iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4164

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

A Comprehensive Study of Vulnerability Assessment Techniques of Existing Banking Apps

Dr. Kiran Prakash Joshi[1], Mr. Nilay R. Mistry[2], Dr. M S Dahiya[3]
[1, 2, 3,] *Cyber Defence Centre, Institute of Forensic Science, Gujarat Forensic Sciences University*

Abstract: ***Online banking solutions have existed for two decades already, and the industry now has a relatively good understanding of security threats and risks against traditional online banking. When dealing with security aspects for mobile banking in the context of mobile devices and applications, a few common themes emerge. If these themes are not addressed properly, through security controls and measures, the underlying threats could compromise the confidentiality, integrity and availability of mobile security assets. Mobile security assets that need protection are mobile devices, the mobile application and private information. Eight threats were identified in this research. These threats can be categorized in the following manner: users, devices, applications and data, and governance. Based on this categorization and testing with professional tool in the field of banking and IT security, the Mobile Banking Security Model was created which can be used to define security controls and measures, perform risk assessments for mobile banking in the context of mobile devices and mobile applications. This paper focus on mobile banking app and its network traffic monitoring for security audit. The network traffic monitor best matching specified criteria is chosen. A network traffic analysis method is implemented for the chosen network traffic monitor. The analysis method is used to show the differing behaviour of two distinct network traffic monitoring approaches (deep packet inspection and flow monitoring). Properties of the chosen network traffic monitor, along with performance measurements, are discussed.***

Keywords: Mobile, banking, security, device, application, audit

I. INTRODUCTION

The human civilization is undergoing one of the greatest transformation ever. The birth and the explosive boom of the internet has been the harbinger of one of the fastest and most impactful changes in the human history.[1] It has significantly accelerated the rate of changes seen in the society. Internet has enabled the transformation in many of the industries and sectors, and the birth of its own sector IT, which in turn has served many sectors. Almost all the sectors have benefitted from the boom of the internet. However, at the inception of the internet, its penetration and there by its benefits had been curtailed by the lack of the high-performance devices and high-speed networks. [2]

Over recent time however, the sectors having realized these bottle necks have put in significant investments and efforts and overcome these challenges. With the technological innovations of Telecom sector, high speed networks have become a reality. The speeds have increased exponentially through 2G/ 3G/ 4G and now upcoming 5G. At the same time the cost of usage has also come down significantly as well. Along with this the technological advancements have made the devices more powerful and capable.[3,4] The boom of the mobile devices and the innovations have made complex applications, software and innovative features to be able to run on the devices. The combined effect of both these innovations & technological advancements has made the internet much more accessible to everyone in the world. This has led to people and the businesses alike to be able to effectively use the internet's power.

Finances and financial transactions have been the life blood of the society. They have defined the transactions of humans, the development of societies, countries and businesses for a long time. Thus, it was one of the promises of internet earlier to be able to transact on the internet, a promise of 24*7 availability of the banking system rather than just in the banking hours in the banks. Internet banking thus was born.[5] However, it received much more traction and penetration with the increase in the capability of the Mobile devices. This helped in advent of the mobile banking. Through this the banks have got a new channel through which to serve the customers. Mobile banking has led to multiple fold increase in the transactions both by value and volume. It is gradually allowing the society to move towards cashless economy and may be even a card-less one in future.[6]

Mobile banking has created a new set of unique challenges. Most important among them is a dilemma. Banks are hard pressed to deliver new features both online and in mobile apps as fast as they can or risk losing business to the competitors. On the other hand, the security is of paramount importance as well. The security of the transactions is something which makes the people able to trust in the banks.[7] In absence of such security the trust of the people would crumble, and the said bank would lose the brand image and

the customer base as well. With the exponential increase in the features of the apps, the computing power of the devices and the speed of the networks, increasingly new challenges and threats to the security are attempted every day.

A. Rationale for Research

Mobile devices are providing a new field for the banking transactions to occur. Banking transactions have shifted the platforms on which they have been performed earlier too. From the traditional brick and mortar the transaction shifted to main frames with large data centres. With time the same evolved to client server model which necessitated the need to install the software on the PC to do the transactions. With the inception of internet banking, which facilitated transactions via web browser and secure sites.[8] This paved the way for the mobile platform to emerge. There are various multiple vendors, each with their own unique strengths and weaknesses. These unique capabilities of these platforms influence the perception of the mobile banking services offered and by extension their adaptation. For the mobile devices, their control, the applications that run on the device, and the data that the app operates on need to be controlled.[9] The confidentiality, integrity and availability of the data are very crucial. Blackberry devices managed to lead the market by providing the much-needed encryption features to offer the level of security. The biggest challenge however in offering the financial services via a customer owned mobile device, much of the control gets lost. Hence the need for this paper, to analyse and access this growing threat in the life blood of the economy, the banking system.

II. LITERATURE REVIEW

As discussed above the banking system has evolved exponentially a lot overtime. A few factors are responsible for the same. As shown in figure from RBI, the growth of mobile banking has increased in value and volumes. [10]

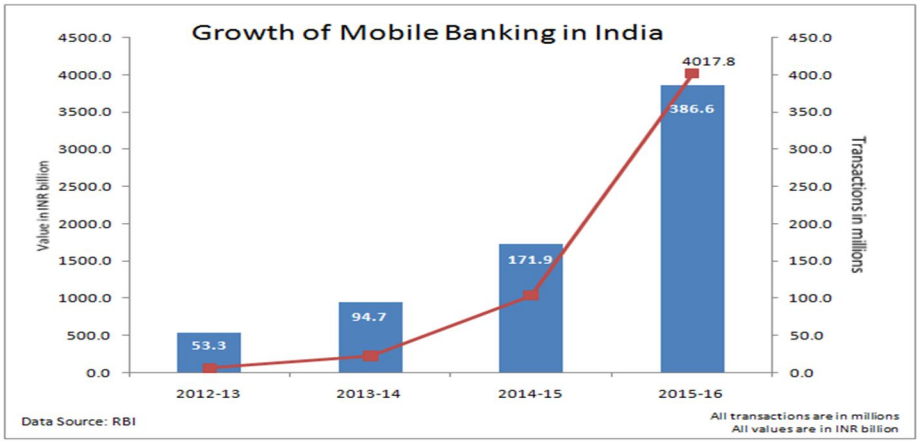


Fig.1 Growth of Mobile Banking in India

As seen in figure below, of all the channels of operation, mobile banking is dominating the entire segment. This is because mobile banking provides an unprecedented level of convenience and cost benefit to the banks and the customers alike. Hence it has become the most preferred channel.

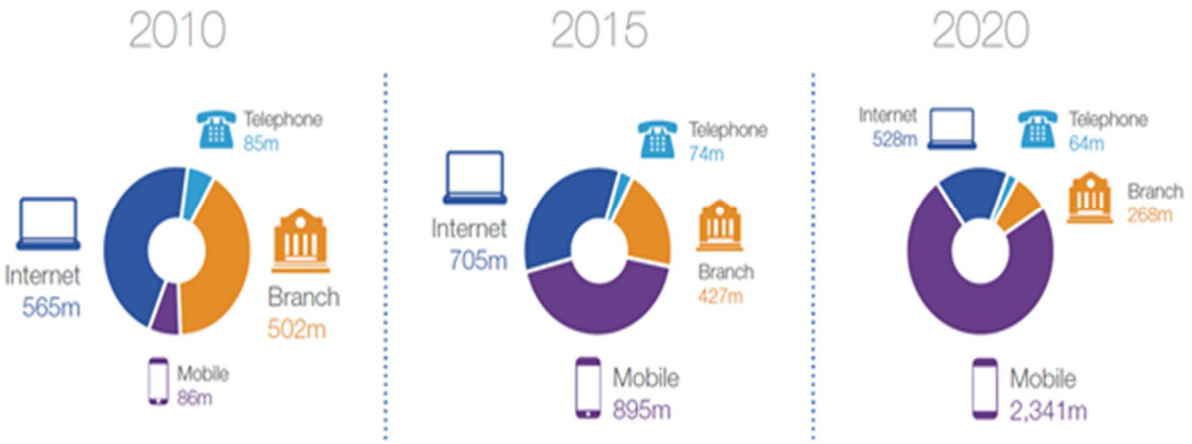


Fig 2. Mobile banking Provider

This has been made possible due to 3 major factors namely: increase in the speed of the mobile networks, increase in the capability of the mobile devices, consolidation of the mobile platforms/ OS into a few large players (Android, iOS & Windows).[11] Due to these three factors however, the flip side is that attacking/ hacking the apps and the transactions has become lucrative and possible. In any mobile device, the threat targets can be majorly classified into three categories, namely Confidentiality, Integrity and Availability.[12] The assets on a mobile device are the device itself, the apps present on the device and the information present on the device (internal or external memory) and the information that can be accessed from the device (cloud or on banking servers). All the assets should remain confidential, it should not be manipulated by unauthorized sources and the information should always be accessible when required. If the physical device is stolen, the permissions changed, the passwords etc cracked, then it could lead to breach in the security of the assets.[13] If the way the app functions, if any vulnerabilities are exploited by an unauthorized source then the integrity of the app and the transactions done can be breached causing manipulated data to flow through the system. At times the system can be locked out by unauthorized persons from the banking or the user side thus denying access to data or the service. As per the different papers studied, the threat sources can be majorly classified into four categories. Users, Devices, Applications & Data and Governance.[14] Users are of the primary stakeholders. However, in case of the mobile banking apps, much of the control is lost by the bank and the security does depend significantly on the users as well.[15] Lack of awareness of the users in various regards like setting a difficult password, not downloading apps from untrusted sources, not sharing the confidential information, not performing or attempting to perform malicious transactions, not attempting to bypass the security measures in place on the device or the app etc. When users do not use the facilities in intended way or are not aware, they can be misguided and thus they become a source of threat. The devices are a source of threat in a way that they need to be updated with the latest security patches and updates failing which they become vulnerable.[16] Devices running on old operating systems can also pose threats. Besides this, the physical theft of the devices, or by-passing the security measures (for e.g. by rooting) by the users or by other unauthorized persons can lead to security threats. The applications & data are stored either physically on the device or on the cloud or banking servers. The applications interact with other applications, have various modes of communication, interact with the servers and they operate on the information as well.[17] Hence any vulnerability if found in the app and exploited by unauthorized people can cause different error and security incidents. Thus, the apps need to be secure and the data access and operation to be highly protected from unintended changes. Governance regarding the status of the apps and phones, on the latest security threats and their resolution via patches can help solve many problems and avert a wide scale security breach. Hence Governance become important. Vulnerabilities are potential areas which can be exploited to cause a security incident.[18] Development level vulnerabilities are those which arise during the design of the banking apps. When developing a new feature, or an update to the app or features etc they need to be at the highest level of security. If there are any weak spots or loop holes in the designs, the same can be exploited to cause a security incident. Permission level vulnerabilities are those which arise due to apps having more permissions than required to perform intended functions. Like for example a banking app might require access to messaging to provide convenience to users to not having to enter the code received via messaging. But the same can be exploited to read other messages as well thus compromising on the private information of the user. Code level errors are those which arise in the coding of the app.[19] There can be intended or unintended loopholes/ backdoors in the code which can allow the same to be exploited thereby causing security incident. Network is a key component in the Mobile Apps. The information travels through the network. The apps should communicate to the correct sources on the network and the information which travels should neither be duplicated and captured by others nor be modified in the transit. Failing either of the above, the security of the apps or the data gets breached. The apps run on the devices. Device provides with the OS, and the hardware capabilities as well. There are precautions and the systems in place in the system. The device can be made vulnerable for e.g. by rooting there by giving the user and apps permissions not intended for them. Or the device can get outdated because of the lack updates due to various reasons. Since the apps and the data are present on the device and the devices are also the gateways for accessing the apps and the data, any vulnerability in the device can easily cause a security incident. There are various solutions which already exist in the current situation. The variety of the solutions target developer side of the problems to the user side of the problems. Secure development and secure networking protocols help add layers of security for the user. Regular audits of the existing apps and the transactions also help in adding layer of security. However, the audit need not be done by the banks or the developers. It can also be done by the users of their transactions as well. Users can actively participate in permissions management not allowing any of apps to have any unrequired permissions. Thus, the user can add a layer of protection. User can take responsibility of becoming aware and safe guard themselves from potential security incidents.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Since these already exist, the scope of this research is limited to using the tools available to test the existing banking and payment apps and attempt to identify the vulnerabilities in them.

III. METHODOLOGY

There are various methods which can be used to analyse the existing applications. There are majorly two widely accepted ways of testing them i.e. static analysis and dynamic analysis. For the static analysis the Quixxi Open Source tool was used. The methodology for the same is illustrated below

A. Open the chrome browser for open the quixxi tool which is open source for static analysis
B. Upload the APK (SBI, PNB, ICICI, DENA, PayTm, BHIM, Tezz, PAI) file for the analysis.
C. Put the email address for the vulnerability report.
D. Start the analysis and the generated report will be sent to the email id.

Once the reports are received the same would be analysed and conclusions drawn from the same. For the dynamic analysis, the packets need to be captured. The packet capture requires the stream to be duplicated and then analysed. A variety of tools can help achieve the same. The tools used in this research are t shark and wireshark.

E. The Methodology for The Same Are As Below
1) Generate a hotspot from laptop by mhotspot connect the mobile.
2) Start tshark or wireshark packet capture
3) Start transaction from the payment apps
4) Stop the packet capture
5) Generate the report
6) Analyse the reports at a professional network minor
7) Results of the pcap reports by wireshark or t shark can be don
8) Windows operating system information by network minor can be seen
9) System service information from service provider and mac address of the laptop can be seen
10) MAC address of the mobile and the OS version can be seen
11) Service provider IP, Service addresses and host details
12) Browser history files, DNS, Sessions and Parameters can be seen.

IV. OUTCOME

Using the methods above, below vulnerabilities were found in the banking and payment apps.

A. Using activities/ Improper export of Andriod application activities
B. SSL Implementation Check SSL Certificate Verification
C. Certificate Pinning
D. File Unsafe Delete Check
E. WebView add lava script interface Remote code execution
F. SQLite Journal Information Disclosure Vulnerability
G. Usage of Root
H. Outputting logs to logcat
I. Usage of Adb backup
J. Usage of installer verification code
K. Emulator Detection check
L. Unencrypted credentials in Databases (squlite db) Vulnerability Check

Following table is mentioning research outcome in terms of components related security threats and what kind of security assets compromised with that assets in terms of CIA (Confidentiality, Integrity and Availability).

Components	Security Threats	Security Assets Compromised
User	Lack of User Awareness	Confidentiality of Private Information
	Loss Theft or Improper disposal of devices	Confidentiality of Private Information
		Availability of Device, Application and Private Information
Devices	Malware	Confidentiality, Integrity and Availability of the device and in turn the application and private information
	Eavesdropping	Confidentiality and integrity of the Private information
	Unauthorized Access	Confidentiality of Private Information
	Device Malfunction	Confidentiality, Integrity and Availability of the device and in turn the application and private information
	Platform Alteration	Confidentiality, Integrity and Availability of the device and in turn the application and private information
	Denial of Service	Availability of the device and in turn the application and private information
Applications & Data	Unauthorized Access	Confidentiality of Private Information
	Application Malfunction	Confidentiality, Integrity and Availability of the device and in turn the application and private information
Governance	Risk on Management of the above threats if not adequately addressed by the organization	Confidentiality, Integrity and Availability of the device and in turn the application and private information

V. CONCLUSION

Today the world is shifting upon electronic economy. There is no full proof cyber secure technology; there are various issues at application level, network level, development level, etc. Electronic Transactions are vulnerable to attacks. User's use electronic banking via two medium first web application-based banking i.e. e-Banking and Mobile phone app-based banking i.e. m-Banking. Our prima facia focus is on mobile based applications. Mobile based applications have various vulnerabilities at different level,

A. Development level
B. Permission Level
C. Code Level
D. Network Level
E. Device Level

In this research all parameters were checked with defined methodology. For identification of Mobile banking app vulnerabilities SBI, ICICI, PNB, Bhim, Tezz, Dena Bank, Paytm, PhonePe etc. android apps was taken into the consideration. As a result, following parameter wise vulnerability identified. From the above results we can concluded that, the vulnerabilities can be minimized if secure code development methods can be applied. Secondly, regular security audit of such applications can minimize the risk of vulnerability exploitation. While defining permissions from the devices or users the minimum required permissions can be used and aware users to disable unnecessary permissions like microphone, location, phone call etc. The research work also suggests that secure network protocols like HSTS can also be implemented at the App level. To provide more security to the mobile apps the device level security is also required, like if the wireless connectivity is not required turn off the options immediately, if the location services not required disable the GPS option in the device etc. Overall from the above extensive research conclusion can be drawn that if users want to minimize the risk of being compromise, two things required, first is secure code development and risk assessment on periodical basis and second is user awareness to usage of such m-Banking app with proper security guidelines published by banks and financial institutions.

VI. FUTURE WORK

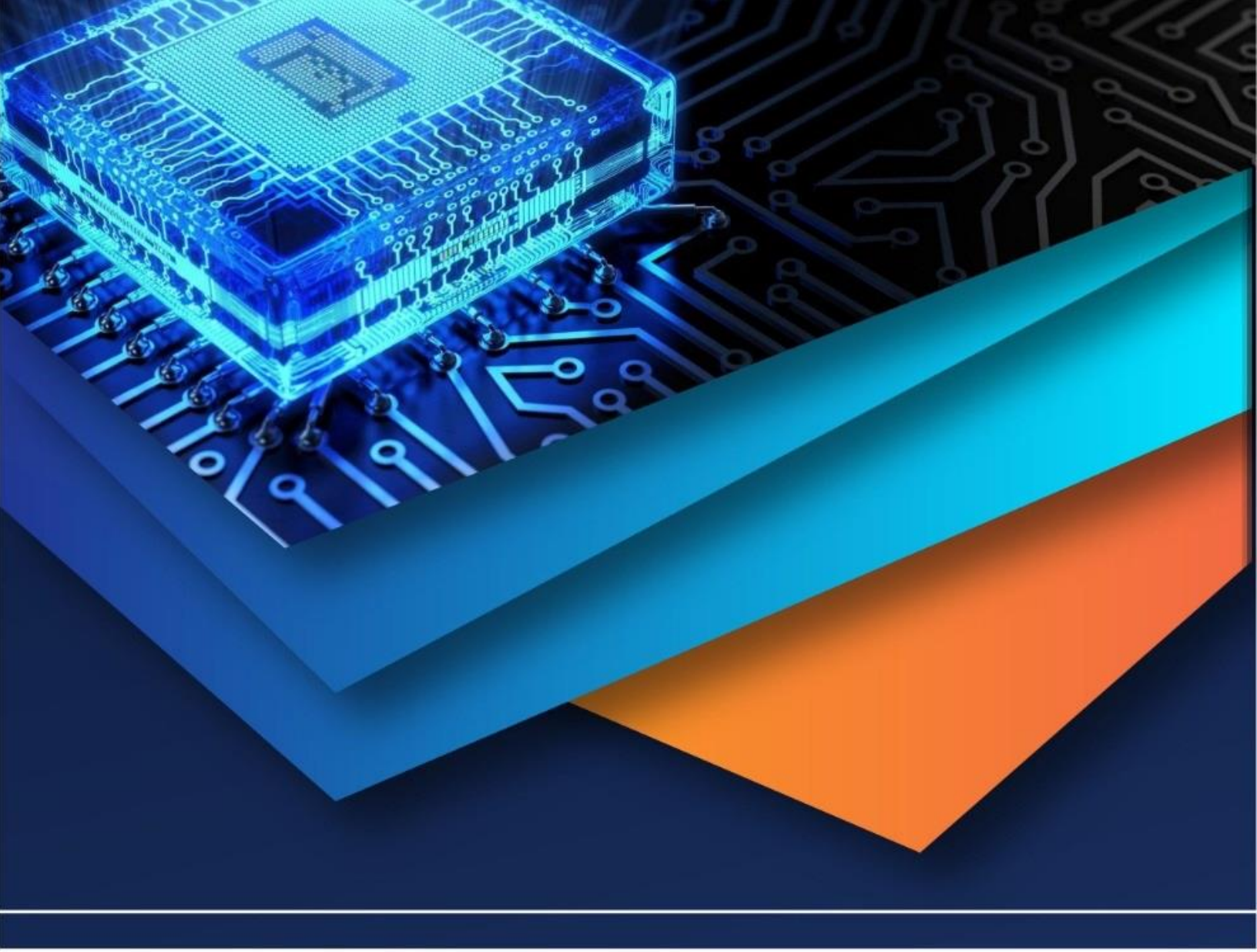
We can make our applications more secured by applying some tips

A. Secure the Apps code from the ground up with encryption
B. Secure the network connection from the back end

C. Put identification authentication and authorization measures in place
D. Be mindful of how the customer data is secured and implement and good mobile encryption policy
E. Have a solid API security strategy in place
F. Test your apps software repeatedly
G. User: Protect your device
H. Bring your own device policies and implementation of VPN
I. Utilise behaviour analysis of a real time text and email alerts.
J. Encourage the usage of NFC embedded Sim cards
K. Add multifactor authentication feature

REFERENCES

[1] Agarwal, S., Khapra, M. & Menezes, B., 2007. Security Issues in Mobile Payment Systems. Security, pp.142-152. Available at: http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/Security-Issues-in-Mobile-Payment-Systems.pdf .
[2] Android Developers Blog, 2009. Android Market update: support for priced applications. Available at: http://android-developers.blogspot.com/2009/02/android-market-update-support-for.html.
[3] Ante, S.E., 2010. Banks Rush to Fix Security Flaws in Wireless Apps. The Wall Street Journal. Available at: http://online.wsj.com/article/SB10001424052748703805704575594581203248658.html#printMode
[4] Apple Inc., 2008. App Store Downloads Top 100 Million Worldwide. Apple Press Info. Available at: http://www.apple.com/pr/library/2008/09/09App-Store-Downloads-Top-100-Million-Worldwide.html
[5] Aviv, A.J. et al., 2010. Smudge Attacks on Smartphone Touch Screens. In WOOT'10 Proceedings of the 4th USENIX conference on Offensive technologies. USENIX Association Berkeley, CA, USA, p. 10.
[6] Bahr, A., 2011. Mobile Apps Auditing & Forensics. Lancelote Institute.
[7] Bangdao, C. et al., 2010. The Missing Link: Human Interactive Security Protocols in Mobile Payment. In Proceedings of the 5th International Workshop on Security. pp. 94-109.
[8] Barati, S. & Mohammadi, S., 2009. An Efficient Model to Improve Customer Acceptance of Mobile Banking. In World Congress on Engineering and Computer Science. San Francisco, USA. Available at: http://b-dig.iie.org.mx/BibDig/P09-0829/content/pdf/WCECS2009_pp759-763.pdf.
[9] Davis, A., 2011. Securing consumer devices. Information Security Forum, (April).
[10] Esmaili, E. et al., 2011. The Role of Trust and Other Behavioral Intention Determinants on Intention toward Using Internet Banking. International Journal of Innovation, Management and Technology, 2(1), pp.95-100. Available at: http://www.ijimt.org/papers/111-E00102.pdf [Accessed January 3, 2012].
[11] GSM Association, 2011. Global Mobile Connections To Reach Six Billion Milestone, With Asia Pacific Accounting For Half, Reports GSMA. Mobile Asia Congress. Available at: http://www.gsmworld.com/newsroom/press-releases/2011/6570.htm.
[12] Hu, X., Li, W. & Hu, Q., 2008. Are Mobile Payment and Banking the Killer Apps for Mobile Commerce? In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS2008). IEEE, pp. 84-84.
[13] Cottrell, L.: Passive vs. Active Monitoring [online]. [cit. 2014-03-06], URL https://www.slac.stanford.edu/comp/net/wanmon/passive-vs-active.html
[14] Capture Setup /Ethernet - The Wireshark Wiki [online]. [cit. 2014-03-06] URL: http://wiki.wireshark.org/CaptureSetup/Ethernet
[15] Leong, P.: Ethernet 10/100/1000 Copper Taps, Passive or Active? [online]. [cit. 2014-03-06]. URL: http://www.lovemytool.com/blog/2007/10/copper-tap.html
[16] Matityahu, E.; Shaw, R.; Carpio, D.; aj.: Gigabits zero-delay tap and methods thereof. 2011 [cit. 2014-03-06], uS Patent App. 13/034,730. URL: http://www.google.com/patents/US20110211446
[17] Datacom Systems: Choosing a Network TAP [online]. [cit. 2014-03-06]. URL http://justnetworktaps.com/article_info.php?articles_id=3
[18] JDSU Storage Network Test: Understanding Fibre Optic Network Tapping [online]. [cit. 2014-03-06] URL: http://www.jdsu.com/ProductLiterature/Understanding-Fiber-Optic-Network-Tapping-white-paper30162800.pdf
[19] Balas, E.; Viecco, C.: Towards a third generation data capture architecture for honeynets. In Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC, June 2005 [cit. 2014-03-06], s. 21–28, doi:10.1109/IAW.2005.1495929.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY