Mobile interaction and security issues

Pornsak Preelakha

Department of Information and Technology, Faculty of Engineering and Technology,
Panyapiwat Institute of Management, Nonthaburi 11120

Received: 6 September 2018/ Revised: 21 November 2018/ Accepted: 6 December 2018

Abstract

People once witnessed an interaction method between a user and mobile devices where buttons used to play a prominent role in interacting with the device. However, such interaction has been developed from the past in a variety of ways as we can see from the advancement of smartphones, tablets, and smart devices. Buttons were replaced with a touch screen system, along with many new methods to interact with a mobile device such as voice, camera, and fingerprint. These novel methods have a lot of input, saying the Virtual Reality and Augmented Reality that already has been taken in by the mobile devices. The modern interaction methods aim to give its users the best experience in the areas of communication and interaction. They are expected to have a great ability to access and simple to use. Regardless of the positive light, the new interaction methods may provide, they arguably have a shortcoming for its safety of use. Seeing that the security issues of advanced interaction methods should be explored further, this article has been conducted on the pattern of interaction, both direct and indirect way, between devices and users in different methods to see the potentiality of the security issues that may harm its users.

Keywords: Mobile, HCI, Security, Interaction, Mobile security

Corresponding author: pornsakpre@pim.ac.th

Introduction

Nowadays, mobile devices have become a must-have item for everyone. The number of smartphone users worldwide is estimated to surpass 2 billion by the end of 2016 [1]. Meanwhile, tablet shipments from 1st quarter to 2nd quarter 2016 stood at 78.3 million units [2]. The reason behind the popularity of mobile devices is its interaction with humans. Its user-friendly feature allowing people at all ages to be able to use is proved to be a key factor for wide adoption of mobile devices.

Given the rising popularity of mobile devices, major manufacturers and researchers have been finding new methods to interact with mobile devices shifting their interest from the traditional touchscreen which was considered as a standard feature installed in any mobile devices. Samsung Electronics released its first smartphone, Samsung Galaxy Note Series which introduced a pressure-sensitive digitizer and a stylus pen developed by Wacom Co., Ltd in October 2011. In 2015, Apple Inc. launched iPhone6s with 3D touch enabling pressure-sensitive touch inputs. In the following year, they removed the physical home button from iPhone7 and replaced it with a touch-sensitive button with haptic feedback.

However, the progress of mobile devices stirs the questions in regards to their security. Several weaknesses have been found in both long-standing and newly-invented approaches to mobile device technology where hackers and cyber-criminals benefit from. They are able to intercept sensitive information from data transmitted between smart watches and smartphones. The security issues of mobile devices must be protected from an array of issues, threats, risks in order to provide security. Moreover, some security measures cause uncomfortable and inconvenient experience where users might decide to disable those measures and expose themselves to even more risks.

From the reasons given above, this paper aims to explore current methods of mobile interaction and its possible security threats upon users. The paper will be divided into five parts. The first part will explain the basic knowledge of the mobile device. The second part will be about the exploitation of mobile security threats. The third part will focus on security challenges related to mobile interaction method. The fourth part is guideline aimed to mitigate mobile security risk, and the final part will provide a conclusion and interesting topics for further study.

General knowledge of mobile technology

Mobile interaction is a study of the interaction between mobile users. Mobile devices are a pervasive part of people's everyday lives. These devices are the first truly pervasive interaction devices that are currently used for a huge variety of services and applications.

As we all know, the mobile device is a computer that comes into a size of the pocket and can be held in one hand, although some models are large and require both hands to hold. Major mobile devices can be separated into two types, smartphones and tablet computers.

A. Smartphone

The smartphone combines the idea of computers and mobile phones together. It is able

to perform computer operations made it outstanding from the traditional mobile phones which provide mostly voice calling and text messaging functionality with limited multimedia and internet capabilities [3] [4].

Even though a term "smartphone" was coined in 1997, a mobile phone considered as the first smartphone was Simon Personal Communicator introduced in 1992. Simon was developed by International Business Machines (IBM) and BellSouth Corporation with approximately 50,000 units being sold. Since then, smartphones' popularity has been increased gradually from the 1990s to 2010s. Some well-known manufacturers from this period were Samsung, Nokia, Motorola, and Sony Ericson. A turning point of smartphone technology took place in 2007 when Apple Inc. revealed the iPhone to the world for the first time. The smartphone introduced in that period of time combined powerful multimedia functions with the same features seen in previous models of the smartphone with a consumer-friendly design. This marked as the beginning of an era for a modern smartphone. Presently, two major smartphones' operating systems are iOS and Android which overwhelm the market with a 99.3% share by the second quarter of 2016 with an insignificant share of other operating systems such as Windows Phone at 0.7%.

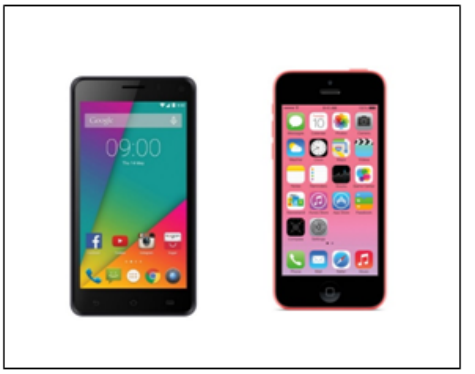


Figure1. Android and iOS Operating System [5]

B. Tablet computer

The tablet computer is a portable wireless computer where its distinction stands between smartphone and personal computer. Tablet computers provide much greater processing power and battery than a smartphone but are lighter than a personal computer. Four general types of tablet computers found in markets are Slate Tablet, Convertible Tablet, Hybrid Tablets, and Rugged Tablet.

C. Summarized characteristics of mobile device

1. Screen display

The majority of the mobile devices has a very large touchscreen occupying over 80% of the front side along with the high-definition resolution.

2. Hardware sensors

Various types of sensors are incorporated in mobile devices which enhance their capabilities to handle the physical world.

3. Connectivity

Mobile devices' ability to send and receive a large amount of data is provided and supplemented by numerous technologies of the wireless data network and wireless data connection such as 2G, 3G, and 4G technologies, Bluetooth, Wi-Fi, Infrared and Near Field Communication.

4. Battery life

The power consumption rate of mobile devices is noticeably high. Therefore, most of the manufacturers would install a powerful battery with ample capacities to ensure that general usage can last long throughout a day.

Exploiting mobile security threats

Mobile devices are identified with several security issues similar to those found in Personal Computers. With rapid growth of mobile device consumption and a lack of knowledge regarding computer security among users, mobile devices thus become an attractive target for all kinds of the malefactor. Security threats can be even more harmful when mobile devices generally store the sensitive and confidential information such as credit card details, personal contacts, emails, as well as users' social media accounts saying Facebook, Google, Microsoft, Apple, or Twitter.

Threats to mobile devices can be grouped into three major categories: data confidentiality, data integrity, and system availability. These threats are more likely to attack the functionality of mobile devices rather than a user.

A. Eavesdropping

Eavesdropping also known as a man-in-the-middle attack is a technique which two parties are communicating with each other and there are third parties rely on or alter data sent between them secretly [6]. The way to steal information is intercepted conversation such as listening to people while talking or other voice communication including an attack by interception data on the network, steal personal information. The eavesdropping attack will most effective when detecting data without encryption service. But sometimes eavesdropping was applying to detect unusual behavior on the network. A concept of eavesdropping is illustrated in the following figure 2.

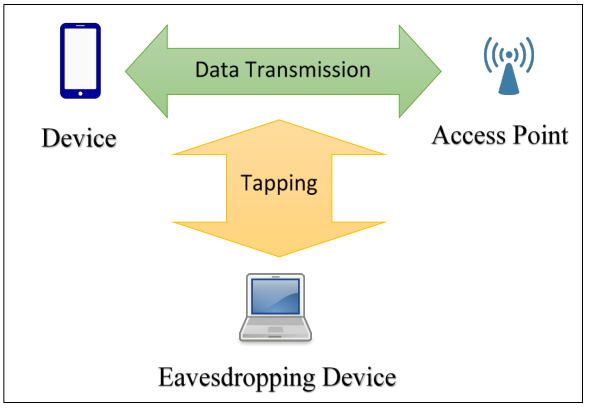


Figure 2. An Illustration of Eavesdropping

B. Smudge attacks

Smudge Attack is a technique for predicting passcode from oily residues left on the touchscreen device using the pattern tracing method. When a user unlocks the screen, the oily smudges are normally left on the screen as shown in figure 3. These smudges can be detected by spotting residues marks on the touchscreen and analyzing the pattern of those marks. An entire operation only requires easy-to-find tools such as a camera and a computer and an image processing software. This way, hackers can access into a smartphone's passcode by taking pictures from a victim's smartphone screen, editing the picture contrast and then inferring the pattern used to unlock the smartphone. An attack is performed by spotting residues marks on the touchscreen and analyzing the pattern of those marks [7].

With most modern mobile devices rely on the touchscreen as the main method to interact with users, smudge attack is considered as a serious threat. The security of mobile devices can be more vulnerable when they are stolen and a robber tries to access the devices to take away some sensitive information or reset devices for reselling.

Figure 3. Oily residues (Smudge) on touchscreen [7]

C. Shoulder surfing

Shoulder Surfing is a relatively straightforward technique for stealing sensitive information. The attacker will simply observe targets via physical eyes when they are filling a form or keyring password [8]. A process could be performed at a distance using vision-enhancing devices like binoculars. Additionally, an attacker may utilize small low-cost camera by concealing them inside ceilings, walls or fixtures to record data entry.

The attackers take advantage of a portable large screen mobile device allowing the users to carry them around in the public, unlike the desktop computers that most of the time remain immobile. These characteristics of the mobile device make them an excellent target for shoulder surfing. The example of the event should look like this: an attacker stands behind the victim and watches at their smartphone when they are filling in a password for e-mail account. By this way, an attacker is able to access a target's e-mail account and reset the password and steal an account as a result. Shoulder surfing requires a physical observation that is very hard for a victim and people in the crowd to notice,

hence it is recommended that the users of the mobile device should search for a quiet location before opening personal accounts on mobile phone staying away from the crowd as much as possible.

D. Malware

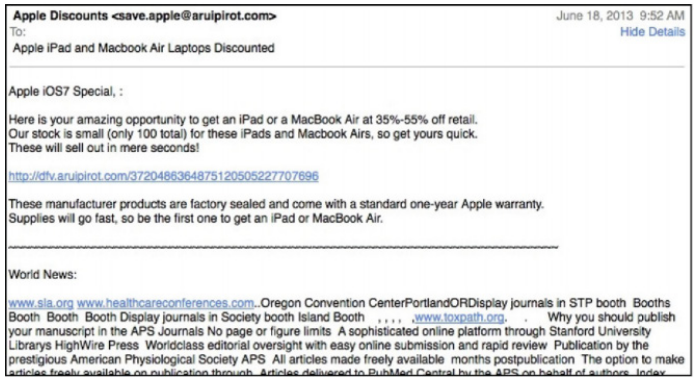
Among a countless number of mobile applications, there are applications embedded with malevolent purposes such as tampering smartphone operations, acquiring sensitive information, gain access to smartphone systems or display undesired advertisement. Attackers run this threat either by employing the phishing technique, disguise malware into completely normal applications then and uploading them to digital distribution platforms (App Store, Google Play, Windows Store), or having smartphone download malware automatically when users visit infected websites [9].

In another word, malware is performed to disrupt the device to gather private information and show unwanted advertisers without users' knowledge. Sometimes, malware can be found in another kind of software or automatic download from websites.

The amount of those applications with a malware found has been rising at an astounding rate. On September 1, 2016, Nokia releases a report stating that an infection rate of a mobile device increased by 96% in the first half of 2016 with 78% of the infected device being found in smartphones. In addition, Malware also has been found to be more tricky and complicated resulted in greater difficulty in protecting or repairing [10, 11].

E. Phishing attack

The general concept of phishing attack is that malefactors will send text messages or contents including link connecting to a website page that convinces the users to enter personal data or malware via SMS, MMS, or e-mail. The intention is to steal sensitive information including usernames and passwords [12]. The examples of phishing messages can be seen from the text claiming that users have won a contest or inviting users to join events is illustrated in figure 4. Recently, several attackers have turned to the spoofed messages claiming themselves to be from legitimate and well-known organizations such as Apple, Google, Microsoft or any other big companies. These messages usually ask for an account validation aiming to deceive users to enter their sensitive information.


Apple Discounts <save.apple@aruipirot.com> June 18, 2013 9:52 AM
To: Hide Details
Apple iPad and Macbook Air Laptops Discounted

Apple iOS7 Special, :

Here is your amazing opportunity to get an iPad or a MacBook Air at 35%-55% off retail.
Our stock is small (only 100 total) for these iPads and Macbook Airs, so get yours quick.
These will sell out in mere seconds!

http://dfv.aruipirot.com/37204863648751205052277076 96

These manufacturer products are factory sealed and come with a standard one-year Apple warranty.
Supplies will go fast, so be the first one to get an iPad or MacBook Air.

World News:

www.sla.org www.healthcareconferences.com..Oregon Convention CenterPortlandORDisplay journals in STP booth Booths Booth Booth Booth Display journals in Society booth Island Booth , , , , ,www.toxpath.org, . Why you should publish your manuscript in the APS Journals No page or figure limits A sophisticated online platform through Stanford University Librarys HighWire Press Worldclass editorial oversight with easy online submission and rapid review Publication by the prestigious American Physiological Society APS All articles made freely available months postpublication The option to make

Figure 4. Example of Phishing Message [13]

F. Data leak

Data leak or data breach involves a situation where a confidential information was disclosed to the untrusted environment both intentionally and unintentionally. A cause of leakage ranges from simple mental recollection and careless discarding of data storage media to a large-scale attack performed by cyber criminals or national institutions. Based on the Breach Level Index, there are 5,329,418,398 data records that have been leaked since 2013 and only 4% of those leaked data were encrypted [14].

Mobile devices have a high possibility of having their data inside leaked given that there is enormous information circulated in and out at every single minute. Users who have little or no knowledge regarding a security protocol of mobile device may unknowingly expose their devices to threats and leak data themselves. An example of a situation would be that an employee sent a new product's design to his boss over an unencrypted Wi-Fi resulted in his work being stolen by a rival company.

G. Unsecured Wi-Fi

Unsecured Wi-Fi refers to any Wi-Fi hotspot which lacks adequate security measures such as having user authentication, enabling security protocols (WPA, WPA2) and disabling wireless administrating. Weak security could be exploited easily by cybercriminals to attack mobile devices having access to Wi-Fi by intercepting and recording transmitted package by packet analyzer software [15].

The majority of free Access Point or Wi-Fi connection offered by mobile operators is unsecured. Most of them lack the encryption for transmitted data attempting to provide a convenience for users to connect an access point. Unsecured Wi-Fi may rely on the spoofed access claiming to be a legit and reliable source. Those fake access points aim to trick users to believe they gain access to a trustworthy connection entering their username and password exposing the important information to criminals resulted from a lack of knowledge regarding security issues.

H. Broken cryptography

While the encryption is necessary and recommended feature of modern mobile devices, inappropriate activities performed by developers still leave the encrypted data vulnerable for hackers to take advantage of. That means the encrypted data can be as vulnerable as the unencrypted one if taken control by malicious developers. Broken Cryptography involves a situation where hackers manage to uncover sensitive information due to the improper use of encryption. There are two major contributors which usually lead to Broken Cryptography as follows [16].

1. Poor Key Management Processes.

Many developers lack expertise in the security field and tend to mishandle the encryption process and leak important information to the attacker unintentionally.

2. Use of Insecure and/or Deprecated Algorithms.

Some cryptographic algorithms like MD5 and RC4 are considered as outdated ones since they could be broken into easily by high-performance computers. Broken Cryptography found in mobile devices typically is a consequence of applications that are developed with the insufficient security standard. For example, novice programmers may make use of weak encryption algorithms (MD5, SHA1) due to the fact that they consume less CPU resources than heavy encryption algorithms. In another case, an application may send out username and password in plain text instead of encrypted form to save time and shorten the work procedures.

Security challenges related to mobile interaction method

There are numerous methods to interact with mobile devices nowadays. Each method possesses issues regarding its security which need to be explored and learned further. Most of the interaction requires specific hardware to detect and communicate with Biometrics or metrics related to human features usually to enable identification and access control. Biometrics have been seen as interesting major manufacturers for years, and several types of Biometric are already integrated with flagship mobile devices. There is three well-known Biometrics which are Iris, Face, and fingerprint. This paper will explore some notable examples including Touchscreen, Voice-Based Interaction, Iris Recognition, Face Recognition, Fingerprint Recognition, and Mobile Device Peripherals.

A. Touchscreen

The most prominent interaction method is touchscreens. Its basis was found in the music industry around 1948 and its concept, which is still used until present time, was proposed in 1965 by E. A Johnson [17]. Touchscreen technology adopted widely by mobile device vendors is capacitive touchscreen which is a grid of tiny, transparent electrodes with its ability to detect user's touches via the change in the electrostatic field [18].

Touchscreen technology definitely comes with advantages. As simple and straightforward as it may seem, it allows users to interact directly with the object appearing on the screen. Thus, mobile devices become less complexed and many users who might rarely experience any electronic devices

so far are encouraged and convinced to use it. Moreover, an interaction operated on the basis of the touchscreen is very easy for users to understand with little effort needed. While touchscreens are an essential part of the modern mobile device, they are also a weak point that could be exploited by hackers. Two main threats to the touchscreen which were already mentioned previously are mainly Shoulder Surfing and Smudge Attack.

B. Voice-based interaction

Voice-based interaction has become a widely-adopted feature among mobile devices as well. It allows users to communicate with devices without the use of the touchscreen, physical button or other interaction devices. Voice-based interactions can be classified into several types. Speech output systems which only utilize speech for output while receiving inputs via other technologies. Google Text-to-speech and Voice-over by Apple fall into this category. Speech recognition systems which utilize speech for input and other techniques for output, such as Google Voice Search, Bing Speech API. Spoken dialogue systems which utilize speech for both input and output. Some well-known systems that are available for smartphones include Siri, Cortana, Google Voice Search, and Google Assistant.

Voice-based interaction enables users to interact with mobile devices via their voice. It is beneficial particularly for elderly people with physical challenges who are hindered from using mobile devices conveniently and effectively. In fact, past research indicated that elderly people generally prefer voice user interface over graphical user interface or traditional physical interaction especially if the voice user interface can support natural input language [19].

Currently, a capability to control mobile devices with speech-based interaction is constrained by its systems having a limitation to define commands. For example, Google Now and Siri rely on pre-defined keywords or phrases to select appropriate functions. If they fail to detect any keywords, the entire input will be treated as a web search query [20]. Main security threat for Voiced-based Interaction is voice impersonation. A hacker expertise in speech synthesis is capable of mimicking voice of valid users to bypass authentication system. A challenge to a voice-based interaction is how it can provide voice recognition system a legit ability to distinguish real human voice from artificial voice generated by third-parties' computers.

C. Iris recognition

Iris Recognition is an identification method that distinguishes each person by detecting unique formats within the ring-shaped region surrounding the pupil of the eye called Iris. It is categorized as one type of Ocular-based identification which based on unshared patterns in the human eye. Other examples of Ocular-based identification such as retina recognition and Eye vein verification [21].

Using Iris for recognition provides several advantages to users. First, humans' eyes are internal organs which have rarely changed from childhood to adulthood except for particular circumstances. Second, Iris patterns are unique that even left and right eye having different patterns. Third, the widely-accepted Iris recognition algorithms like John Daugman's IrisCode have a very low false match rate which indicates accuracy of this method.

Regardless of the mentioned benefits, Iris recognition still has many shortcomings. The necessary equipment is particularly costlier than some other forms of biometrics. The lower grade of iris scanners could be deceived by a high-quality image of an iris. Users are required to hold their head steady at very close range from the camera resulted in difficulty in using among users. In another case, ocular surgery may cause changes in iris patterns and the recognition might not be functioned as a result.

D. Face recognition

Face Recognition or Facial Recognition is an identification method by analyzing determined facial features such as the relative position, size, and shape of a nose, eyes, jaw, and cheekbones. Currently, it is used for a variety of purposes ranging from security, gaming, and photography. A major company like Facebook also uses facial recognition technology to help tag user in photographs automatically [22].

E. Fingerprint recognition

Fingerprint recognition is an identification method using human fingerprints. It works by detecting and comparing unique patterns found in fingerprints like arch, loop and whorl. It is one of the widespread techniques that many mobile devices already integrated with fingerprint recognition such as Apple Touch ID.

Fingerprint has several advantages comparing to other biometrics. First, it is considerably cheaper than some methods like iris recognition thus more economical for large-scale deployment. Second, fingerprint recognition is a standardized technology and one of the most developed biometrics. Third, it is easy to use by users who may be unaccustomed with modern technologies. Forth, it provides a high security standard since fingerprints are hard to be copied or spoofed and modern fingerprints scanners are very accurate in processing, although they are still affected by dryness or dirty of the finger's skin as well as the age of users [23].

Therefore, using biometrics has several advantages. First, they are easy to use by users who may be unaccustomed with modern technologies. Two, they are hard to be lost in normal situations. Third, current biometric scanners have been developed well and their accuracy is in satisfied level for large-scale deployment.

However, there are still some security challenges to biometric which need to be taken seriously. Unlike text password, it is nearly impossible to change an individual's biometrics except under some special circumstances. If copies of biometrics are made, there are no effective means to disable a falsification allowing further misuse to be taken place. While biometrics are difficult to lose, they still can be stolen rather easily. For instance, human facial features could be captured from the users being unaware and a trail of fingerprints can be left everywhere in everyday life. Although they have been developed for a long time, current biometrics sensors still can be deceived in many ways. Fake fingerprints which are made from various materials to replica human skin can probably get the pass through smartphone's fingerprint scanners. In another example, a low-tier of iris scanner can be tricked by high-quality images of iris.

F. Mobile device peripherals

Mobile Device Peripherals refer to any hardware that can receive inputs, send output and store data in mobile devices. In this paper, other types of computer like a desktop computer, laptop computer are also studied as well. A purpose of Peripherals is to enhance mobile device capabilities. To give examples, external speakers can generate better quality sound compared to embedded speakers. Wireless mobile hard drive offers additional storages to smartphone. Desktop computers are capable of processing high-end game and stream it to tablet [24].

Peripheral also introduces the user to handle their device in new ways other than the experience in using touchscreen and buttons. Some sample cases are as follows. Most users think that using stylus pen give them better results for drawing images on a tablet, using the external keyboard is much quicker and more comfortable than small virtual keyboard, using a Bluetooth headphone allowing users to continue their current activities during conversations with a partner, etc.

Security issues might not be a worthy topic to be discussed in the past when most of the peripherals still were connected to computer via cables. Nevertheless, the growth of mobile device usage and increasing numbers of wireless peripherals also create new opportunities for hackers since the characteristics of wireless connection make it easier to be attacked than the connection busing wires. Peripherals themselves can be used to initiate an attack as well. Security concerns regarding Mobile Device Peripherals mostly are from technologies used to connect them to mobile devices. Mainstream connection methods are Bluetooth and Wi-Fi which are analyzed by various researches in regards to their vulnerabilities. Connection over Wi-Fi exposes mobile devices to have eavesdropped and unnecessarily Bluetooth enabling could increase the possibility of devices being harmed from hackers' threat.

G. Measurable metrics

When developers designed interfaces for modern application making use of human-computer interaction. However, each method also has security issues that come with its new technology. From the table below, the measurable metrics are summarized into different interaction methods and their possible mobile security issues.

The relation between the security challenges and mobile interaction as shown in Table 1.

Table 1 security challenges related to mobile interaction method

Interaction method	Security Issues
Touch Screen	smudge attack, shoulder surfing
Voice-based	eavesdropping, voice impersonation
Iris Recognition	data leak, uncomfortable
Face Recognition	photograph, spoofing attack
Fingerprint Recognition	smudge attack, data leak
Mobile Device	unsecured wi-fi, broken
peripherals	cryptography

Conclusion

The main purpose of HCI is designed to the interface is easy to use, easy to understand, make it attractive and make the difference for modern application. But most of the interaction method was designed by without security concern. The currently various mobile application falls in risk and may cause the mobile device is not safety. This article proposed a mobile interaction method and their security threats in measurable metric to minimize the possible vulnerabilities that could be exploited by the attackers when designing human-computer interaction in a modern application for the mobile device. The security issues of mobile devices must be protected from an array of issues, threats, risks in order to provide security.

In the future work, we will study the proposed data trace method to detect mobile security threats with the analysis of the noncompliant coding styles and collection of the attacking patterns by exploiting the vulnerability to prevent data leakage and unauthorized access.

References

1. Statista. Number of smartphone users worldwide (in millions). [Internet]. 2016 [cited 2019 February 11]. Available from: http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
2. Statista. Worldwide tablet shipments from 2nd quarter 2010 to 2nd quarter 2016 (in million units). [Internet]. 2016 [cited 2019 February 11]. Available from: https://www.statista.com/statistics/272070/global-tablet-shipments-by-quarter/
3. Techopedia. Mobile Device. [Internet]. [cited 2019 January 15]. Available from: https://www.techopedia.com/definition/23586/mobile-device
4. Dictionary.com. Mobile device. [Internet]. [cited 2018 December 10]. Available from: http://www.dictionary.com/browse/mobile-device

5. IDC Research. Smartphone OS Market Share, 2016 Q2. [Internet]. 2016 [cited 2018 December 11]. Available from: http://www.idc.com/prodserv/smartphone-os-market-share.jsp
6. Tran H, Zepernick HJ. Proactive attack: a strategy for legitimate eavesdropping.in 2016. In: IEEE Sixth International Conference on Communications and Electronics (ICCE), 2016. pp. 457-61.
7. Aviv AJ, Gibson K, Mossop E, Blaze M, Smith JM. Smudge attacks on smartphone touch screens. In proceedings of the 4th USENIX Conference on Offensive Technologies, Berkeley, CA, USA; 2010. pp. 1-7.
8. Mali YK, Mohanpurkar A. Advanced pin entry method by resisting shoulder surfing attacks in 2015. In: International Conference on Information Processing (ICIP), 2015. pp. 37–42.
9. Chang WL, Sun HM, Wu W. An android behavior-based malware detection method using machine learning in 2016. In: IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 2016. pp. 1-4.
10. Nokia. Nokia malware report shows surge in mobile device infections in 2016. [Internet]. 2016 [cited 2017 September 1]. Available from: http://company.nokia.com/en/news/press-releases/2016/09/01/nokia-malware-report-shows-surge-in-mobile-device-infections-in-2016
11. Nokia. A mobile device infections surge in 2016. [Internet]. 2016 [cited 2017 September 1]. Available from: https://www.msn.com/en-za/news/techandscience/mobile-device-infections-surge-in-2016-nokia
12. Ahmed AA, Abdullah NA. Real time detection of phishing websites in 2016. In: IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2016. pp. 1-6.
13. Julie JCH, Ryan C, Cade K. Predicting susceptibility to social influence in phishing emails. Int J Hum Comput Stud 2019;(128):17-26.
14. Gemalto NV. Data breach statistics. [Internet]. 2016 [cited 2018 August 30]. Available from: http://breachlevelindex.com/
15. Chen Y, Trappe W, Martin RP. Detecting and localizing wireless spoofing attacks in 2007. In: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007. pp. 193-202.
16. TechTarget. Broken cryptography and data security. [Internet]. 2015 [cited 2018 August 20]. Available from: http://searchsoftwarequality.techtarget.com/photostory/2240177848/Top-ten-threats-to-mobile-enterprise-security/10/Broken-cryptography-and-data-security

17. Banks R. The origin of the touchscreen. [Internet]. 2015 [cited 2018 August 23]. Available from: http://www.mobileindustryreview.com/2015/04/touchscreen-inventors.html
18. Baanto. History of touch screen technology. [Internet]. 2016 [cited 2018 September 11]. Available from: http://baanto.com/touch-screen-technology-history
19. Schlogl GCGMTLS. Exploring voice user interfaces for seniors. In: Pervasive Technologies Related to Assistive Environments (PETRA), Rhodes, 2013.
20. University of Rochester, Google Research, Carnegie Mellon University. Just speak: enabling universal voice control on android. In: The International Cross-Disciplinary Conference on Web Accessibility, Seoul, 2014.
21. Patil S, Gudasalamani S, Lyer N. A survey on Iris recognition system in 2016. In: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016. pp. 2207-10.
22. Khan N, Gupta M. Face recognition system using improved artificial bee colony algorithm in 2016. In: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016. pp. 3731-5.
23. Priya R, Tamilselvi V, Rameshkumar GP. A novel algorithm for secure Internet Banking with finger print recognition in 2014. In: International Conference on Embedded Systems (ICES), 2014. pp. 104-9.
24. Farooq A, Evreinov G, Raisamo R. Enhancing mobile device peripheral controls using Visible Light Communication (VLC) in 2015. In: 9th International Conference on Sensing Technology (ICST), 2015. pp. 623-8.