kernel address space layout randomization with intel tsx. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 380-392).

[14] Kenny, F., Jihyun, H., Chung, Y. E. C., & A, L. M. M. (2007). Providing secure inter-application communication for a mobile operating environment.

[15] Khan, S. N., & Usman, I. (2019). Amodel for english to urdu and hindi machine translation system using translation rules and artificial neural network. Int. Arab J. Inf. Technol., 16(1), 125-131.

[16] Khan, S., & Kannapiran, T. (2019, March). Indexing Issues in Spatial Big Data Management. In International Conference on Advances in Engineering Science Management & Technology (ICAESMT)-2019, Uttaranchal University, Dehradun, India.

[17] Khan, S., Mir, U., Shreem, S. S., & Alamri, S. (2018). Translation Divergence Patterns Handling in English to Urdu Machine Translation. International Journal on Artificial Intelligence Tools, 27(05), 1850017.

[18] Kim, J.-M., & Kim, J.-S. (2012). AndroBench: Benchmarking the Storage Performance of Android-Based Mobile Devices. ICFCE, 667–674.

[19] Leung, C., Ren, J., Choffnes, D., & Wilson, C. (2016, November). Should You Use the App for That? Comparing the Privacy Implications of App-and Web-based Online Services. In Proceedings of the 2016 Internet Measurement Conference (pp. 365-372).

[20] Mohamed, I., & Patel, D. (2015). Android vs iOS Security: A Comparative Study. 2015 12th International Conference on Information Technology - New Generations

Authorized licensed use limited to: Vivekanand Education Society's Inst of Tech. Downloaded on August 26,2024 at 04:01:08 UTC from IEEE Xplore. Restrictions apply.

[21] Morrill, D. (2008). "Announcing the Android 1.0 SDK, release 1". Android Developers Blog. September 23, 2008, https://android-developers.googleblog.com/2008/09/announcing-android-10-sdk-release-1.html, Retrieved September 11, 2020.

[22] Novac, O. C., Novac, M., Gordan, C., Berczes, T., & Bujdoso, G. (2017). Comparative study of Google Android, Apple iOS and Microsoft Windows Phone mobile operating systems. 2017 14th International Conference on Engineering of Modern Electric Systems (EMES).

[23] O'Dea, S. (2020a). Market share of mobile operating systems worldwide 2012-2020, https://www.statista.com/, published on Aug 17, 2020, Retrieved on September 10, 2020.

[24] O'Dea, S. (2020b). Market share of mobile operating systems worldwide 2012-2020, https://www.statista.com/, published on Feb 28, 2020, Retrieved on September 10, 2020.

[25] Primault, V., Boutet, A., Mokhtar, S. B., & Brunie, L. (2018). The long road to computational location privacy: A survey. IEEE Communications Surveys & Tutorials, 21(3), 2772-2793.

[26] Sehgal, K., Jain, A., Nagrath, P., & Kumar, A. (2018). Recent Advances in Networks and Data Security Survey on Various Mobile Operating Systems. International Conference on Innovative Computing and Communications Lecture Notes in Networks and Systems, 181–190.

[27] Shahnawaz, & Mishra, R. B. (2013a). Rule-based approach for handling of case markers in English to Urdu/Hindi translation. International Journal of Knowledge Engineering and Soft Data Paradigms, 4(2), 138-165.

[28] Shahnawaz, & Mishra, R. B. (2013b). Statistical machine translation system for English to Urdu. International Journal of Advanced Intelligence Paradigms, 5(3), 182-203.

[29] Shahnawaz, & Mishra, R. B. (2015). An English to Urdu translation model based on CBR, ANN and translation rules. International Journal of Advanced Intelligence Paradigms, 7(1), 1-23.

[30] Shahnawaz, M. R. (2011). ANN and rule based model for English to Urdu-Hindi machine translation system. In Proceedings of National Conference on Artificial Intelligence and agents: Theory& Application (AIAIATA 2011) (pp. 115-121).

[31] Zhou, Y., & Jiang, X. (2012). Dissecting Android Malware: Characterization and Evolution. In 2012 IEEE Symposium on Security and Privacy (pp. 95–109).

Authorized licensed use limited to: Vivekanand Education Society's Inst of Tech. Downloaded on August 26,2024 at 04:01:08 UTC from IEEE Xplore. Restrictions apply.