Scholars Journal of Economics, Business and Management e-ISSN 2348-5302
Sch J Econ Bus Manag, 2017; 4(8A):474-481 p-ISSN 2348-8875

(An International Publisher for Academic and Scientific Resources) **DOI:** 10.36347/sjebm.2017.v04i08.002

The Security Risk Issues of Smart Phones on a Global Level (A Case Study of the President of the United States, Barack Obama)

Mr. Yaseen Myasar Fathi
Lecturer at Department of Management Information Systems, College of Administration and Economics University of Mosul - Erbil - Iraq.

*Corresponding Author
Yaseen Myasar Fathi
Email: yaseen.myasar@yahoo.com

Abstract: During this modern age of technology, security risk issues of smartphones have increased recently, despite the high adoption of smartphones globally, with different ages of users and with a wide variety of smartphone functionalities and services, such as, video calls, multimedia services, and Bluetooth and Global Positioning System (GPS). User data and sensitive information has become more general and pervasive, because users have to agree on providing some of the personal details, for example, an email address in order to download an app in addition to software use, such as Viber and WhatsApp. Furthermore, users do not know if the mobile data accessed by application providers is legal or not. All these reasons make for an easy penetration of smartphones and the manipulation of personal information of users, either through malware or hackers. However, these risks will not stop in the future, as they evolve and grow with the development of technology. Moreover, it is not legally acceptable. Consequently, this report discusses the diffusion of smartphones, with an analysis of the increasing security risks of using smartphones globally. Also, this report covers security risk statistics and examples, in addition to focusing on the security threats aspects from malicious software and attacks by hackers. FlexiSpy and Ikee.B are examples of virus software. Usually consumers do not achieve the main purpose of using smartphones such as accessing their bank account and online shopping because of the worry of these threats. For example, 12 million Americans had their identity stolen. Furthermore, it affects businessmen, politicians and employees in companies. This paper focuses on legal and technical solutions which can control and manage the risks. Therefore, users and companies need to use some of these important legal measures and techniques when using smartphones in order to protect their devices from attacks. For example, users are advised to register with legal data protection companies and buy only legal copies of software security. Finally, the research discusses some legal security applications for users.

Keywords: Smartphone, security risks issues, threats, malicious software, BYOD

INTRODUCTION:

The development of mobile device technologies has rapidly increased during recent years. This development has included both hardware and software techniques. There has been an increasing appetite for smartphones from users on a global level, because of the ease of use, in addition to the services and applications which are provided, Jeon *et al*. [1] On the other hand, these functionalities enjoyed by smartphones have led to an increasing in security risks, such, as the impact of malware on them. However, smartphone became such as the computers vulnerable to malware threats and attacks are more than that.

This paper presents the case study of smartphone prevalence worldwide and then will focus on an analysis and detailed discussion of the risks associated with their use, in addition to smartphone risk statistics. In fact, there are two sources that are risks to smartphones which effect consumers, employees and companies. The research will cover these threats with examples of virus applications, as well as security risk examples. Also, there is a group of security software that can identify these risks. Finally, this paper will suggest solutions divided into two aspects: consumers and corporations with supported examples.

DEFINITION AND THE FAMOUS TYPES OF SMARTPHONE:

A smartphone is a type of mobile phone which appeared recently, and is a combination of the services and functions of mobile phones and computers. Furthermore, it includes many advanced features and facilities. For example, most have internet access, different kinds of applications, web browsers, a high ability of communication video calls, multimedia service, games, Global Positioning System (GPS), network and easy use of operating systems with a touch screen. They can also share data and have apps [2,3].

The most famous makes of smartphones are iPhone Apple and Android 'Samsung', in addition to

"Research in Motion (RIM) Blackberry, Symbian, and Windows Mobile-based devices" [3]. Therefore, customers have adopted and used them for personal and business purposes, in different areas of the world, and their platforms have become famous [4]. Siciliano [5] claims that 417 million mobile phones were sold in 2010 worldwide, and that smartphones sales made up to 19.3 percent of them. Furthermore, there are up to 5 billion Smartphone users worldwide.

ANALYSIS OF THE DIFFUSION OF SMARTPHONES GLOBALLY AND THE INCREASE OF SECURITY RISKS:

Kakihara [6] summarized in his study the diffusion of smartphones globally. The study covered 28 countries and an analysis of consumer behaviour in adopting smartphones between 2011 and 2013, as shown in figure 1 that demonstrates smartphone penetration.

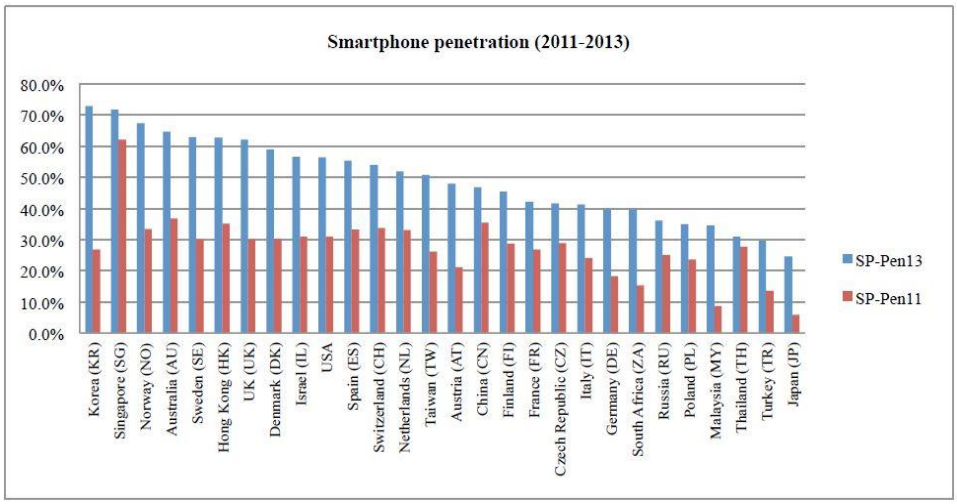

Fig-1: Illustrates the diffusion of smartphones globally, Kakihara [6].

However, these multi-purpose smartphones require more personal information of users, for example, an electronic mail address, home address, personal photos and a phone number [4]. All these things influence security risk issues. Furthermore, Chin *et al*. claimed that despite the popularity of the smartphones in the world, users still do not achieve the full potential and benefit of their smartphone devices because they are worried about the privacy and security risks [7]. For instance, half of American adults have smartphones, but purchases made by mobile phones only make up just 3 percent of overall online shopping.

As Chin *et al*. add in another instance, a recent commercial survey shows that 60 percent of device users do not make payments using their mobiles because of the uncertainty regarding security [7]. Customers are worried that they will be putting their financial and personal information at risk.

Chin et al. claim that to provide, improve and increase smartphone securty, users need to understand the danger and worries of dealing with it [7]. According to this, Chin and *et al*, studied 60 smartphone user opinion about excecuting a specific action using their mobile compared with a laptop. For example, the tasks were managing their bank account, online shopping, social safety numbers and health data.

This study also covers smartphone applications for Android and Apple, and the understanding of all installation aspects; for example, which sources individuals usually use to gain them and whether these sources are reliable. Finally, the result of Chin *et al*. showed firstly, that individuals are extremely concerned when conducting their business, especially when connected with finance because of the risk to privacy [7]. Secondly, users are worried about theft, personal data damage and malicious or cunning applications. In addition, there is also the threat of wireless network assailants, as illustrated in the following figure 2.

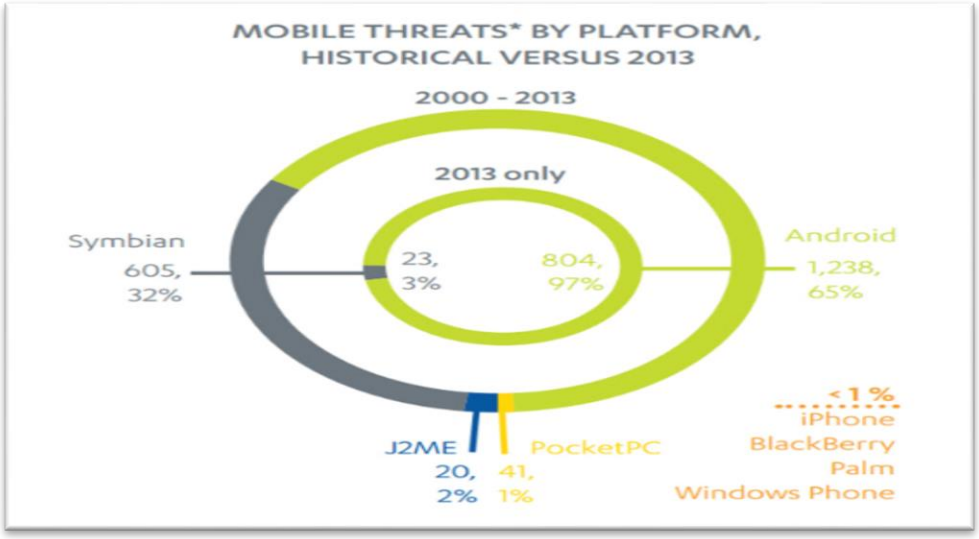

Fig-2 shows smartphone threats from 2000 to 2013 compared with 2013 only, Kelly [8].

SMARTPHONE RISK EXAMPLES AND STATISTICS OF UNLAWFUL DESTRUCTION:

According to Orlando Sentinel [9] statistics show that 12 million Americans had their identity stolen in 2011. In addition, 62 percent of smartphones users do not have a good security application on their devices to save them from attacks. As Lipka [10] added, one-third of smartphone users are more susceptible to identity theft. Another study by Rotenberg [11] uncovered that 533 million cases were registered in the reports of Privacy Clearinghouse about information being penetrated via smartphones.

HP company completed a study about the level of applications' security risks. This study covered more than 2000 software from 600 different organizations. The results showed that 97 percent of surveyed software included weak privacy points. Additionally, approximately 86 percent of them were without standard features of security, while 75 percent of the contained weak encryption issues, Jundi [12].

ASPECTS OF SECURITY THREATS FOR SMARTPHONES:

There are two kinds of threats to smartphones. In fact, both of them occurs with the use of applications. First of all, there is penetration by malicious software which tampers with the contents of the device to annoy users and which is completely similar to those that occur with computers. Secondly, there are breakouts by hackers and attackers. This kind involves the attacking and intercepting of personal information, such as user name and password [13]. This will be discussed later in detail; therefore, the following are some examples of these applications:

MALICIOUS APPS:

This type of malware was created more than ten years ago to affect and threaten smartphone security, and increased in 2004. For instance, Cabir is kind of Bluetooth worm impacting apps, and it moves between smartphone devices with Bluetooth. It aims to keep Bluetooth always connected, annoying users and manipulating the data, Technical Information, [3].

IKEE.B:

Is the other important example, because it was a first iphone worm and it is one of the malwares inspired by financial motivation, created by an Australian programmer. This virus runs on iPhone Apple and it affects them through the manipulation of stored delicate financial data, in addition to the movement from the device to others and control by WiFi. However, those especially at risk are those who firstly have installed a secure shell application which allows them remote control. The hacked system allows them install unreliable apps from the Apple store, especially, users do not change the default password of the secure shell application [14,15].

FLEXISPY:

Is a type of Spy software, and it works as commercial spyware on smartphone devices. It is priced up to $349.00 per year. It has many extremely dangerous function and abilities. For example, it can eavesdrop on calls remotely, tapping the calls when they occur, accessing and reading the texts of short

message service and call logs in addition to electronic mail. Displays and location of the user can also be discovered through GPS. Also, it can control and change emails remotely. Furthermore, it can control all phone communication by accepting or rejecting it. However, FlexiSpy has the ability to apply all these dangerous jobs without being detected [3, 16].

In a critical way, this application claims that it is an educational program, but in fact, it has serious functions on the smartphones when users install it [3]. Therefore, the individuals have to understand these threats and how to deal with it, especially, if the consumer has sensitive information on his phone, or is part of an important working environment, such as an employee of the bank, company or government. Global malware statistics are shown in figure 3 below.

Fig-3 shown global malware statistics, *Canadian* [17].

SECURITY RISK EXAMPLES:

The President of the United States, Barack Obama, stressed in more than one meeting that he does not use Apple's iPhone due to issues regarding security because the iPhone does not cover the required level of security clearance[18]. This is despite the iphone occupying the first place in terms of reliability and sobriety in smart devices (then followed by Samsung). As the Washington Post stated there are some legal limitations and legitimacy, which does not allow the country's director to use the digital devices as a public user [19].

Whittaker [20] gives the example about the registered case by security researchers of FireEye about a security flaw in the operating systems IOS 7 and IOS 8 called 'Masque Attack. This flaw uncovered fake download applications via reliable applications such as Google Mail to bring the device under the control of electronic hacking. The idea is to lure the user to press the subversive malware links or a text message to install them, and then the application that was installed will be tooled to theft device information without the user's knowledge. This has been know to attack versions of IOS 7.1.1, 7.1.2, 8.0, 8.1 and 8.1.1.

Security Issues [13] confirmed that when consumers in some countries use the internet in public and congested places, for example, markets, public libraries and restaurants, where the Internet connection is unencrypted and non-security, this provides an easy opportunity for attackers and hackers to penetrate personal information such as user names and passwords. This then allows access to various financial infromation and other accounts, such as bill payments, bank account access and financial transfers. Even if the user has the protection program of the bank, the attacker can make changes to the information path from the secure path to insecure path to be able to penetrate them more easily.

THE IMPACT OF SECURITY RISKS ON COMPANIES AND STAFF:

Buliox claims their study showed the effect of using smartphones on the employees [21]. The private communications devices for companies may be subject to legal surveillance. Therefore, when the employees use their private smartphones for email or communication rather than companies' devices, this means they will be on probation. Here is a very

important issue, as the impact will be from two sides: firstly, the risk on the privacy information for employees, and by the tracking communications legally from the Company. Secondly, there could be a catastrophic effect on the privacy information of companies or banks through the easy access of the attackers into employees' smartphones, because they do not contain any strong protection system, and the result is that companies' information will be in enormous danger when the employees use their own devices, as illustrated in the following figure 4.

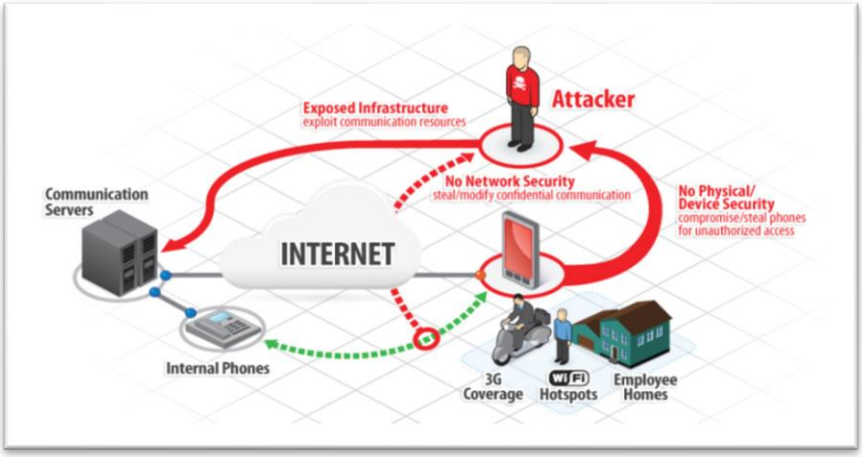

Fig-4 shows the use of smartphones across unreliable networks by employees, [22].

The best example is 'BYOD- Bring Your Own Device'; this is one of the policies that is used by some companies. It allows for employees to do the company's communications by using their own smartphone. Therefore, this policy is incorrect, because they may not have a security application on their phones, and that will put the organization's information at enormous risk in addition to the employee's information [23].

RESULTS OF THE DISCUSSION

The legal measures and procedures of smartphones security risks in technology : "Data protection brings positive benefits to the management of information and, properly applied, is not a barrier to effective business practice in either the public or the private sector " [24]. Data controller "means a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed" [25]. Use of Codes of Practice – Information Security Management ISO 2006. Therefore, the solutions can be divided into two main points.

Firstly, the Legal technical responsibilities for companies: to avoid all the risks, attacks and threats, at first, do not use 'BYOD- Bring Your Own Device' because it is incorrect policy and leads to many security information risks. Employees should only use the company devices during work time and they should have a strong operating system with continually updated protection applications. Another point is that employees should only buy the original copy of software security. Alos, there should be more active security measures about sensitive information of the organization, for example, VoIP protocol [23, 26], as illustrated in figure 5.

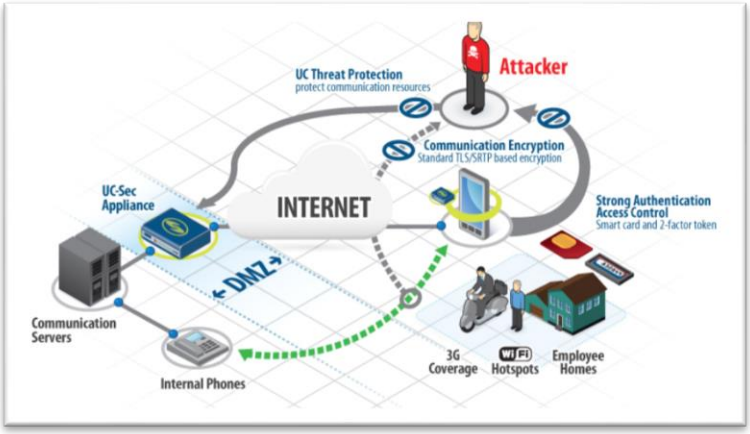

Fig-5 shows the use of smartphones via reliable protocols by employees [22].

Secondly, the technical legal responsibilities for individuals: Firstly, consumers should not break the smartphone security system which is provided by Android or Apple stores, to obtain free applications, because this is the main reason of threats. Also, they should not install or download free and unlegal applcations or, unofficial and unknown resource software such as Amazon Appstore. Thirdly, they should click on links from mailings and advertisements that are from an anonymous source, because they are just a hoax, especially, anything conncete with finance.

In addition, users should not save sensitive information on their phone, especially information such as banking accounts passwords. This will ensure that consumers will be protected, even if they lose or have their devices stolen, because 24 percent of users did that [5]. Also, buying the original and legal copy of software security will be reliable from the smartphone platform such as Google Play, with continually updated antivirus applications Mylonas *et al.* [26], for example AirWatch and the AirWatch Software Development Kit (SDK) [27].

Moreover, if the operating smartphone system included security features, the usuer should enable all these functions. The best example of protection is using a PIN to lock the phone; however, 55 percent of individuals do not use it, and for that reason their phones are susceptible to piracy [5]. An important point, especially for officials and individuals who working in important places, is for them to remove their phones names from remote access services by re-registring on the servers, Beach *et al.* [28].

Therefore, all these protective methods will help people to protect their smartphones from two aspects of the risks; firstly, from malicious applications such as a worm virus; and secondly, from targeted attacks, which target specific individuals or use smart phones to attack them [13].

Recommendation of some legal security applications for users: Encryption applications, which means all the communications between the user and the aim points will be encrypted is called 'end- to-end communications' and furthermore, it is highly useful especially, for communications in public places. This is illustrated in figure 6 below. This means there is no opportunity for 'the man in the middle' to intercept the information through hacking attacks [13]. In addition to anti-malware applications, lookout security is also vital such as Snap Secures, BullGaurd Security 10, IHound for iphone And Family Tracker, McAfee Wave, KasperSky, F-Secure**,** Norton Lite, Virus Barrier, **Dell Sonic Wall** and **Web root**. Consequently, all these security softwares have the same aim, but some of them with different functions to protect users' smartphones from all the risks and attacks, which are coverd in this paper. Therefore, users can install them via the Apple or Android store.

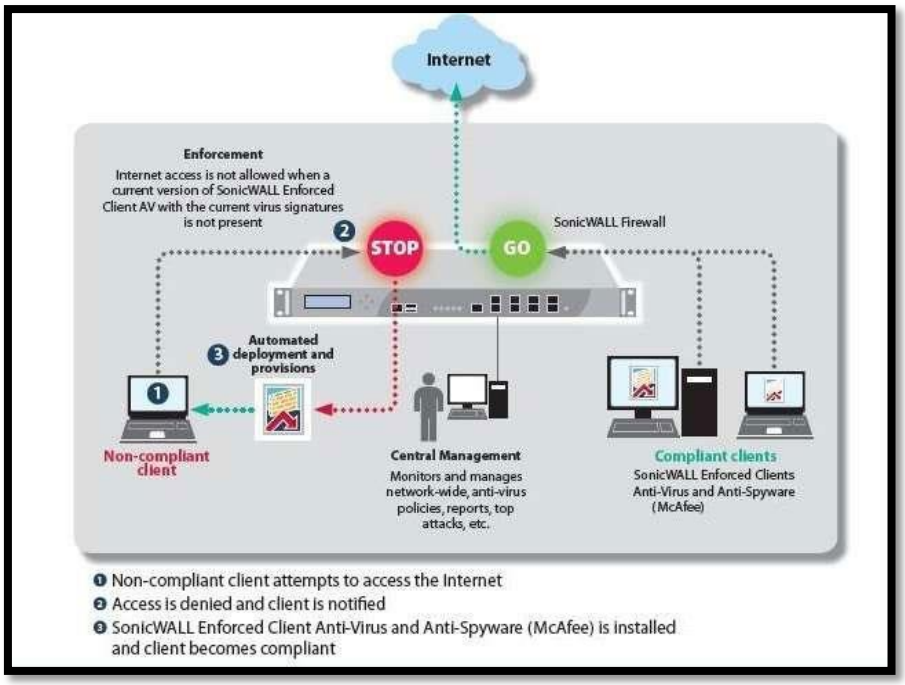

Fig-6 shows the automated enforced update of Dell Sonic Wall (for internet and smartphones), [29].

The recent study in 2014 showed that Apple and Google companies launched a new operating smartphone system, which prevents the return of all the removed data on users devices in order to protect the personal data [29].

In conclusion, the diffusion and adoption of smartphones, such as the Apple iphone and Samsung, continues worldwide, especially in this 'age of technology'. However, there are many security risks connected with this diffusion and also with the functionality enjoyed by these devices. For example, determining the user's location using GPS service, accessing sensitive information whether for consumers or at company level. Risk also includes the penetration of financial information, emails and spying on calls, as even the President of the United States, Barack Obama, pointed out.

Furthermore, all these risks happen firstly by attackers and hackers and secondly by malicious software, such as, IKee.B and FlexiSpy. Research has found that consumers most affected by these risks are those who do not have legal protection programs, or they have disabled the protection system to obtain free apps. Furthermore, there are companies that allow employees to implement corporate communications using their smartphones. Moreover, security vulnerabilities can also be found in operating systems such IOS 7, 8 for iPhone.

Subsequently, research has discovered the best legal security solutions. For example, companies need to be responsible and provide active security systems and legal technical protocols to protect the company's communications network, such as VOIP protocol. Also, they should not allow employees to do the company's work using their own devices. Also employers, should activate the phone's security properties, use legally protected platforms to install applications, do not follow announcements from an unknown source, and in addition continually update antivirus applications. Furthermore, employees should use the recent security applications, which run on different platforms such as Encryption, McAfee Wave, KasperSky and lookout security.

RECOMMONDATIONS:

There should be an establishment of specialized legal international organizations, for instance, 'The European Network and Information Security Agency' to increase security awareness among smartphone users through identifying the current and future risks, and then identifying security measures and procedures to address them. Also, users should not use the open platforms which provide free and unprotected software, such as Android platforms. In addition, users should not save sensitive information on mobile devices, especially the financial data. Finally, Smartphone companies must serioulsy tackle security vulnerabilities in operating systems and issuing protection software, to generate confidence in

smartphones use, especially in terms of access to digital information.

REFERENCES LIST:

1. Jeon, W., Kim, J., Lee, Y. And Won, D. 'A Practical Analysis of Smartphone Security': *Springer-Verlag Berlin Heidelberg*. 2011, 6771, pp. 311–320.
2. Barrera D, Van Oorschot P. Secure software installation on smartphones. IEEE Security & Privacy. 2011 May; 9(3):42-8.
3. Olver FW, editor. NIST handbook of mathematical functions hardback and CD-ROM. Cambridge University Press; 2010 May 17.
4. Perelson S, Botha R. An Investigation Into Access Control For Mobile Devices. Inissa 2004 Jun (pp. 1-10).
5. Siciliano R. The rise of smartphones and related security issues. Infosec Island. 2011 Apr 18;18.
6. Kakihara M. Grasping a Global View of Smartphone Diffusion: An Analysis from a Global Smartphone Study. Inicmb 2014 (p. 11).
7. Chin E, Felt AP, Sekar V, Wagner D. Measuring user confidence in smartphone security and privacy. Inproceedings of the eighth symposium on usable privacy and security 2012 Jul 11 (p. 1). ACM.
8. Kelly G. Report: 97% of mobile malware is on android. This is the easy way you stay safe. Forbes Tech. 2014 Mar.
9. Stutzman R. George Zimmerman arrest Sanford: Police gave mixed messages about George Zimmerman's arrest–Orlando Sentinel. Articles. Orlandosentinel. Com. Retrieved September. 2012;28.
10. Brinthaupt TM, Lipka RP, editors. Understanding early adolescent self and identity: Applications and interventions. Suny Press; 2012 Feb 1.
11. Rotenberg D, Vahidi A, Kolmanovsky I. Ultracapacitor assisted powertrains: Modeling, control, sizing, and the impact on fuel economy. IEEE Transactions on Control Systems Technology. 2011 May;19(3):576-89.
12. El Jundi B, Smolka J, Baird E, Byrne MJ, Dacke M. Diurnal dung beetles use the intensity gradient and the polarization pattern of the sky for orientation. Journal of Experimental Biology. 2014 Jul 1;217(13):2422-9.
13. Popović K, Hocenski Ž. Cloud computing security issues and challenges. Inmipro, 2010 proceedings of the 33rd international convention 2010 May 24 (pp. 344-349). IEEE.
14. Hall CB, Weinberg GA, Iwane MK, Blumkin AK, Edwards KM, Staat MA, Auinger P, Griffin MR, Poehling KA, Erdman D, Grijalva CG. The burden of respiratory syncytial virus infection in young children. New England Journal of Medicine. 2009 Feb 5;360(6):588-98.
15. Porras P, Saidi H, Yegneswaran V. An analysis of the ikee. B iphone botnet. Ininternational Conference on Security and Privacy in Mobile Information and Communication Systems 2010 May 27 (pp. 141-152). Springer, Berlin, Heidelberg.
16. Hymel JA, Lindner JE, inventors; Blackberry Limited, assignee. Methods and apparatus to audibly provide messages in a mobile device. United States patent US 8,655,661. 2014 Feb 18.
17. Bettinger JA, Scheifele DW, Halperin SA, Vaudry W, Findlow J, Borrow R, Medini D, Tsang R, the members of the Canadian F, Program IM. Diversity of Canadian meningococcal serogroup B isolates and estimated coverage by an investigational meningococcal serogroup B vaccine (4cmenb). Vaccine. 2013 Dec 17;32(1):124-30.
18. Sparkes AC, Smith B. Qualitative research methods in sport, exercise and health: From process to product. Routledge; 2013 Oct 15.
19. Tamura K, Stecher G, Peterson D, Filipski A, Kumar S. MEGA6: molecular evolutionary genetics analysis version 6.0. Molecular biology and evolution. 2013 Oct 16;30(12):2725-9.
20. Gonzalez D. Managing online risk: Apps, mobile, and social media security. Butterworth-Heinemann; 2014 Sep 25.
21. Villagarcia MR, Carter TE, Rufty TW, Niewoehner AS, Jennette MW, Arrellano C. Genotypic rankings for aluminum tolerance of soybean roots grown in hydroponics and sand culture. Crop Science. 2001 Sep 1; 41(5):1499-507.
22. Iranmanesh SA, Sengar H, Wang H. A Voice Spam Filter to Clean Subscribers' Mailbox. Ininternational Conference on Security and Privacy in Communication Systems 2012 Sep 3 (pp. 349-367). Springer, Berlin, Heidelberg.
23. Konc J, Janežič D. Probis-2012: web server and web services for detection of structurally similar binding sites in proteins. Nucleic acids research. 2012 May 16;40(W1):W214-21.
24. Bartle RA. Designing virtual worlds. New Riders; 2004.
25. ICO. 'Privacy in Mobile Apps Guidance for App Developers': *Information Commissioner's' Office*. 2013, 1, pp1-25.
26. Mylonas A, Gritzalis D, Tsoumas B, Apostolopoulos T. A qualitative metrics vector for the awareness of smartphone security users. Ininternational Conference on Trust, Privacy and Security in Digital Business 2013 Aug 28 (pp. 173-184). Springer, Berlin, Heidelberg.
27. Song J, Sörös G, Pece F, Fanello SR, Izadi S, Keskin C, Hilliges O. In-air gestures around

unmodified mobile devices. Inproceedings of the 27th annual ACM symposium on User interface software and technology 2014 Oct 5 (pp. 319-329). ACM.

28. Beach A, Gartrell M, Han R. Solutions to security and privacy issues in mobile social networking. Incomputational Science and Engineering, 2009. CSE'09. International Conference on 2009 Aug 29 (Vol. 4, pp. 1036-1042). IEEE.
29. Sonic WALL SRA 4600 Add 100 User-Firewalls.com. 01-SSC-7120. https://www.firewalls.com/products/firewalls/sonicwall/sonicwall-upgrades-software/sonicwall-sra-user-upgrade/dell-sonicwall-sra-4600-add-100-user.html