IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. IX (Mar-Apr. 2014), PP 35-42
www.iosrjournals.org

Identifying Threats Associated With Man-In-The-Middle Attacks during Communication between a Mobile Device and the Back End Server in Mobile Banking Applications

Anthony Luvanda[1], *Dr Stephen Kimani[1] Dr Micheal Kimwele[1]

[1.] *School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, PO Box 62000-00200 Nairobi Kenya*

Abstract:
Mobile banking, *sometimes referred to as M-Banking, Mbanking or SMS Banking, is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device such as a mobile phone or Personal Digital Assistant (PDA).*

Mobile banking has until recently most often been performed via SMS or the Mobile Web. Apple's initial success with iPhone and the rapid growth of phones based on Google's Android (operating system) have led to increasing use of special client programs, called apps, downloaded to the mobile device hence increasing the number of banking applications that can be made available on mobile phones . This in turn has increased the popularity of mobile device use in regards to personal banking activities.

Due to the characteristics of wireless medium, limited protection of the nodes, nature of connectivity and lack of centralized managing point, wireless networks tend to be highly vulnerable and more often than not they become subjects of attack.

This paper proposes to identify potential threats associated with communication between a mobile device and the back end server in mobile banking applications. The paper should be able to identify the techniques associated with Man in the middle attacks during communication between a mobile device and a back end server and propose controls that will ensure that data theft does not occur during such sessions.

Key words*: man in the middle attack, mobile banking applications secure communication*

I. Introduction

Mobile Banking refers to the provision and availing of banking- and financial services with the help of mobile telecommunication devices. This may include but not confine itself to facilities to conduct bank and stock market transactions, to administer accounts and to access customized information. (Dwivedi 2008)

According to this model Mobile Banking can be said to consist of three inter-related concepts:

- Mobile Accounting
- Mobile Brokerage
- Mobile Financial Information Services

In most cases services that fall under Accounting and brokerage are transaction-based. The non-transaction-based services may consist of an informational nature, however such services are essential for conducting transactions for example a balance enquiry may be required before withdrawing money from your account and placing it into your Mpesa account(mobile phone financial transaction service). The accounting and brokerage services are therefore offered invariably in combination with information services. Information services, on the other hand, may be offered as an independent module.

The advent of the Internet has enabled new ways to conduct banking business, resulting in the creation of new institutions, such as online banks, online brokers and wealth managers. Such institutions still account for a tiny percentage of the industry. (Stallings 2006)

Over the last few years, the mobile and wireless market has been one of the fastest growing markets in the world and it is still growing at a rapid pace. According to the GSM Association andOum, the number of mobile subscribers exceeded 3 billion in September 2009, and should surpass the 4 billion mark by end of 2014.

Mobile banking has until recently (2012) most often been performed via SMS or the Mobile Web. Apple’s initial success with iPhone and the rapid growth of phones based onGoogle’s Android (operating System) have led to increasing use of special client programs, called apps, downloaded to the mobile device.

Deploying banking applications on mobile Android tablets or an iPad has a different set of security requirements than backing up your address book. It requires thinking about the software security and privacy vulnerabilities in a systematic way.

There were relatively few dangers when wireless technology was first introduced, as the effort to maintain the communication was high and the effort to intrude was always lower, but this is no longer the case.

The variety of risks to users of mobile wireless technology have increased as the service has become more popular and the technology more commonly available, (McMillan 2012) the same can be said about mobile banking. Today there are a great number of security risks associated with the current wireless protocols and methods, as carelessness and ignorance exists at the user and corporate IT level.(Anderson 2009) with the most common being the man in the middle attack. A man in the middle attacker entices computers to log into a computer which is set up as a soft AP (access point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transpire. One type of Man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a "de-authentication attack". This attack forces AP-connected computers to drop their connections and reconnect with the cracker's soft AP. (McClure 2009) Man in the middle attacks are enhanced by software such as LANjack and AirJack, which automate multiple steps of the process. What once required some skill can now be done by script writing novices.

II. Man In The Middle Attacks On Mobile Banking Applications

A Man in the middle attacksis 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 attacks, 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)

A Man in the middle attacksis 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.

2.1 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.

The Trillian 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.

"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, e-mails and instant messaging 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 attacksattacks 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.

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.

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 APIs are extremely confusing, they are very easy to get wrong and people do get them wrong all the time.

The risks and prevalence associated with Man in the middle attacks attacks cannot be taken for granted, as understated by the cases bellow:

- 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)

  FinFisher has been used for some time in compromising personal computers. The commercial version was originally sold to law enforcement 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 our 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.
- The malware risk on Android phones is a growing concern. A study released 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 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 Sametime. In addition, the researchers were able to disable anti-virus apps and remotely inject and execute code.

2.1.1 Methods And Techniques Used By Hackers In Perpetrating Man In The Middle Attacks

The most common Man in the middle attacks 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 atrojan horse that steals banking information by keystroke logging and form grabbing. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States department of transportation, it became more widespread in March 2009. In June 2009, (Buger 2010)

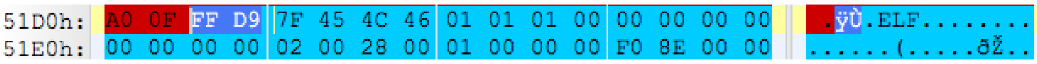
It was largely believed thatThe Zeus Botnet only targets Microsoft Windows machines, and computers running Windows Vista make up the majority of the Botnet, though Zeus newer than Version 1.4.0.0 can also affect Windows Vista SP1. (Buger 2010) It was further believed that (and it's still the case now) Every criminal can control which information he's 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 700USD(if sold from a reseller) and up to 15,000USD 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, Symbiam, 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 AxelleAprville, 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)

Another common strategy for perpetrating Man in the middle attacks used by hackers is the new variant of Legacy NativeLeNa**.** LeNamasquerads as a legitimate application and attempts to trick a user into activating its malicious payload by invoking the SU utility, which is used by "rooted" users to selectively grant superuser privileges to applications that request them. After the repackaged application gains root access, it functions properly, but simultaneously installs a native binary file to the device granting remote control, including the ability to install additional software without any user notification. Because of its dependency on the SU utility to gain root permissions, the pool of users vulnerable to LeNA is inherently limited to those that root their devices – a relatively small, albeit technically adept set of users. (Jiang 2011)

There exists a significant update to LeNa that uses the GingerBreak exploit to gain root permissions on a device. By employing an exploit, this new variant of LeNa does not depend on user interaction to gain root access to a device. This extends its impact to users of devices not patched against this. All Lookout users are already protected against LeNa and it is not (at this time) believed to have been in the Google Play market. This new variant of LeNa hides its payload just past the "End of Image" marker of an otherwise fully-functional JPEG.



```
51D0h: A0 0F FF D9 7F 45 4C 46 01 01 01 00 00 00 00 00   .ÿÙ.ELF........
51E0h: 00 00 00 00 02 00 28 00 01 00 00 00 F0 8E 00 00   ......(.....ðŽ..
```

Hidden at the end of this JPEG is a nested pair of ELF binaries. One exploits the GingerBreak vulnerability to drop and launch the second, an updated version of LeNa. As in its predecessor, this payload communicates with a remote Command and Control server and accepts instructions to install additional packages and push URLs to be displayed in the browser. At this time, LeNa seems to be focusing on pushing a single package to the device: com.the9.gamechannel, a Chinese-language alternative market that publishes Android games. This package is installed without the user's knowledge and subsequently launched – the result being that this alternate market may be front-and-center on a device after a user leaves it unattended for a prolonged period of time. While it shares much of the same functionality as any mobile application store, this alternate market has not been designed to mimic the official Google Play market. (Jiang 2011) This latest version of LeNa has recently emerged in alternative markets, and it is not (at this time) believed to have been in the Google Play market. Among the apps in which this payload appears, however, is a fully functional copy of the recently released Angry Birds Space. The authors are undoubtedly hoping to capitalize on the latest release from this popular franchise to increase uptake on distribution.

2.2 Existing related efforts/dissertations for implementing security against man in the middle attacks

2.2.1 Human Interactive Security Protocols as proposed by Cheng Bangdao and A.W. Roscoe

Cheng and Roscoe identified a growing trend of integrating mobile phones with electronic identity, giving the phone the ability to prove or support the identity of the owner by containing for example, for example a tuple of name, ID photo and public key. They further state that though this helps phone owners prove who they are, it does not prove to them that they are giving their identities to intended parties.

Their dissertation is a Human Interactive Security Protocol (HISP) which may enhance privacy and avoid cases of identity theft by bootstrapping security over insecure networks such as the internet and WiFi without any pre-existing network of secrets. This they state may be achieved by transferring a small amount of non-secret information, usually by human users that is authenticated by context. [Adida 2006]

The down side to such a dissertation is that depending on human interaction can be dangerous since humans can be lazy, which can be a great impediment to well-designed security

2.2.2 Site key

SiteKey is a web-based security system that provides one type of mutual authentication between end-users and websites. Its primary purpose is to deter phishing. SiteKey has been deployed by several large financial institutions since 2006, including bank of America and The Vanguard group.The product is owned by RSA Data Security which in 2006 acquired its original maker, Passmark Security. [Kugler 2003]

SiteKey uses the following challenge-Response technique:

1. User *identifies* (**not** authenticates) himself to the site by entering his username (but not his password). If the username is a valid one the site proceeds.
2. Site authenticates itself to the user by displaying an image and accompanying phrase that he has earlier configured. If the user does not recognize them as his own, he is to assume the site is a phishing site and immediately abandon it. If he does recognize them, he may consider the site authentic and proceed.
3. User authenticates himself to the site by entering his password. If the password is not valid for that username, the whole process begins again. If it is valid, the user is considered authenticated and logged in.[Asokan 2005]

SiteKey is designed to prevent users from disclosing their login credentials to a phishing site. The rationale is that a phishing site wouldn't have the SiteKey info for a user. The obvious flaw in the design is that 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]

2.2.3 The WiKID Strong Authentication system

WiKid Strong authentication approach relies on two-factor authentication.**Two-factor authentication** (TFA, T-FA or 2FA) is an approach to authentication which requires the presentation of "two or more" of the three authentication "factors" ("something the user knows", "something the user has", and "something the user is").

Two-factor authentication is commonly found in electronic computer authentication, where basic authentication is the process of a requesting entity presenting some evidence of its identity to a second entity. Two-factor authentication seeks to decrease the probability that the requestor is presenting false evidence of its identity. The number of factors is important as it implies a higher probability that the bearer of the identity evidence indeed holds that identity in another realm (i.e.: computer system vs real life). In reality there are more variables to consider when establishing the relative assurance of truthfulness in an identity assertion, than simply how many "factors" are used.

Two-factor authentication is often confused with other forms of authentication. Two factor authentications require the use of two of the three regulatory-approved authentication factors.

These factors are:

Something the user knows (e.g., password, PIN);

Something the user has (e.g., ATM card, smart card); and

Something the user is (e.g., biometric characteristic, such as a fingerprint). [Roscoe 2010]

Two-factor authentication is not a new concept, having been used throughout history. When a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card the customer slides into the machine ("something the user has"). The second factor is the PIN they enter ("something the user knows"). Without both of these factors, authentication cannot succeed. This scenario illustrates the basic concept of most two-factor authentication systems; the "something you have" + "something you know" concept. [Nguyen 2010]

Two-factor authentication (or multi-factor authentication) is sometimes confused with "strong authentication", however, "strong authentication" and "multi-factor authentication" are fundamentally different processes. Soliciting multiple answers to challenge questions may be considered strong authentication but, unless the process also retrieves "something you have" or "something you are", it would not be considered multi-factor. The U.S. Federal Financial Institutions examination council issued supplemental guidance on this subject in August 2006, in which they clarified, "By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category would not constitute multifactor authentication."

According to proponents, TFA could drastically reduce the incidence of online identity theft, and other online fraud, because the victim's password would no longer be enough to give a thief permanent access to their information. However, many TFA approaches remain vulnerable to Trojan controlled websites and Man in the middle attacks.

In addition to such direct attacks, three aspects must be considered for each of the 2 (or more) factors in order to fully realize the potential increase in confidence of authentication:

The inherent strength of the mechanism, i.e. the entropy of a secret, the resistance of a token to cloning, or the uniqueness and reliability of a biometric.

However the quality of provision and management is an issue. This has many aspects, such as the confidence you can have that a token or password has been securely delivered to the correct user and not an imposter, or that the correct individual has presented himself for enrolment of his biometric, as well as secure storage and transmission of shared secrets, procedures for password reset, disabling a lost token, re-enrolment of a biometric, and prompt withdrawal of credentials when access is no longer required. [Roscoe 2010]

Proactive fraud detection, e.g. monitoring of failed authentication attempts or unusual patterns of behavior which may indicate that an attack is under way, and suitable follow-up action However WiKID strong authentication protocol still does not adequately deal with the problem of Man in the middle attacks especially within mobile applications.

2.3 proposed used of a probabilistic model checker to secure mobile transactions

Probabilistic model checking is an automatic procedure for establishing if a desired property holds in a probabilistic model, aimed at verifying probabilistic specifications. A probabilistic model checker calculates the probability of a given temporal logic property being satisfied, as opposed to validity [Kwiatkowska 2002]. In contrast to conventional model checkers, which rely on reachability analysis of the underlying transition system graph, probabilistic model checking additionally involves numerical solutions of linear equations and linear programming models.

Probabilistic modeling is widely used in the design and analysis of computer systems, and has been rapidly gaining importance in recent years. It is an automatic procedure for establishing if a desired property holds in a probabilistic system model.

Conventional model checkers input a description of a model, representing a state-transition system and a specification, typically a formula in some temporal logic and a return of “yes” or “no”. In the case of probabilistic model checking, the models are probabilistic (typically variants of Markov chains), in the sense that they encode the probability of making a transition between states instead of simply the existence of such a transition. A probability space induced on the system behaviors enables the calculation of likelihood of occurrence of certain events during the execution of the system. This in turns allows one to make quantitative statements about the system, in addition to the qualitative statements made by conventional model checking.

III. Conclusion

It is evidently clear that there exist high risks of man in the middle attacks being perpetrated via various techniques during communication between a hand held mobile device and the back end server of a banking institution. The proposed solutions mentioned in this paper rely heavily on human intervention, are not highly suitable for mobile applications especially when communicating to back end servers and tests have proven that they are still susceptible to Man in the middle attacks.

Hence the need to identify a framework that will enhance secure communication between mobile applications and back end servers from man in the middle attacks while at the same time reducing the heavy reliance on human intervention. This can be achieve by employing a probabilistic model checker to calculate the probability of a given temporal logic property to ensure that it is satisfactory, i.e. perform an analysis of certain factors with the aim of calculating a satisfactory ration as to whether the program a user is communicating with is consistent with the factors that revolve around a genuine program belonging to a bank or not. This will in turn offer a more secure environment for performing mobile based banking transactions while at the same time reducing the risk of introducing further threats to the communication.

References:

[1]. 3GPP TS 33.102, “3G security; Security architecture,” 3GPP, Rel-11, version11.1.0, Dec. 2012.

[2]. Abhijit S. Pandya, ErcanSen, ATM Technology for Broadband telecommunications Networks, CRC Press, 1998.

[3]. B. Adida, M. Bond, J. Clulow, A.Lin, S. Murdoch, R.J Anderson and R.Rivest. Phish and chips.In Security Protocols Workshop, 2006.

[4]. Bruce scheinier, Applied cryptography,protocols, algorithms and source code in C, John Wiley and Sons 2006.

[5]. Charles P. Pfleeger, Security in computing, Revised edition, Prentice Hall 2007.

[6]. Douglas C Montgomery, design and Analysis of experiments, John Wiley and sons 2009

[7]. D.Kugler. “man in the middle” Attacks on Blue tooth. In Proc. Financial Cryptography 2003

[8]. Englewood Cliffs, Data Networks: Concept theory and practice, NJ: Prentice- hall, 2005

[9]. Ray Harok, communication systems and networks, Wiley publishing 2009.

[10]. Gen Louis C. Wagner, "Modernizing the Army's C3I", Signal, January 2009

[11]. George Ou. "Ultimate wireless security guide: A primer on Cisco EAP-FAST authentication".

[12]. TechRepublic.http://articles.techrepublic.com.com/5100-10878_11-6148557.html. Retrieved 2008-10-02.

[13]. http://www.blm.gov/wo/st/en/prog/more/bea/Glossary.html#mhttp://www.engadget.com/tag/carputer/

[14]. http://www.microsoft.com/technet/network/eap/eap.mspx.Retrieved 2008-10-02. http://www.wifialliance.org/knowledge_center_overview.php?docid=4486. Retrieved 2008-02-06.

[15]. Joshua Bardwell; Devin Akin.CWNA Official Study Guide (Third ed.). McGraw-Hill.p. 435.ISBN0072255382.2005

[16]. Kevin Beaver, Peter T. Davis, Devin K. Akin. "Hacking Wireless Networks For Dummies". Prentice hall 2009

[17]. LachuAravamudhan, Stefano Faccin, RistoMononen, BasavarajPatil, YousufSaifullah, Sarvesh Sharma, Srinivas Sreemanthula. "Getting to Know Wireless Networks and Technology", InformIT 2009

[18]. Lance J. Hoffman, Rogue Programs: Viruses, Worms, and Trojan Horses, 1990

[19]. B. Yan, G. Chen, J. Wang, and H. Yin, "Robust Detection of Unauthorized Wireless Access Points," Mobile Networks and Applications Journal, vol. 14(4), pp. 508-522, Aug. 2009. Bangdao, C., & Roscoe, BMobile Electronic Identity: Securing. (2011)

[20]. D. Jiang, L. Xinghui, and H. Hua, "A Study of man-in-the-Middle Attack Based on SSL Certificate Interaction," 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp. 445-448, Oct. 2011.

[21]. F. Callegati, W. Cerroni, and M. Ramilli,, "man-in-the-Middle Attack to the HTTPS Protocol," Security & Privacy, IEEE, pp. 78-81, 2009.

[22]. http://www.passmarksecurity.com/BofA.jsp

[23]. http://www.wikidsystems.com

[24]. Internet Incident Response Support Center, “Internet Attack Trends and Analysis,” Korea Information Security Agency, pp. 22-37, Jun. 2007

[25]. K. Cheng, M. Gao, and R. Guo, "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.

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

[27]. K. kuofong, L .ien, and L. Yuehchia, "Detecting rogue access points using client-side bottleneck bandwidth analysis," Computers & Security, vol. 24(3-4), ELSEVIER, pp. 144-152, May. 2009.

[28]. K. Kuofong, Y.Taoheng, Y.waishuoen, and C.Huihsuan, "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, 2011.

[29]. L. Watkins, R. Beyah, C. Corbett, "A Passive Approach to Rogue Access Point Detection," Global Telecommunications Conference, 2007. IEEE. pp. 355-360, Nov.2007

[30]. M. 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

[31]. M. Moixe, "New Tricks For Defeating SSL in Practice", BlackHat Conference, USA. Feb. 2009.

[32]. Man Young Rhee, Internet Security: Cryptographic principals, algorithms and protocols, John Wiley and sons, 2003.

[33]. N. Asokan, V. Niemi, and K. Nyberg. Man in the middle in tunneled authentication protocols.In security protocols workshop, 2005.

[34]. Nate Anderson "One-minute WiFi crack puts further pressure on WPA".2009

[35]. Ars Technica.http://arstechnica.com/tech-policy/news/2009/08/one-minute-wifi-crack-puts-further-pressure-on-wpa.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss. Retrieved 2010-06-05.

[36]. Payment on Mobile Phones. Proceedings of WISTP 2011.
R. Beyah, "Rogue access point detection_challenges, solutions, and future directions," IEEE Security and Privacy Article, vol. 9(5), IEEE, pp. 56-61, 2011

[37]. R. Meyer, "Secure Authentication on the Internet, " SANS InfoSec Reading Room - Securing Code, Feb. 2008.

[38]. Ralf Burger, Computer Viruses. A High Tech Disease, 2010

[39]. RamezElmasri and Shamkant B. Navathe.Fundamentals of Database Systems, 4th Edition.Addison-Wesley, 2004.

[40]. Robert McMillan. "Once thought safe, WPA Wi-Fi encryption is cracked". IDG.http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119258. Retrieved 2008-11-06.

[41]. Ross M. Greenberg, "Know Thy Viral Enemy", Byte, June 1999

[42]. Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed, Network Security secrets and solutions, Mcgraw hill 2009.

[43]. Susan Kellam, "Adapso Urges Congress to Act on Viruses", Washington Technology, July 13, 1999

[44]. Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2006): Customer on the Move: Strategic Implications of Mobile Banking for Banks and Financial Enterprises, in: CEC/EEE 2006, Proceedings of The 8th IEEE

[45]. International Conference on E-Commerce Technology and The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), San Francisco, pp. 522–529

[46]. Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2006): Mobile Banking as Business Strategy: Impact of Mobile Technologies on Customer Behaviour and its Implications for Banks, in: Technology management for the Global Future - Proceedings of PICMET '06.

[47]. S. Yimin, Y. Chao, and G. Guofei, "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.

[48]. T. Chomsiri,"HTTPS Hacking Protection, " 21st International Conference on Advanced Information Networking and Applications Workshops, IEEE, May. 2007.

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

[50]. U Black, Foundation for Broadband Networks, NJ: Prentice- hall, 2011

[51]. William A Shay, Understanding data communication and Networks, Second Edition, Brooks/Coe publishing company. 2012

[52]. William Stallings, Computer Networking with internet protocols and technology, Peason NJ: Prentice- hall, 200

[53]. William Stallings, Cryptography and Network Security, Prentice Hall, 2003

[54]. William stallings, Cryptography and network security, principles and practices, NJ: Prentice- hall 2011

[55]. WiMAX Forum - Technology. Retrieved on 2008-07-22.

[56]. Yogesh Kumar Dwivedi,TheHandbook of Research on Global Diffusion of Broadband Data Transmission, Information Science Reference, 2008