Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.4, No.12, 2014
www.iiste.org

Proposed Framework for Securing Mobile Banking Applications from Man in the Middle Attacks

Anthony Luvanda
School of Computing and Information Technology,Jomo Kenyatta University of Agriculture and Technology,
PO Box 62000-00200 Nairobi Kenya
* E-mail of the corresponding author: luvanda@gmail.com

Abstract
Mobile phone banking and payments continues to not only be a popular way of transacting business but it also seems to evolve rapidly. Despite its popularity however there seem to be some very genuine concerns on the security issues revolving around it, particularly in regard to man in the middle attacks. This paper seeks to propose a secure framework for communication between a mobile device and the back end server for protecting mobile banking applications from man-in-the-middle attacks without introducing further threats to the communication channel.
Keywords: Defense- in-depth, Security, man in the middle attack, secure framework, bank server

1.0 Introduction

1.1 Man in the Middle Attacks on Mobile Banking Applications

A Man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other (Chellegati 2009)

The attack gets its name from the ball game where two people try to throw a ball directly to each other while one person in between them attempts to catch it. In a Man in the middle attack, the intruder uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it (Koutney, 2010).

Man in the middle attacks are sometimes known as fire brigade attacks. The term derives from the bucket brigade method of putting out a fire by handing buckets of water from one person to another between a water source and the fire. (Cheng 2010)

1.2 Risks Associated With Man In The Middle Attacks

Researchers have uncovered defects in a wide range of applications running on computers, smartphones, and Web servers that could make them susceptible to attacks exposing passwords, credit card numbers, and other sensitive data. (Kuoffong 2011)

The Trillion and AIM instant messaging apps and an Android app offered by some international banks are three apps identified as vulnerable to so-called Man-in-the-middle attacks. Like the other dozen or so applications identified, the threat stemmed from weak implementations of the secure sockets layer and transport layer security protocols. Together, the technologies are designed to guarantee the confidentiality and authenticity of communications between end users and servers connected over the Internet. (Beyah 2012)

The weak implementations caused the programs to initiate encrypted communications without first assessing the validity of the digital certificates on the other end. As a result, one of the fundamental guarantees of the SSL- that the computer on the other end of the connection belongs to the party claiming ownership was fundamentally compromised. Instead, the apps will trust imposter certificates that are signed by attackers or fail established validity tests for a variety of other reasons. (Peterson 2014)

"Our main conclusion is that SSL certificate validation is completely broken in many critical software applications and libraries," a team of researchers wrote in a paper titled “The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software”. When presented with self-signed and third-party certificates including a certificate issued by a legitimate authority to a domain called AllYourSSLAreBelongTo.us; they establish SSL connections and send their secrets to a Man in the middle attacker (Georgiev, Iyenga, Jana 2012)

The scenario described by the researchers is precisely the attack SSL is intended to protect against. The research demonstrated how holes in apps downloaded as many as 185 million times from Google's official Android market left passwords, emails and instant messages contents vulnerable to theft.

Instant messaging clients Trillian and AIM are among the apps that fail to properly validate SSL certificates before establishing a secure connection, according to the researchers. Man in the middle attacks on Trillian, depending on the specific setup, can yield login credentials for a variety of third-party services (including Google Talk, AIM, Yahoo!, and Windows Live services). The AIM client version 1.0.1.2 on

Windows also accepts certificates signed by untrusted parties and also fails to verify if the host name on the certificate conforms to the Internet address the app is connected to. (Salif 2012)

Similar weaknesses in the mobile banking app for Google's Android operating system also put users at risk, the researchers said. "Even a primitive network attacker—for example, someone in control of a malicious Wi-Fi access point—can exploit this vulnerability to harvest the login credentials of mobile banking customers," the paper warned.(Ornaghi 2014)

The researchers attributed weaknesses to the "terrible design" of the programming interfaces provided in widely used code libraries that implement SSL. In some cases, the libraries leave it up to individual apps to validate the certificates presented when they connect to a server. In other cases, options chosen by app developers inadvertently turn off validation routines that by default are supposed to run. In actual sense these Application Program Interfaces (APIs) are extremely confusing, they are very easy to get wrong and people do get them wrong all the time. (Ornaghi 2014)

The risks and prevalence associated with Man in the middle attacks cannot be taken for granted, as In October 19, 2012 the FBI warning on Android malware included the mobile version of spyware that was sold to law enforcement and governments, demonstrating how such commercial applications can pose a threat to private companies and consumers. The FBI's Internet Crime Complaint Center said during the time that FinFisher was among the latest malware brought to its attention, along with a Trojan called Loozfon. To infect phones, criminals were sending text messages with links leading to a malicious web site. (Beyah 2012). For some time now, FinFisher has been used in compromising personal computers. The commercial version was originally purchased understated by the cases bellow:

(a) by law enforcement agencies and governments as spyware in almost a dozen countries. This piece of software developed for law enforcement purposes has now turned out to pose a threat to Android phones. The Android version of FinFisher enables cybercriminals to take control of a device and monitor its use to steal personal information, such as user IDs and passwords to online banking sites. Loozfon steals contacts lists and the infected phone's number. Criminals use such information to create more convincing text messages to lure more people to malicious websites. Both malware take advantage of vulnerabilities within WebKit, an open source layout engine used in Apple Safari and Google Chrome browsers, Daniel Ford, chief security officer for mobile security firm Fixmo, said. In that respect, FinFisher and Loozfon are similar to other data-stealing Android malware.

(b)The malware risk on Android phones is a growing concern. A study released this in 2002 by Symantec found that 67% of large companies were worried about malware spreading from mobile devices to Internal networks. McAfee reported finding in the first three months of the year 2011 7,000 malware targeting the Android platform versus 1,000 for other mobile operating systems. By comparison, the total number of malware discovered in the middle of 2011 was in the hundreds, McAfee said. Part of the increase was due to improvements in detection. Despite the growing threat, wireless carriers and Android device makers continue to do a poor job at patching the software (Beyah 2012)

Hundreds of free apps in the Android market vulnerable to Man in the middle attacks as a result of unsound use of secure socket layer (SSL). In October 19, 2012—German university researchers have found hundreds of popular Android apps in the Google Play market that leave millions of users vulnerable to attackers looking to steal banking credentials, credit card numbers and other personal information.

The problem is in the way the tablet and smartphone apps implement the security protocol used in communicating with users' Web browsers, the researchers said. An analysis of thousands of free apps found nearly 8% vulnerable to Man in the middle attacks as a result of unsound use of secure socket layer (SSL).

In general, mobile apps use transport layer security (TLS), which includes the SSL protocol, for transmitting and receiving sensitive data while communicating with a Web server. The researchers claim that flaws in the implementation make it possible for an attacker to intercept and control the data traffic. During the analysis, researchers were able to intercept from the apps a variety of user information, such as credit card numbers, bank account information, PayPal credentials and social network credentials. The researchers, who worked in teams from the Leibniz University in Hanover and Philipps University of Hamburg, used a homegrown proof-of-concept tool called MalloDroid, which was designed to identify exploitable SSL bugs, Threatpost. The apps analyzed with the tool represented 17% of the apps that contain HTTPS URLs, which indicate that they use SSL. The researchers manually audited 100 apps and found 41 vulnerable to Man in the middle attacks because of SSL misuse. The cumulative install base of all the vulnerable apps ranged between 39.5 million and 185 million users, based on information the researchers gathered from Google Play."The actual number is likely to be larger, since alternative app markets for Android also contribute to the install base," the researchers said. From the 41 apps analyzed manually, the researchers were able to capture credentials for American Express, Diners Club, Paypal, bank accounts, Facebook, Twitter, Google, Yahoo, Microsoft Live ID,

Box, WordPress, remote control servers, arbitrary email accounts and IBM Same time. In addition, the researchers were able to disable anti-virus apps and remotely inject and execute code.

1.3 Methods and Techniques Used by Hackers in Perpetrating Man in the middle attacks

The most common Man in the middle attack that can be associated with mobile banking applications is the Zeus attack (also known as Zbot, Wsnpoem or Gorhax). This is more or less like a Trojan horse that steals banking information by keystroke logging and form grabbing. Zeus is spread mainly through downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the USA department of transport, it became more widespread in June 2009, (Buger 2010).

It was largely believed that The Zeus Botnet only targets Microsoft Windows machines, and computers running Windows Vista make up the majority of the Botnet, though newer versions also affect higher versions of windows. (Buger 2010) It was further believed that (and it's still the case now) every criminal can control whatever information he/she is interested in and fine tune his copy of Zeus to only steal those. Examples include login credentials for online social networks, e-mail accounts, online banking or other online financial services. The most disturbing aspect of Zeus is perhaps the fact that it is readily available to buy in underground forums for as little as 700 USD (if sold from a reseller) and up to 15,000 USD for the newest version with all available features. (Anderson 2009) The package contains a builder that can generate a bot executable, web server files (PHP, images, SQL templates) for use as the command and control server. While Zbot is a generic back door that allows full control by an unauthorized remote user, the primary function of Zbot is financial gain - stealing online credentials such as FTP, email, online banking, and other online passwords. The latest public version that is available is 2.0.8.9. (Buger, 2010).

Zeus is very difficult to detect even with up-to-date antivirus software. This is the primary reason why its malware family is considered the largest botnet on the internet.

Unfortunately for mobile banking application users, the Zeus banking Trojan has jumped the bridge to the large and growing ecosystem of mobile devices powered by Google's Android operating system. Security researchers at Fortinet say they have obtained a Zeus variant, dubbed "Zitmo," that can run on Android phones and that has the ability to intercept one time pass codes sent to mobile phones as an added, "two factor" security measure. (Anderson, 2009). The same researchers were responsible for discovering Earlier Zeus variants that run on Nokia Symbian, RIM Blackberry and Microsoft Windows Mobile devices.

ZitMo (Zeus-In-The-Mobile) ZitMo is not a MitB Trojan itself (although it performs a similar proxy function on the incoming SMSes), but is mobile malware suggested for installation on a mobile phone by a Zeus infected computer. By intercepting all incoming SMSes, it defeats SMS-based banking OOB two-factor authentication on Windows Mobile, Android, Symbian, BlackBerry. ZitMo may be detected by Antivirus running on the mobile device. It is also worth noting that SpitMo (SpyEye-In-The-Mobile, SPITMO), is similar to ZitMo.The new Android variants are just the latest evidence that malware authors are expanding their operations to mobile devices. Fortinet researcher Axelle Aprville, claims that Fortinet researchers have observed conversations relating to Zeus for Android, but were finally able to obtain and test a sample. The malware they obtained looks much like known Android malware variants. It masquerades as a banking security application. The malware is intended to thwart online banking security systems that rely on so-called out-of-band (OOB) authentication: sending pass codes to pre-registered cell phones that are required to start an online banking session (Aravamudhan, 2009).

2.0 securing communication in mobile banking against man in the middle attacks

2.1 Defense Startegies againts man in the middle attacks

There are a myriad of possible countermeasures that can be deployed to help control if not deter man in the middle attacks attacks and their implications in mobile banking and general secure communication (Claudio and Zhou 2011). Few of the defensive considerations may allow for a stronger security posture for multiple parts of the overall network infrastructure, while others will focus specifically on defenses against man in the middle attacks attacks.

2.2 Knowing the Threats

Knowing the threats and how the threats can be identified and mitigated will provide valuable information need to implement defensive controls. Whether the controls implemented are active controls to stop attacks in their tracks, or passive controls used to monitor for attacks, knowing t

he types of attacks used by attackers is one of the greatest things that can be done to prepare agains such attacks. The threat landscape as with the technogical world is dynamic and keeps changing, as such continued awareness of the threats and attack techniques will allow for preparation of defenses and stay vigilant in your defensive initiatives, including sucurity controls and protocols. (Claudio and Zhou 2011; Kim, 2013).

2.3 Defense-in-Depth Approach

Implementing defensive security controls at various layers within the network allows for more challenges an attacker will have to overcome to be successful at obtaining his or her objective. The primary layer for instance could include Intrusion Detection Systems (IDSes) and early detection which are vital to minimizing the impact of attacks, reducing potential losses.

The Secondary defensive measure woud be physial secrity measures such as a well-placed proxy or firewall devices. The goal of this line of defense is to slow attacks or at least to make it very challenging and tedious to perform them. Next layer of defence provide the last line of defence and are security measures such as such as malware and virus protection, host-based firewalls and IDS, patch management, and system auditing controls. (Peterson and Reiher, 2014).

These multi-layered implemention of some of these controls will reduce the overall likelihood of an attacker being successful in their exploits and minimize loss incase of succesful breach. Monitoring, evaluation and review of these security controls is important and since no single solution will provide all the security needs it is important to understand that secrity is a procces and not a product and each layer provides a part of the overall solution. (Claudio and Zhou 2011).

2.3.1 Public Key Infrastructure (PKI)

One possible solution to address man in the middle attacks involves deploying a Public Key Infrastructure (PKI) that implements mutual authentication. PKI manages the use of public key cryptography. In a PKI, there are several components that handle the issuance and revocation of certificates as well as attesting for the validity of certificates that are implemented. These are important components as it is the basis of ensuring we can trust encryption, signatures, and the implementation a given PKI is responsible for. (Claudio and Zhou 2011).

As it relates to SSL and HTTPS connections, the process verifies the validity of a certificate is as follows: when connecting to a server that is using a digitally signed SSL certificate, the server will send the certificate to the Web user's browser. Upon verification of the validity of the SSL certificate, the browser will connect to the server using the SSL protocol. A session key is created and used to protect the data that travels between the user's browser and the server. The session key is unique to the session and is used as a means of ensuring private communication between the user and the Web server. (Prowell, 2010).

It is important to note that, implementing a PKI by itself is not enough to prevent man in the middle attacks. If an attacker can capture key exchanges at the beginning of a session, he or she may still be able to perform man in the middle attacks, therefore implementing other controls that complement PKI implementations should be considered. Although PKI on its own is not a sufficient mitigating control against man in the middle attacks attacks, when it is coupled with mutual authentication, the solution is more appealing. Mutual authentication is the concept of requiring not just a client to authenticate to a server but also the server to authenticate to the client. With many client and server implementations, the initial trust is only confirmed by a one-way verification between the client and the server. With mutual authentication, the server verifies the client and the client verifies the server to ensure legitimate communications are being exchanged. Verification can be conducted by using public and private keys. Implementing mutual authentication and PKI together can increase the complexity of and significantly reduce the likelihood of successful man in the middle attacks attacks. (Kim, 2013; BITS, 2013).

2.3.2 Encrypted Protocols

Encrypted protocols should be implemented whenever possible to reduce the likelihood that credentials will be sniffed off the network by attackers. Some examples of clear-text protocols still heavily used in networks today include; FTP, TELNET, and HTTP. Most clear-text protocols today have an encrypted alternative that can provide an additional layer of security. Some of the popular alternatives for the previously mentioned protocols include Secure File Transfer Protocol (SFTP), Secure Shell (SSH), and HTTPs. It is important to keep in mind that encrypted protocols should be used for protecting communications for remote administration and for protecting sensitive data that is being transmitted for everyday applications.

Implementing encrypted protocols not only protects data while it is in transit but also can add an additional layer of complexity for attackers to deal with when trying to perform attacks such as an man in the middle attacks attack. As a basic security recommendation, encrypted protocols should always be used instead of clear-text protocols, not just because of the threat of MAN IN THE MIDDLE ATTACKS attacks, but for the protection of data while in transit in general, (Claudio and Zhou 2011).

2.3.3 Securing Server Interactions (Application Development)

Mobile banking entails securing data transmission off the device to other parties, notably servers that the client application interacts with. The risk analysis of the data being transfered over the network will dictate the level of protection needed. (Bahr,2011).

2.3.4 Confidentiality and Authentication

When data is being sent off the device to somewhere else, a security-minded developers must consider two primary considerations. The first is authentication. In this context, it refers to the capability of verifying that the

entity we are communicating with, either sending data to or receiving data from, is the entity that we think it is. This is important for many reasons: First, to ensure that the computer to which we are uploading data from the device is an entity that should have it, otherwise, we may be exposing confidential data to a party that should not have access to it, and also to download data only from a trusted source (Jeon et al, 2011).

An increasing number of internet-based end-customer applications require two-factor authentication. Text message (SMS) based one-time code distribution (as second factor) is rapidly becoming the most popular choice when strong authentication is needed, for example in e-banking. When implemented correctly, multi-factor authentication can make it significantly more difficult more difficult for man in the middle attacks (Kim, 2013).

The other consideration is the confidentiality of the data being transmitted over the network. This refers to steps that prevent a third-party from reading the data while it is being transmitted. For instance financial data sent from a bank server to an app running a device to be read by another party who happens to have access to a critical part of the cellular data network (Bahr, 2011; Jeon et al, 2011).

According to Dacosta (2012) the Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS), have become the de facto means of providing strong cryptographic protection for network traffic. While vulnerabilities are occasionally found in specific implementations, SSL/TLS are widely viewed as robust means of providing confidentiality, integrity and server authentication. The SSL/TLS protocols are the main security mechanisms used to protect the communications between browsers and web applications. By providing a transparent encryption layer, SSL/TLS guarantee the confidentiality and integrity of the data in transit. Moreover, SSL/TLS allow browsers to authenticate web application's servers via digital certificates. A digital certificate binds the server's identity (i.e., domain name) to the server's public key and it is signed by a Certification Authority (CA) trusted by both the server and the browser. Initially, due to performance considerations, most web applications used SSL/TLS only to protect requests carrying private data (e.g., passwords, credit card numbers). However, due to the increasing number of attacks against web sessions (e.g., session hijacking), many applications have been forced to protect all their communications with SSL/TLS (Prowell, 2010; Dacosta, 2012).

2.4 Conclusion

Judging by the evidence carried out in this research, it is quite apparent that a single defense strategy for protecting mobile phone based banking transactions is still far from being achieved.

This is mainly due to the complex nature of implementing the transactions but also due to the fact that there are a multiple number of parties involved and each of this parties have a role to play in ensuring that the transactions being engaged have the bare minimum of acceptable security controls.

This dissertation proposes a defense-in-depth strategy for implementing controls against man-in-the middle attacks on mobile phone based banking transactions.

A normative comparison of existing efforts for implementing controls against man in the middle attacks show that the proposes solution in this thesis addresses a major concern which revolves around an attempt to curb further threats from other sources within the communication channel.

As mentioned earlier in chapter three, the human interaction Protocol, the Site key and the WiKID strong authentication system all have flaws associated with them. The human interactive security protocol heavily relies on human intervention to implement controls against man in the middle attacks ; however it does not address other loopholes or techniques that can be exploited during such an attack. The site key approach on the other hand has an obvious flaw in the design since a phishing site can get the correct SiteKey info from the genuine site, then serve it to the user, "proving" its legitimacy SiteKey is thus susceptible to a Man-in-the-middle attack. (Kugler 2003). As far as the WiKID strong authentication protocol is concerned, it attempts to secure transmission on a LAN, MAN or WAN, however it does not adequately deal with the problem of man in the middle attacks on either such or within mobile applications.

Based on the normative comparison of the existing studies and the proposed frame work. It is quite clear that for a mobile application channel of communication to be secured from man in the middle attacks, then the defense in depth approach has to be taken. The proposed model arrived at in this thesis therefore differs from the earlier models due to the implementation of a defense in depth approach.

A defense in depth approach revolves around the notion that implementing defensive security controls at various layers within the network allows for more challenges an attacker will have to overcome to be successful at obtaining his or her objective. More importantly the controls need to complement each other for them to work effectively.

The defense mechanism for protecting mobile banking applications can be divided into three essential security layers, namely: The client; the communication channel and the server.

The client is represented by the mobile phone user who also happens to own the handset, the communication channel is owned by the TELCOs who happen to be the infrastructure service providers and the

server is represented by the banking/financial institutions. These layers can be further broken down into sub layers depending by their security needs as illustrated in the diagram bellow.

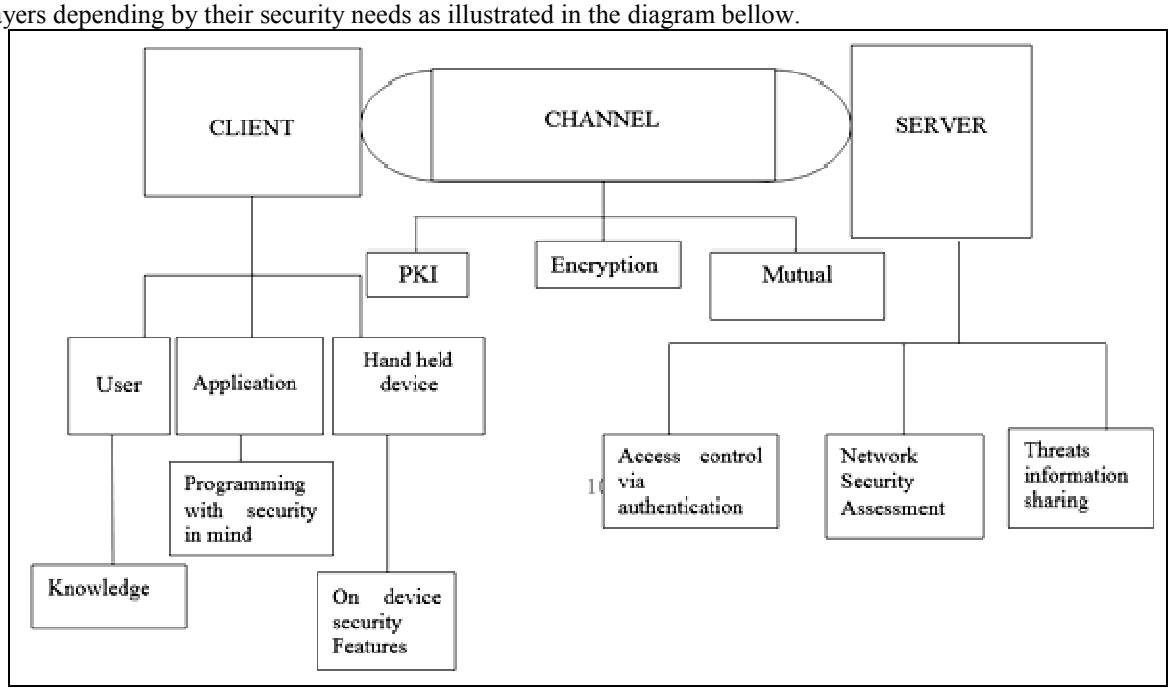

Figure 2.1: framework for securing mobile transactions from a man in the middle attack

The framework can be implemented at each level as illustrated in the table bellow

2.4.1 Client Level

Sub level	Strategy	Implementer
User Level	Provide Knowledge to users by creating awareness among users on the possibility of an attack being perpetrated during transactions.	Banking/ Financial Institutions
Application (mobile banking apps)	Apps should facilitate implementation of - Multi-Factor Authentication - Implementation of Transaction Limits - Code meant to implement security Code The code should also be regularly analyzed and reviewed	Venders/apps developers
Device	Phones supporting mobile banking should exhibit the following features; Power on passwords, Automatic locks, Mobile security software such as anti-virus and firewalls, data wiping features **NB** some smart phones have this features but some users may not have enabled them due to lack of awareness	

Table 2.1: Client level

2.4.2 Communication Channel Level

Strategy	Implementer
PKI and mutual authentication deployment through (PKI), through proper implementation of TLS and SSL, that implements mutual authentication	TELCO
Encryption: Data being transmitted over wireless medium should always be encrypted so as to add an extra layer of security	TELCOs, app Developers and banking institutions

Table 2.2 : Communication channel level

Due to the low level of technological awareness by the users of mobile banking services and the high level of risk that they are exposed to; securing mobile banking transactions will continue to generate greater research interest.

2.4.3 Server Level

Access control via authentication: This can be achieved through Multi-factor authentication, or customer authentication, which is a key control for verifying that the end user attempting to access the financial institution's mobile banking solution is the actual authorized consumer.

Network Security Assessment: These include (a) Security Policy (b) Network Management (c) Identification and Authentication (d) Resources Management (e) Account Management

Threats information sharing: All financial institutions implementing mobile banking need to set up a mechanism for sharing new information and threats in regards to mobile banking

At the moment there are no known standalone techniques for securing the aforementioned transactions. The existing ones either do not fully secure the transaction or simply introduce further threats to the transaction. This is probably the area where further research needs to be carried out.

REFERENCES

Abhijit S. Ercan P. (1998). ATM Technology for Broadband telecommunications Networks. CRC Press.

Adida, B. et al., (2006). *Phish and chips*. In Security Protocols Workshop.

Aissi S. and Dabbous N. (2007). *Security for Mobile Networks and Platforms*. Artech House. University of Michigan

Aravamudhan, L. et al., (2009). *Getting to Know Wireless Networks and Technology*, *InformIT.*

Asokan, V. Niemi, and K. Nyberg. (2005). *Man in the middle in tunneled authentication protocols.* In security protocols workshop.

Bahr, A., (2011*). Mobile Apps Auditing & Forensics*. Lancelote Institute. Lancelote.

Bardwell, J. and Akin, D. (2005). *CWNA Official Study Guide*, (Third ed.). McGraw-Hill. p. 435. ISBN 0072255382.

Beyah, Y. (2011). *Rogue access point detection_challenges, solutions, and future directions.* IEEE Security and Privacy Article, vol. 9(5), IEEE, pp. 56-61, 2011.

BITS, (2013). *Mobile Technology Layered Security Model*. BITS/The Financial Services Roundtable 1001 Pennsylvania Avenue NW, Suite 500 South.

Cheng, M. Gao, and R. Guo, (2010). Analysis and Research on HTTPS Hijacking Attacks," 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, IEEE, pp. 223-226, Apr. 2010.

Chomsiri, T. *(2007). HTTPS Hacking Protection.* 21st International Conference on Advanced Information Networking and Applications Workshops, IEEE, May.

Claudio A and Zhou A. (2011). *Information Security Theory and Practice: Security and Privacy of Mobile Devices in Wireless Communication*: 5th IFIP WG 11.2 International Workshop, WISTP 2011, Heraklion, Crete, Greece, June 1-3, 2011, Proceedings.

Cliffs, E. (2005). *Data Networks: Concept theory and practice***,** NJ: Prentice- hall, 2005.

DongPhil, K. chulbum, and K. Sangwook, (2004). *Rogue AP Protection System Based On Radius Authentication Server,* Korean Institute of Information Scientists and Engineers, vol. 31(1), April, 2004.

Frank Adelstein (2005) Fundamentals of mobile and pervasive computing. McGraw Hill.

George O. (2008). *Ultimate wireless security guide: A primer on Cisco EAP-FAST authentication*. *TechRepublic*. http://articles.techrepublic.com.com/5100-10878_11-6148557.html. Retrieved 2014-09-02.

Government Accountability Office -GAO, (2012). *Information Security Better Implementation of Controls for Mobile Devices Should Be Encouraged.* Report to Congressional Committees. United States Government Accountability Office.

Government Accountability Office -GAO*, Information Security Better Implementation of Controls for Mobile Devices Should Be Encouraged.* Report to Congressional Committees. United States Government Accountability Office. 2012. http://www.passmarksecurity.com/BofA.jsp

Harok, R. (2009). *Communication systems and networks.* Wiley publishing.

http://savannah.gatech.edu/people/lthames/dataStore/WormDocs/arppoison.pdf

Jeon, W., et al (2011). *A practical analysis of smartphone security*. Human Interface and the Management of Information, 6771, pp.311-320.

Jeon, W., et al (2011). *A practical analysis of smartphone security.* Human Interface and the Management of Information, 6771, pp.311-320. 2011.

Kevin Beaver, K. et al., (2009). *Hacking Wireless Networks For Dummies***.** Prentice hall.

Kim D. (2013). *Fundamentals of Information Systems Security*. Jones & Bartlett Publishers. Virginia, USA.

Kim, D. (2013). *Fundamentals of Information Systems Security*. Jones & Bartlett Publishers. Virginia, USA. 2013.

Koutny, T. (2010). *Detecting Unauthorized Modification of HTTP Communication with Steganography.* Fifth International Conference on Internet and Web Applications and Services, IEEE, pp. 26-31, May. 2010.

Kugler, D. (2003). M*an in the middle Attacks on Blue tooth.* In Proc. Financial Cryptography
kuofong, L .ien, and L. Yuehchia (2009). *Detecting rogue access points using client-side bottleneck bandwidth analysi.* Computers & Security, vol. 24(3-4), ELSEVIER, pp. 144-152, May. 2009.
Kuofong, Y.Taoheng, Y.waishuoen, and C.Huihsuan, (2011). *A locationaware rogue AP detection system based on wireless packet sniffing of sensor APs,*. SAC '11 Proceedings of the 2011 ACM Symposium on Applied Computing, ACM.
Kwiatkowska, G. Norman, and J. Sproston. Probabilistic model checking for deadline properties in the IEEE 1394 Fire Wire root contention protocol. Special issue of formal Aspects of computing, 2002
Lambert M. el al. (2010). *Man-In-The-Middle Attack. VDM Publishing*. Henssonow, S.F.
Lambert M. el al. (2010). *Man-In-The-Middle Attack. VDM Publishing*. Henssonow, S.F.
Man Young Rhee, Internet Security: *Cryptographic principals, algorithms and protocols*, John Wiley and sons, 2003.
MAS, (2012). *Technology Risk Management Guidelines*. Consultation Paper. P012 – 2012. Monetary Authority of Singapore.
MAS, (2012). *Technology Risk Management Guidelines.* Consultation Paper. P012 – 2012. Monetary Authority of Singapore.
Meyer, R. (2008). *Secure Authentication on the Internet,* SANS InfoSec Reading Room - Securing Code, Feb. 2008.
Moixe*, M. (2009). New Tricks For Defeating SSL in Practice.* BlackHat Conference, USA. Feb. 2009.
Montgomery, D. (2009). *Design and Analysis of experiments*, John Wiley and sons.
National Institute of Standards and Technology - NIST (2012), *Special Publication 800-164*: Guidelines on Hardware-Rooted Security in Mobile Devices, crsc.nist.gov, 12 November 2012.
National Institute of Standards and Technology - NIST (2012). *Special Publication 800-124*: Guidelines on Cell Phone and PDA Security, crsc.nist.gov, 12 November 2012.
Ornaghi A. and Valleri M. (2013). *Man in the middle attacks*. Blackhat Conference.
Ornaghi A. and Valleri M. (2013). *Man in the middle attacks*. Blackhat Conference. Payment on Mobile Phones. Proceedings of WISTP 2011.
Peterson A. and Reiher P, (2014). Man in The Middle and other Network Attacks. http://flynn.zork.net/~pedro/docs/seclabs/mitm.pdf.
Peterson A. and Reiher P, (2014). *Man in The Middle and other Network Attacks*. http://flynn.zork.net/~pedro/docs/seclabs/mitm.pdf.
Pfleeger, P. (2009). *Security in computing*. Revised edition, Prentice Hall.
Prowell S. (2010). *Seven Deadliest Network Attacks Syngress Elsevier*. Corporate Drive, Suite 400, Burlington, MA 01803, USA
Prowell S. (2010). *Seven Deadliest Network Attacks Syngress Elsevier*. Corporate Drive, Suite 400, Burlington, MA 01803, USA 2010.
Ralf Burger, R. (2010). *Computer Viruses. A High Tech Disease,* 2010
Salifu A. (2011). Detection of man-in-the-middle attack in IEEE 802.11 networks. Kwame Nkrumah University Of Science And Technology.
Salifu A. (2012). *Detection of man-in-the-middle attack in IEEE 802.11 networks*. Kwame Nkrumah University of Science and Technology. 2012.
Scheinier, B. (2006), *Applied cryptography, protocols, algorithms and source code in C***,** John Wiley and Sons.
Stallings, W. (2006). *Cryptography and Network Security,* Prentice Hall, William stallings, Cryptography and network security, *principles and practices,* NJ: Prentice- hall 2011
Stewart J. (2011). *CompTIA Security+ Review Guide: SY0-201*. John Wiley & Sons.
Stewart J. (2011). CompTIA Security+ Review Guide: SY0-201. John Wiley & Sons.
Tenenbaum, S. (2006). *Computer Networks*. NJ: Prentice- hall.
Tom Olzac, T. (2006). *Just enough Security*, information security for business managers, Rrudio Security.
Wagner, G. (2009). *Modernizing the Army's C3I. Signal*, January.
Wagner, R. (2011). Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks. Retrieved from;
Wagner, R. (2011, August 30). *Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks*. Retrieved from http://savannah.gatech.edu/people/lthames/dataStore/WormDocs/arppoison.pdf
Watkins, R. Beyah, C. Corbett, *A Passive Approach to Rogue Access Point Detection,"* Global Telecommunications Conference, 2007. IEEE. pp. 355-360, Nov.2007
Yimin, Y. and G. Guofei G. (2010). *Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point.* International Conference on Dependable Systems & Networks (DSN), IEEE, June. 2010.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar