SCIREA Journal of Computer Science and Technology

http://www.scirea.org/journal/Computer

October 28, 2016

Volume 1, Issue1, October 2016

RECENT SECURITY ISSUES IN PERSONAL COMMUNICATION SYSTEM

QI ZHU

Department of Computer Science, University of Houston-Victoria

Abstract

Personal Communication System (PCS) designates a set of wireless communications capabilities that allows the combination of terminal mobility, personal mobility, and service profile management. PCS can provide users with an all-in-one wireless phone, paging, messaging, and data service through portable devices.

However, mobile services relaxed security has effectively made device users a target for hackers; mobile users have become increasingly concerned with security risks. The need for security has never been more detrimental than it is now. In this paper, we present a survey on emerging security issues of personal communication system, such as virus, worm, phishing and many others. In addition, some real recent examples are studied and finally some security rules are given to PCS users.

Keywords: Security, personal communication, virus, worm, phishing, malware

Introduction

Personal communication systems (PCS) have become a necessary part of human lifestyle. PCS is referred as several types of wireless voice and/or wireless data communications systems, typically incorporating digital technology, and providing services via Smartphones or personal digital assistants (PDAs) to give users mobile access to email, the internet, GPS navigation, and many other applications (Cheng, 2008). Furthermore, PCS can also be used to provide wireless-phone technology that combines a range of features and services surpassing those available in analog- and digital-cellar phone systems, including services which permit users to transmit and receive communications from a device within a WLAN and abroad.

However, Smartphone's popularity and relatively relaxed security has made them more attractive targets for attackers. Nowadays, people are using smartphones for an increasing number of activities and often store sensitive data, such as email, calendars, contact information, and passwords on the devices. The PCS/mobile infrastructure requires many antenna towers within a coverage area that essentially give users the ability to change positions or move around the grid as a signal is transmitted to each node according to the antenna or cell tower within the vicinity (Foote & Ruggiero, 2015). The mentioned issues with PCS could have various security infractions resulting in identity theft, denial of service, and even social engineering to name a few. Although many of the referred to encumbrances are also prevalent in Ethernet networks, similar issues are also present within the PCS spectrum. Meanwhile, PCS applications for social networking keep personal information in jeopardy. Recent technology innovations in m-commerce have allowed users to run many things directly from their smartphones, such as purchasing goods, buying tickets, buying/selling stocks, banking, redeeming coupons, processing point-of-sale (POS) payments, and even paying at cash registers. The traditional security techniques such as firewalls, antivirus, and encryption, are uncommon on mobile phones, and also mobile phone operating systems are not updated as frequently as those on personal computer (NIST, 2013). Unfortunately, many Smartphone users do not recognize the security shortcomings of PCS, they fail to enable the security software that comes with their phones, and most of them believe that surfing the internet on PCS is as safe as or even safer than on their personal computers (Fischer, et. al., 2012).

PCS Wireless System Design

There are three types of architectures of PCS wireless system structures: Distributed, Heterogeneous and Intelligent. PCS offers transmission mediums such as Bluetooth, Wi-Fi, text messaging and more. Social media has taken PCS/mobile development by storm considering that users can now communicate through various architectures. Figure 1 shows the various devices, objects, and entities employed by PCS and mobile system (Kang, et al, 2013).

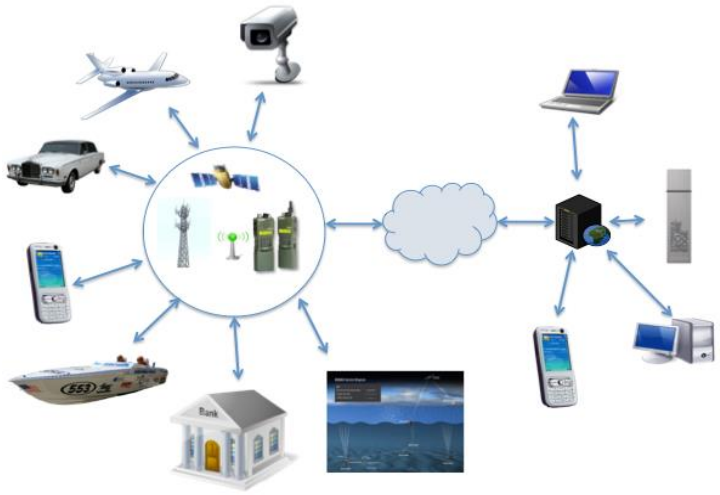

Figure 1. PCS and mobile system with the various devices, objects and entities.

Distributed network architecture is used to support the use of PCS with distributed antennas, distributed processors, and distributed control (Zhou, et. al. 2003). The PCS system capacity can be expanded through dense frequency reuse with distributed antennas, and the transmission power can be decreased as well. In addition, the different standards can coexist because of distributed processors control. Finally, IEEE 802.6 or Metropolitan Area Networks (MAN) can be deployed to assist with higher user demand technology, and supports voice and data transmission across the architecture. Heterogeneous PCS (HPCS) is a network that connects computers with alternate types of operating systems (OS) and protocols used in wireless networks. HPCS implements access technologies that are used to allow wireless networks to switch and integrate with cellular networks. Intelligent network is telecommunication system that promotes an open architecture and flexibility in improving networks using economic measures. Integrating various telecommunication methods is advantageous in creating mobile environments

(Cheng, et al, 2008). Though complex, the communication services used to deploy the previously mentioned protocols can also be a concern.

PCS Security Risk

The impact of security incidents in PCS is increasing day by day due to the complexity, growing reliance on software with known vulnerabilities, higher user expectations and expanding and changing systems. The complicated system environment increases the change of the number of potential entry points to a network. The large number of interconnected networks, computers, web sites, routers, switches, and gateways increase the probability of security breaches and other security attacks (Singh & Asthana, 2012).

The exchange of personal information is the central focus here, and users are to determine protocols that promote security against potential issues that could result in extensive consequences such as identity theft, social engineering and spoofing. Using PCS services come with a price if users are not aware of the impending intrusions that are waiting to breach devices over the network. Some hackers are skilled enough to attack a user's mobile phone services with malicious code and provide the hacker access to the user's services. This type of attack often leaves the primary user responsible for any incurred charges that may result. The clever tactics of hackers have even resorted to using text messages to entice unsuspecting users to bite; with this tactic, social engineering is demonstrated to deceive the user into providing personal data (Cheng, et al, 2008).

Another security issue is the use of location service applications that require users to give the target device permission to determine the user's location position using a global positioning system (GPS). Location services are often used to provide information to developers in relation to the primary user's location patterns for statistical purposes. What goes unnoticed about location services is as primary users agree to have GPS tracking enabled; other users have the potential to locate the target user as well. There are variations to security measures but none a completely secure scheme that can be configured on a device or system (Wang, 2013). Therefore, users should be more involved with device security and implement a concise security plan if global spike in mobile device use.

Users should be cautious of selecting random links on mobile devices when browsing the web or checking email messages that look suspicious. The downloading of software is also problematic if applications are sourced from sites that the user is unfamiliar with. Many times a new device is already equipped with basic security features that can be downloaded from the developer; these options should be explored as the device may be susceptible to breaches soon after purchase. As previously mentioned, a real danger is the unauthorized access of personal data and the ability to transfer and display that information as manipulated or compromised. Within a PCS environment, the perception of security without applying security principles is as dangerous as having no security at all. As hackers manipulate information and coerce users into unlocking personal data, the potential encumbrances that are taken place is the violating of confidentiality, authenticity, integrity and availability (mentioned later) (Cheng, et al, 2008).

The following trends suggest that mobile devices have a greater impact on information technology in changing the way business is implemented (Wang, 2013):

- Personal devices will become the norm in enterprise computing
- Seamless, on-demand mobile "virtualization" will overtake MDM
- HTML5 enterprise apps will proliferate, fueled by better connectivity
- Identity-based mobile services will put privacy in the spotlight.

PCS Security Issues

Smartphones and other mobile devices have outsold PCs in more people's pockets, purses, and briefcases with advanced capabilities like miniature computers, however, attackers have been hit this popular market by using old techniques along with new ones. Virus, worm, phishing are some of them, next we will survey the different types of PCS attacks with some real cases.

Viruses, worms, Trojans, and bots are different types of malware, which is a code or software that is designed to destroy, interrupt, steal, or create some undesirable activities on data, computer system, or networks (Aycock, J., 2006). Malwares often perform some type of harmful activities such as using CPU time or memory space, corrupting data, stealing private information, modifying or deleting some certain documents, displaying political or humorous messages on the

screen, or even rendering the computer useless. Social engineering and security vulnerabilities are exploited by the malware writers to gain access to the computers' resources. Currently malwares cause billions of dollars' worth of damage each year because of system failures, corrupting data, and maintenance costs (Skoudis, E,. 2004).

Some of the commonly known types of malware are viruses, worms, Trojans, bots, back doors, spywares, and adwares.

Virus

A virus is one type of malware, which is normally a piece of programming code installed itself without user consent. Almost all viruses are associated with an executable file, and they are only active when the host files are run or opened by the users. And it can be spread from one computer to another via the network, disks, or email attachments. Usually the host file keeps its original function even it is infected by the viruses; however, some viruses can destroy the associated files too.

The "Melissa" virus, also known as "Mailissa", "Kwyjibo", or "Kwejeebo", is the first successful email-aware virus. The virus is written by David Smith who later was sentenced to jail for 10 years since of causing over $80 million worth of damage. When opened, the virus resent to the first 50 people in each of user's address books, in addition, Melissa can disable the mail servers as the ripple of email distribution for a larger wave, and around 20% computers are infected (Crunkish 2015).

The first known mobile virus "Timofonica" was identified in Spain in 2000, "Timofonica" sent SMS messages to GSM mobile phones randomly with some fooling message (Hillebrand, M., 2000). After that, mobile phone viruses are widespread. One example is called "Doomed", which is like a regular application. However, it stops the normal applications from working, prevents the phone from restarting properly, and also introduces all other viruses like Skulls, CardTrap, CommWarrier, etc.

Worms

Like viruses, computer worms can replicate themselves and cause the similar type of damages. However, worms can be active alone and do not require attaching on a host program like viruses. Furthermore, worms can propagate through vulnerability in the system or trick users to executing them. Mobile worms always cause some harm to the network, such as consuming bandwidth, whereas viruses always corrupt or change the targeted mobile computer system (Moskovitch 2008).

One of the famous worms is ILOVEYOU, which spread itself by email in 2000 via an attachment in the message, once the attachment is opened; it loaded itself to the memory to infect all executable files. Also the virus sent itself to others by looking up the addresses in the Microsoft Outlook contact list. The virus spread throughout the world in a day, causing billions of dollars in damages. Commwarrior was the first worm to use MMS messages to contaminate mobile devices, which searches a user's address book for phone numbers and sends the infected files to other devices using a random name. The first Bluetooth-based worm is Cabir to propagate through Bluetooth connections and Ikee is the first known worm for iOS platforms (Peng, 2014).

Trojan Horses

Unlike viruses and worms, a Trojan Horse is a non-self replicating or non-reproduce malware named after the ancient Greeks wooden horse used to break into Troy. Trojan Horses only spread through user actions such as opening an email attachment or downloading and executing a file from the Internet. Once activated in mobile devices, Trojan horses can demolish mobile phone systems, attack the mobile devices remotely, corrupt or deactivate files, spy on users' inputs, steal passwords or other personal information, and broadcast to a third party server.

Like in a Hollywood movie, in Aug. 2010, the Zeus Trojan siphoned off over $70 million from large multinational corporations and banks such as Amazon, Oracle, BOA, Cisco etc in the Us and Europe, and infected more than 1 million computers through a drive-by downloads or phishing scams. People who visited a compromised site would unknowingly get the Zeus Trojan as a cookie, hidden as part of a legitimate ad on any website, which can steal the login credentials

of social network, email, and banking accounts. In late 2010, more than 100 people were arrested in connection of the Zeus Trojan operations (Alazab, 2012, Kalige, 2012).

Gingermaster is a trojan malware developed for the Android phone platform to incorporate a hidden malware for installation while installing other applications. It then steals information including phone number, user ID, IMEI, IMSI, SIM card number and native time. Some other notable Trojans for smartphone systems are DroidDream, GGTracker, Fakneflic, and Nickispy (Seo, 2012).

Bots and Botnets

Derived from the word "robot", a bot is a type of malware that allows hackers to take control over an affected computer and turn it into a "zombie" via the internet. Bots are usually part of a network of many infected machines "botnet" to spread viruses, generate spam, and commit other types of online crimes and frauds. Not only a bot can self-propagate like a worm, but also it can gather passwords, log keystrokes, capture and analyze packets, collect financial information, relay spam, and open back doors on the infected zombies.

Also known as Downup, Conficker appeared in 2008 to infect more than 9 millions computers all around the world from governments, business and individuals. It was one of the largest known botnet causing an estimate damage of $9 billion (Shin 2010). Another famous botnet is Ramnit, which affected around 3.2 million Windows users since of 2011. Ramnit provides attackers to monitor infected machine's web browsing sessions and steal banking credentials, also it grants the attackers remote access to exfiltrate stolen information or download additional malware (Martins, 2015).

From a report by IBM X-Force, GanjaMan (GM) bot is mobile malware that deployments on top of running banking applications to steal users' access credentials from a fake window. The source code of GM bot is leaked in 2015 and has been propagated by cybercriminals with some alternative such as Bilal Bot, Cron Bot and KNL Bot. It definitely plays a big role in the realm of mobile threats (Kessem, 2016).

Backdoor or Trapdoor

A back door is a method to access a computer that bypasses security mechanisms. Backdoors are often used for obtaining access to plaintext in cryptographic by attackers. Sometimes a worm is designed to take advantage of a back door to attack, one example is Nimda gained entrance through a back door left by Code Red. Another example is Mydoom, which installed a backdoor on the affected computer so that spammers can send junk email from those machines (Bank, 2004).

Most mobile phones have a universal back door to listen through their microphones, which has been used to turn them malevolent. In 2014, a backdoor was found in Samsung Galaxy products to provide remote access to the data on the device, so the attackers could issue remote file server command and access the file system on the phone's storage (wiki, 2014). Google has a back door called GTalkService to remotely install or delete applications. the US National Security Agency (NSA) can get data from smart phones, including iPhones, Android, and BlackBerry (Egners, 2012).

Spywares/Adware

Spywares are programs that installed in someone's computer or cellphone to secretly collect information without their consent. The main task of spyware is to track users' activities on the internet. Adware is usually considered as one type of spywares as well since it not only serves advertising, but also includes components for tracking and reporting user's information. As a result, both spywares and adware are identified as unwanted programs. Spyware can monitor a user's computing, collect personal information such as user logins, bank or credit account information, and change computer settings that result in slow internet speed or degrade the system performance.

First appeared in 2003, CoolWebSearch is a set of programs to change the user's web browser homepage to coolwebsearch.com, rewrite search engine results, and create pop-up ads to redirect to other websites including pornography sites (Keizer, G., 2005). 180search Assistant is an adware that displays pop-up advertisement to the user's computer. Whenever a user entered a key

word into a search engine, 180search Assistant opens a separate browser window to show an advertiser's web page that is related to the keyword (Luo, 2008).

For Android phone system, it is estimated at least 10 million phones were infected by HummingBad, one of the most pernicious pieces of malware. HummingBad will trick users to click on web ads, and steals your back login information by monitoring your personal information. Also, the NSA have used mobile spyware Smurf Suite to access the data of tens of millions of citizens, notably brought to public attention by Edward Snowden in 2013 (Lyon, 2014).

PCS Network Principles and Security Rules

The need for security has never been more detrimental in the realm of PCS than it is now as countless users collect and analyze data on large scales, protection of confidential data goes beyond that of emails or hard copy documentation, but it extends to mobile communications as well. "One study found that, from 2009 to 2010, the number of new vulnerabilities in mobile operating systems jumped 42 percent. The number and sophistication of attacks on mobile phones is increasing, and countermeasures are slow to catch up" (Foote & Ruggiero, 2015).

Many security concerns are resolved with the use of end-to-end and link encryption methods. Some integrated varied network protocols are implemented to provide more secure architectures such as addressing schemes and updating integrity requirements with authentication protocols and digital signatures (Laurila, et. al. 2012).

PCS Principles

Many of the principles used in computer network technology are synonymous with mobile and PCS networks. Terms such as confidentiality, authenticity, integrity and availability are also holds true with PCS/mobile devices within mobile networks.

- **Confidentiality** ensures that the given data is transmitted between the owner and the targeted individual, not made available or disclosed to unauthorized individuals, entities, or any

3rd parties. Virtual private network (VPN) is one method that is currently used to provide a level of confidentiality through secured tunneling.

- **Authenticity** verifies that the PCS device is who it claims to be and has subscribed to the targeted services. In PCS system, usernames and passwords are inadequate for strong authentication. Many require a second factor such as a token, digital certificate, or other out-of-band method (Camenisch, 2015).

- **Integrity** refers to the accuracy and validity of stored data over its life cycle. In many cases the accuracy of that data is the core focus of the security solutions. Technology such as RAID and parity to provide error protection schemes on the backend and give the element of fault tolerance to supersede data redundancy and other errors that may occur during transmission of data.

- **Availability** is also a security issue because data or services are required to be accessible at all times from PCS devices within a network. High availability (HA) is escalating for ensuring that single point of failure is non-existent. For instance, instead of using one file server for a domain, an administrator may deploy several files servers with various priority settings. Also, load balancing ensures continuity of the network using hardware and software resources to optimize and ultimately maximize security, essentially activating failover features (Singh & Asthana, 2012).

Encryption

Encryption is always the most effective way to achieve data security. There are two popular encryption methods available for wireless technologies: Data Encryption Standard (DES) and Advanced Encryption Standard (AES). DES has a key length of 56 bits and was published to keep government data private; however, the standard has been decommissioned. AES is an algorithm that holds various key sizes ranging from 128 to 256 bits (Arora, 2012). None of security algorithms is sufficient for today's security requirements of wireless use. Some other encryption methods are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access II (WPA2); each poses varying effects when encountered by hackers. Out of the three, WEP is less desirable as a line of defense considering WEP is limited to only

128-bit encryption. On the other hand, WPA holds 256-bit encryption by adopting Temporal Key Integrity Protocol (TKIP) and WPA2 has the following improvements: the use of AES algorithms, Counter Cipher Mode with Block Chaining Message Authentication Code Protocol which supersedes the option of TKIP. The vulnerabilities of the afore-mentioned security algorithms cause that WEP has been easily cracked and is not recommended for wireless security, so the benefits of WEP pale in comparison to that of WPA (Ohmori, et al, 2000); for WPA the hacker must figure out the password key to access the network. Attaining the pass key for WPA can be time consuming but it is not an impossible task. Users are warned to be aware of the available options.

Anti-malware Software

Users can install anti-malware software to protect cell phones from threats. Today is a fast changing world where every day some malwares getting discovered, it is so hard to say a particular antimalware as the best. Companies like Kaspersky, Sophos, Avast, AVG, Symantec (Norton), and TrendMicro have long and established histories as some of the most trusted brands in this area. Also new applications like Lookout and TrustGo recently ranked as the top two antivirus programs on the Android platform based on protection and usability. Most of the applications will offer additional features including anti-theft protection, safer web browsing, device tracking, remote wiping for a small monthly fee.

Protecting Rules

In addition, there are several general principles that we recommend to ensure that a device is as secure as possible:

- Immediately upon purchasing and activating a device, if applicable, change the default administrative password, considering that anyone can access this password.
- Use MAC filtering and authentication to access the network for users' mobile device.
- Encrypt data whenever possible using the afore-mentioned encryption methods.

- Always choose to disable SSID broadcasting to avoid hackers from viewing this critical information.
- Finally, use firewalls if applicable and virus software to detect spyware and other damaging viruses.

Conclusion

Personal communication and mobile services (PCS) are great improvements to the way consumers communicate in comparison to primitive technologies such as the telephone system; however, those improvements bring security issues that compromise personal information when every user is connected to wireless networks. Users need to be more informed of the potential dangers imposed by hackers on a daily basis. The mobile industry is constantly susceptible to intrusions as users are moving towards using devices for purchases, banking, storing financial data and enabling location services, further imposing greater risks. This can be a dangerous trend, when having extensive pertinent information centralized to a single or even multiple devices. In conclusion, protecting data will become more detrimental as mobile devices are hard-pressed to be a dominant method of accessing and transmitting data while on the go.

References

[1] Alazab, M., Venkatraman, S. Watters, P. and Alazab, A. (2012) Cybercrime: The Case of Obfuscated Malware. *International Conference in Global Security Safety and Sustainability*, pp. 204-211.

[2] Arora, M. (2012). How secure is AES against brute force attacks? Retrieved May 6, 2015 from http://www.eetimes.com/document.asp?doc_id=1279619

[3] Aycock, John (2006). Computer Viruses and Malware. Springer. p. 14. ISBN 978-0-387-30236-2.

[4] Bank, D. (2004). NEW VIRUS CAN TURN YOU INTO A SPAMMER; MYDOOM OPENS A'BACK DOOR'THAT HACKERS CAN ACCESS; SIGNING UP FOR SECURITY ALERTS. The Wall Street Journal, 1.

[5] Camenisch, J., Ortiz-Yepes, D. A., & Preiss, F. S. (2015). Strengthening Authentication with Privacy-Preserving Location Verification of Mobile Phones. *In Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, *ACM*, pp. 37-48.

[6] Cheng, H., Wang, X., Huang, M., & Yang, S. (2008). A review of personal communications services. In *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for* (pp. 616-621). IEEE.

[7] Crunkish (2015). Top Ten Most Destructive Computer Viruses of All Time. *Crunkish.com*. Retrieved 1 February 2015. Retrieved Jan 14, 2016 from http://crunkish.com/top-ten-worst-computer-viruses/

[8] Egners, A., Marschollek, B., & Meyer, U. (2012). Hackers in your pocket: a survey of smartphone security across platforms. RWTH Aachen University, Technical Report, AIB-2012-07, Aachen, DE.

[9] Fischer, I., Kuo, C., Huang, L., Frank, M. (2012). Short Paper: Smartphones: Not Smart Enough? *Proc. 2nd ACM CCS Workshop on Security and Privacy in Mobile Devices.*

[10] Foote, J & Ruggiero, P. (2015). Cyber Threats to Mobile Phones. Retrieved May 1, 2016 from https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

[11] Hillebrand, M. (2000). Mobile Phones Swapped by E-Mail Virus. In ecommercetimes.com. June 2000. http://www.ecommercetimes.com/story/3502.html

[12] Kalige, Eran, Darrell Burkey, and I. P. S. Director (2012). "A case study of eurograbber: How 36 million euros was stolen via malware." Versafe (White paper).

[13] Kang, et al, 2013. Anonymity, Privacy, and Security Online. Retrieved September 5, 2013 from http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

[14] Keizer, G. (2005). CoolWebSearch tops spyware threat list.

[15] Kessem, L, Karlinsky, A. (2016) Android Malware about to get worse: GM bot source code leaked, IBM Security Intelligence, Retrieved Aug 30, 2016 from https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/ .

[16] Klein, B., Miller, T., & Zilles, S. (2005). Security issues for pervasive personalized communication systems. In *Security in Pervasive Computing* (pp. 56-62). Springer Berlin Heidelberg.

[17] Luo, X., & Warkentin, M. (2008). Developments and Defenses of Malicious Code. Encyclopedia of Multimedia Technology and Networking, 3.

[18] Laurila, J. K., Gatica-Perez, D., Aad, I., Bornet, O., Do, T. M. T., Dousse, O., ... & Miettinen, M. (2012). The mobile data challenge: Big data for mobile computing research. In *Pervasive Computing* (No. EPFL-CONF-192489).

[19] Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. Big Data & Society, 1(2), 2053951714541861.

[20] Martins, Eduardo José Valadar, et al. (2015) "A hands-on approach on botnets for a learning purpose." Retrieved Aug 25, 2016 from https://web.fe.up.pt/~jmcruz/ssi/trabs-als/final/G6T12-Botnets-final.pdf

[21] Moskovitch R., Elovici Y., Rokach L. (2008), Detection of unknown computer worms based on behavioral classification of the host, *Computational Statistics and Data Analysis*, 52(9):4544–4566, DOI 10.1016/j.csda.2008.01.028.

[22] National Institute of Standards and Technology (NIST 2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise (SP 800-124 Revision 1). http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

[23] Peng, S., Wu, M., Wang, G. and Yu, S. (2014) Propagation model of smartphone worms based on semi-Markov process and social relationship graph. *Computers & Security*, pp. 92-103, no. 44.

[24] Ravi, S., Raghunathan, A., Potlapally, N., & Sankaradass, M. (2002, June). System design methodologies for a wireless security processing platform. In Proceedings of the 39th annual Design Automation Conference (pp. 777-782). ACM.

[25] Shin, Seungwon, and Guofei Gu. (2010) "Conficker and beyond: a large-scale empirical study." Proceedings of the 26th Annual Computer Security Applications Conference. ACM, pp. 151-160.

[26] Singh, R. K. & Asthana, A. (2012). Architecture of wireless network. *International Journal of Soft Computing and Engineering (IJSCE)*, *2*(1), 208-210.

[27] Skoudis, E., (2004). Infection mechanisms and targets. Malware: Fighting Malicious Code. Prentice Hall Professional. pp. 31–48. ISBN 978-0131014053.

[28] Seo, S. H., Yim, K., & You, I. (2012, August). Mobile malware threats and defenses for homeland security. In International Conference on Availability, Reliability, and Security (pp. 516-524). Springer Berlin Heidelberg.

[29] The Concept of Security. (2014). Retrieved April 30, 2015 from *http://www.mttgroup.ch/how_it_works/*

[30] Wang, C. (2013). *2013 Forrester Mobile Security Predictions. Retrieved May 4, 2015 from http://resources.idgenterprise.com/original/AST-0105400_2013_Forrester_Mobile_Sec.pdf*

[31] Wiki (2014) Samsung Galaxy Back-door on Replicant, *Retrieved Aug 25, 2016 from* http://redmine.replicant.us/projects/replicant/wiki/SamsungGalaxyBackdoor.

[32] Zhou, S., Zhao, M., Xu, X., et. al, (2003) Distributed Wireless Communication System: a New Architecture for Future Public Wireless Access, *IEEE Transactions on Communications*, 41(3), pp 108-113.