IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 2, February 2016.
www.ijiset.com
ISSN 2348 – 7968

Securing Online Banking Services against Man in the Middle Attacks by use of two Factor Authentication.

Alexis Rusagara, Dr. Cheruiyot W.K, Dr. Anthony Luvanda

Abstract- In this paper, enhanced security of online banking transactions against man in the middle is presented basing on two factor authentications by use of one time password and single password. Online banking is a system allowing individuals to perform banking activities at home via the internet. Online banking through traditional banks enable customers to perform all routine transactions, such as account transfers, balance inquiries, bill payments, Account information can be accessed anytime, day or night, and can be done from anywhere. Online transactions are considered most sensitive. Doing such online transactions via a public network consequently introduces new challenges for security and trustworthiness, They are two types of common attacks in online banking which are offline credential stealing attacks and online channel breaking attacks. This paper provide a solution to the problem encountered in online channel-breaking attacks. The intruder unnoticeably interrupts messages between the client PC and the banking server by masquerading as the server to the client and vice versa.

This kind of attack is used to anonymously perform some operations on the user's account. For this purpose the current paper proposed a new approach of two factor authentication with one time password generated on two sided which are client side and server side. Qualitative methods are used for data collection. The qualitative methods can be classified in three broad categories: in-depth interview, observation methods, document review. Finally, the paper discuss and analyze how two factor authentication will enhance security of online banking services against man in the middle and provide recommendations for further security.

Keywords: Internet banking , man in the middle attack, factor authentication, one time password.

1. Introduction

Information technology takes the task of supporting and raising service efficiency in all businesses. Banking industry is one of the businesses that have brought IT to help with banking transactions and expand bank service opportunities to its customers.

The Internet of today has become an integral part of our everyday life and the proportion of users expecting to be able to manage their bank accounts anywhere anytime is constantly growing. As such, Internet banking has come to age as a crucial component of any financial institution. Internet banking is defined as the use of the Internet to deliver banking activities such as funds transfer, paying bills, viewing current and savings account balance, paying mortgages and purchasing financial instruments and certificates of deposits (Singhal and Padhmanbhan, 2008; Ahasanul et al, 2009). Internet banking is also called Online banking, e–payment and e–banking (Ozuru et al, 2010; Singhal and Padhmanbhan, 2008; Beer, 2006; Jun and Cai, 2001; IAMAI, 2006). E–payment is described as a means whereby banking businesses are transacted through automated processes and electronic devices such as personal computers, telephones, and fax machines, Internet card payments and other electronic channels (Turban et al, 2006; Ozuru et al, 2010). The electronic communications used in Internet banking includes: Internet, e–mail, e–books, data base and mobile phones (Chaffey et al, 2006). Cell phone banking apart from Internet banking is considered the way of the future (Fisher – French, 2007; Masocha et al, 2011).

Internet has changed the dimensions of competition in the retail banking sector. Following the introduction of PC banking, ATMs and phone banking, which are the initial cornerstones of electronic finance, the increased adoption and penetration of Internet has added a new distribution channel to retail banking: Internet/Online-banking. Allen et al (2002) define E-finance as “the provision of financial services and markets using electronic communication and computation” and today retail banks are switching to multi-channel distribution of financial services in hybrid platforms where the traditional services of banks are provided through both “bricks and mortar” branches and Internet.

Internet technology holds the potential to fundamentally change banks and the banking industry. An extreme view speculates that the Internet will destroy old models of how bank services are developed and delivered (DeYoung, 2001a).

The widespread availability of Internet banking is expected to affect the mixture of financial services produced by banks, the manner in which banks produce these services and the resulting financial performances of these banks.

ISSN 2348 – 7968

Whether or not this extreme view proves correct and whether banks take advantage of this new technology will depend on their assessment of the profitability of such a delivery system for their services. In addition, industry analysis outlining the potential impact of Internet banking on cost savings, revenue growth and risk profile of the banks have also generated considerable interest and speculation about the impact of the Internet on the banking industry (Berger, 2003). The Internet has changed the way people bank. Banks have actively promoted online services to save costs and create new business opportunities; their customers benefit from being able to pay bills and transfer funds without having to go to a bank branch.

2. Methods and Techniques Used by Man in the middle attacks Against online banking services.

The security of information may be one of the biggest concerns to the Internet users. For electronic banking users who most likely connect to the Internet are faced with a risk of someone breaking into their computers and steal their online banking credentials. Organizations such as banks with dedicated Internet connections face the risk of someone from the Internet gaining unauthorized access to their computer. However, the electronic banking system users face the security risks with unauthorized access into their banking accounts while doing their transactions.

Man in the middle is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting their own public key for the requested one, so that the two original parties still appear to be communicating with each other. This kind of attack is used to anonymously gain user's credentials and perform some operations on the user's account later. A man-in-the-middle (MITM) attack is a form of eavesdropping where communication between two users is monitored and modified by an unauthorized party. Generally, the attacker actively eavesdrops by intercepting a public key message exchange and retransmits the message while replacing the requested key with his own. In the process, the two original parties appear to communicate normally. The message sender does not recognize that the receiver is an unknown attacker trying to access or modify the message before retransmitting to the receiver. Thus, the attacker controls the entire communication. This term is also known as a janus attack or a fire brigade attack

3. Similar Works on Security on Online Banking Services Against Man In the Middle

3.1 Single-Factor Authentication

Virtually all secure systems require restriction of user to authenticated identities only, commonly through a username and password combination. The traditional single-factor authentication is considered as “inadequate” to protect the transactions from criminal attacks such as account fraud and identity theft (FFIEC, 2005; Hong Kong Post 2007). This method is well understood by users and requires no additional hardware, software or training beyond the most basic authentication server and asking a user to register a password initially. The use of passwords, however, has many flaws and is considered by most as a weak authentication mechanism. Authentication mechanisms are not keeping up with the usage and security requirements of online services. The CERT/CC (Computer Emergency Response Team / Coordination Center), a federally funded organization has estimated that 80% of network security problems are caused by bad passwords. The problem is that the average user can only remember a maximum of about 7 passwords and these are usually of low complexity (Yan et al., 2004). By low complexity it is meant that they are based on dictionary words that can be guessed or predicted with relatively little effort or are sufficiently short that a man in the middle can be performed very quickly.

To solve the problems with passwords, two-Factor authentication are used. Rather than relying solely on the single factor of what the user knows, e.g. password, it introduces either what the user is, e.g. biometrics, or what the user has, e.g. a token (O’Gorman, 2004). Once the user has logged in to the system, the session can be hijacked and any additional transactions performed without the user’s knowledge (Schneier, 2005).

3.2 Tokens and biometrics

Tokens and biometrics are also an authentication option for online banking services. The user will have to carry the token with them and may require further software installed on each computer. The near ubiquity of the mobile phone, and the

ISSN 2348 – 7968

propensity for the user to carry their mobile wherever they go, mean that this is a good device to select for a second factor or token. Solutions using mobile phones are becoming more common from the sending of OTPs via SMS to software OTP tokens to run on devices such as RSA's SecureID software token (RSA, 2011).

These, however, suffer the same problems as above and are not immune to being cracked or cloned, with tools able to mimic them freely available for download (OXID, 2011). Due to the cost and delay caused by delivery of the token by sms, this solution have not been applied in this paper. Here an architecture is proposed to provide 2-factor authentication for securing online banking services against man in the middle by using an algorithm,

which is used to produce its own one-time pass code. Simply displaying a onetime pass code on the screen.

3.3 The Quick Response code authentication

The Quick Response (QR) code authentication systems have been proposed for web-based authentication. One such example is proposed by Mizuno et al. (2005). The system uses the mobile phone as a token in the authentication process by displaying a QR code in the user's web browser passing a session-ID and nonce back and forth between the authentication server and the mobile device. The weakness of this system stems from relying on the cellular network to be secure. If the link between the mobile and the authentication servers can be intercepted then the security fails. The mobile phone is identified solely by the ability to send and receive. An improved system was proposed by Tanaka et al. (2007), which sends the unique ID of the mobile device, the user's PIN and the network service provider username to the authentication server in order to lock the authentication down to an individual, unique mobile phone. However, the token, T, displayed in the QR code is sent in the clear and used, concatenated with the other data, in the return channel, as follows:

T || h(T || ID || PIN || username) || username

where h(M) is a hash function and || denotes concatenation. T and username would be known to an attacker and it is possible to find the ID as well. In this scenario, if the ID were to become known then a simple brute-force attack of the 10,000 possible PIN numbers is feasible. Also, in the case of a collision in T, then a simple replay attack is possible. Again, this system relies on the security of the cellular network assuming that it will be secure. This is not a valid assumption. Whilst UMTS security may currently be proof against practical attacks, GSM is not and frequently phones will have to drop back to GSM. Indeed, it is possible to jam the signals of other services and only leave GSM open. In addition to this, although out-of-band channels can help security, they also hurt usability and availability. If users are out of network coverage or in an environment where the use of wireless transmission is prohibited, then this authentication mechanism fails. It could also put the financial burden on the end user due to data transfer requirements over the cellular network.

3. Proposed Approach For Securing Online Banking Services Against Man In The Middle Attacks

Many technologies and methodologies have been developed for online banking services security to authenticate customers. Therefore, in this paper the combination of login password and password generating token which result two factor authentication for solving the problem of security of online banking for making online transaction more secure have been proposed, by not sending sms but by generating its own OTP using the information which comes from authentication server. This produces a unique pass-code, also known as a one-time password each time it is used. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token. The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor). The customer is authenticated if the regular password matches and the OTP generated by the token matches the password on the authentication server.

This approach is very secure and fraudsters can't steal the user's credentials. One time password approach will be achieved by developing an algorithm which generates its own one time password by using the time and customer's information which comes from authentication server.

ISSN 2348 – 7968

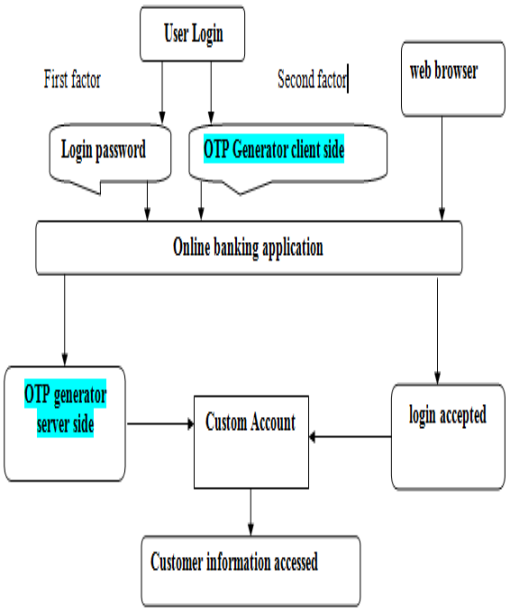

Figure 1: Conceptual framework

3.1 One Time Password Algorithm

An algorithm is a procedure or formula for solving a problem. A computer program can be viewed as an elaborate algorithm.

In mathematics and computer science, an algorithm usually means a small procedure that solves a recurrent problem.

The following algorithm describe how one time password are generated.

1. Start
2. Get account number of customer
3. Get time from server
4. If the time from server is not fund then the password equals to zero which means that there are problem of the network
5. If the time from server is found then the password receives the concatenation of the account number and time from server
6. Encryption of the password
7. New password receives nine digit from the encrypted password
8. Display the new password
9. Stop

3.2 One Time Password Flow chart

A flow chart is a type of diagram representing a process using different symbols containing information about steps or a sequence of events. Each of these symbols is linked with arrows to illustrate the flow direction of the process.

Flowcharts are a methodology used to analyze, improve, document and manage a process or program. Flowcharts are helpful for: Aiding understanding of relationships among different process steps, Collecting data about a particular process, Helping with decision making, Measuring the performance of a process, Depicting the structure of a process, Tracking the process flow, Highlighting important steps and eliminating the unnecessary steps.

A flowchart in computer science typically has the following types of symbols to represent a process or program: Oval/Rounded Rectangle/Circle: Represents any process having a start and an end activity. Rectangles: Represents a process activity or step. Diamonds: Used when there is a decision to be made or a question to be answered, such as Yes/No or True/False. The path to be taken is determined by the answer to the question. Arrow lines: Used to show the flow of control from one step to the other. They also indicate progress from one step to another. Parallelograms: Used to represent input/output.

Flowcharts are commonly used in developing business plans, designing algorithms and determining troubleshooting steps. Many software programs are available to design flowcharts. Some of the commonly used software programs are SmartDraw, Visio (designed for PCs) and OmniGraffle (designed for Macs). The algorithm flowchart in this research was developed by using visio.

ISSN 2348 – 7968

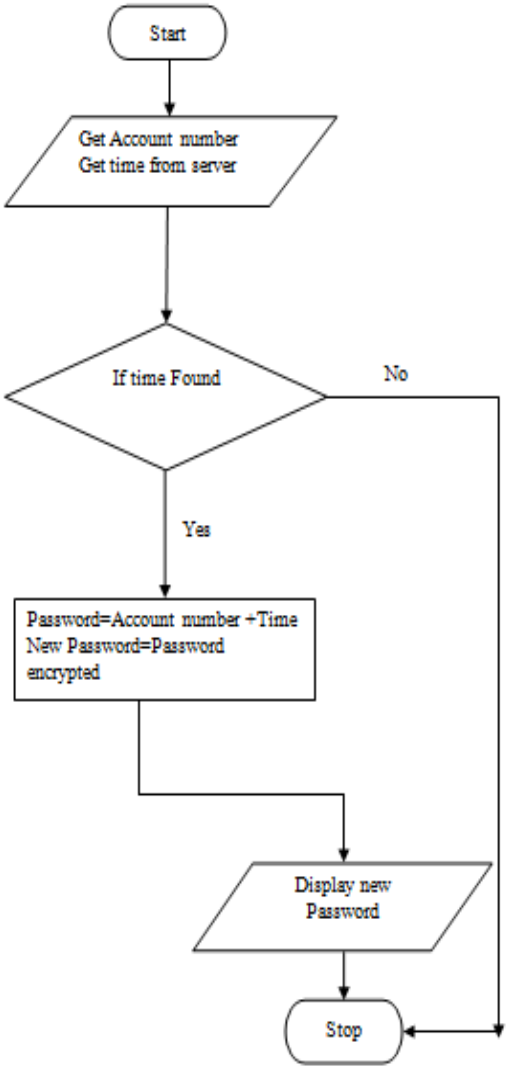

Figure 2: One time password flowchart

4. Methods of generating One Time Password

OTP generation algorithms typically make use of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed:

- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging. Finally, in some systems, OTPs are printed on paper that the user is required to carry.

In this paper we have used time-synchronization between the authentication server and the client pc combined with customer's information.

4.1 Time synchronized

A time-synchronized OTP is usually related to a piece of hardware called a security token (e.g., each user is given a personal token that generates a one-time password). It might look like a small calculator or a keychain charm, with an LCD display that shows a number that changes occasionally. Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server.

On these OTP systems, time is an important part of the password algorithm, since the generation of new passwords is based on the current time rather than, or in addition to, the previous password or a secret key. This token may be a proprietary device, or a mobile phone or similar mobile device which runs software that is proprietary, freeware, or open-source.

5. Results and Discussion

The results of the analysis are realized by developing an algorithm with token which generate one time password for securing online banking transaction against man in the middle. The result were analyzed from secondary data collected from equity bank Rwanda. Two Factor Authentication, also known as 2FA, two step verification or TFA (as an acronym), is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have

ISSN 2348 – 7968

immediately. Using a username and password together with a piece of information that only the user knows makes it harder for man in the middle or potential intruders to gain access and steal that person's personal data or identity. Many people probably do not know this type of security process is called Two-Factor Authentication and likely do not even think about it when using hardware tokens, issued by their bank to use with their card and a Personal Identification Number when looking to complete Internet Banking transactions. Simply they are utilising the benefits of this type of multi factor Authentication - i.e. "what they have" AND "what they know".

The two factor authentication with first factor encrypted and one time password was used in this paper to enhance security of online banking against man in the middle. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors. In this paper we have chosen to use MD5 message-digest algorithm to encrypt customer's password which is first factor in this research. The second factor in this paper is one time password. The purpose of a one-time password (OTP) generator is to make it more difficult to gain unauthorized access to restricted resources, like a bank account or a database with sensitive information. Static user names and passwords can be accessed more easily by an unauthorized intruder given enough attempts and time. By constantly altering the password, as is done with a one-time password, this risk can be greatly reduced. In this paper the token to generate password to be used only one time has been develop. The next figure shown password generated.

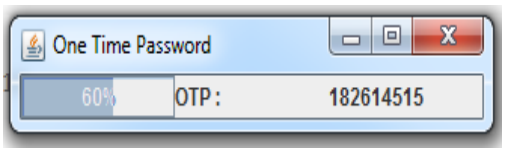

Figure 3: One time password Token

As shown by the figure above, the developed token generate nine digit which is a combination of time from server and customer's account number encrypted and selected by hazard.

Those nine digit are change every one minute as shown by the progress on the token, the percentage indicate that the digit are about to be change when comes to 100% of its lifetime. The next table shows generated password in different time.

One Time Password Generated

Time	OTP
02:35	378062814
02:36	631744817
02:37	70145850
02:38	41751168
02:39	718607837
02:40	563415770
02:41	815474647
02:42	51854057
02:43	724688868
02:44	355746516
02:45	357524743
02:46	17668577
02:47	151141657
02:48	78353120
02:49	484333841
02:50	135685576
02:51	757211043

Figure 4: one time password generated report

As shown on the table of generated password, every minute the new password are generated every minute and each password is different with the next one. The researcher has chosen to develop client and server token which generate similar one time password, to be authenticated on online banking, the client password must be the same as the password generated on server side.

At the login page, users send his username, first password and second password to server and the sever verify if the user exist and generate one time password according to the user's information, the user will be authenticated if one time password of client side is the same with one time password generated on server side. The next figure shows login page for the purpose of testing.

ISSN 2348 – 7968

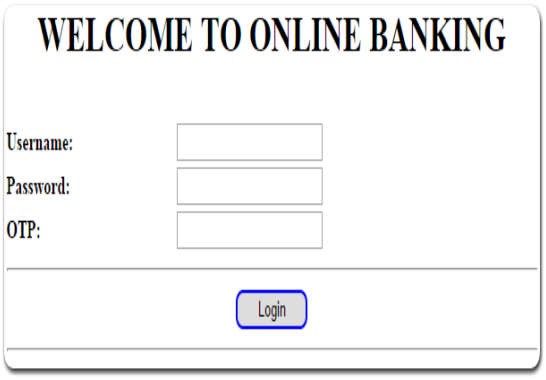

Figure 5: login page of online banking

From the login page above, its shows two factor authentication login level, always to be authenticated, the username are required and password which is first factor and OTP which is second factor are required. The user will be authenticated when the OTP of client side is the same with the OTP on server side.

Login Report

UserName	First Password	OTP	Login Status	Login Time
kamana	kamana	125365898	fail	2015-13-04 08:13:03
kaka	kaka	32568988	succes	2015-02-11 09:02:21
kiki	kiki	32568988	succes	2015-23-11 09:23:20
alex	rus4g4r4	134182564	succes	2015-25-11 09:25:26
			fail	2015-26-11 09:26:39
jagua	jijna	65895565	fail	2015-26-11 09:26:59
john	john	370773404	fail	2015-17-12 07:17:30
john	john	648805450	succes	2015-17-12 07:17:57
kalisa	kalisa	1235689	fail	2015-18-12 07:18:14
lklksjls	kjdlgjkd	kmdfljksd	fail	2015-06-12 08:06:18

Figure 6: Online banking Login Report

6. Conclusion

Every scientific work should bring something of innovation or enhancement in the field where it was made. Thus, the overall intend of this paper was to enhance security of online banking against man in middle attacks using two factor authentication of first password encrypted combined with one time password. The two factor authentication was chosen in this paper because this type of authentication is considered faster, quicker and cheaper to set up and maintain.

Based on the result of the new approach concerned the use of MD5 message-digest algorithm for encryption and the development of an algorithm which generate one time password. The analysis of the algorithm outputs showed that generation of one time password have been achieved and the security of online banking against man in the middle by the use two factor authentication have been done. Lastly, at the banking industry, the new approach has an enhancement highlighting on encouraging bank 's customers to the use of online banking which keep their online transaction more secure and confidential.

REFERENCES

1. Meyer, R. (2008). Secure Authentication on the Internet, SANS InfoSec Reading Room Securing Code.
2. Abhishek Gandhi, BhagwatSalunke, SnehalIthape, VarshaGawade, Prof. SwapnilChaudhari, “Advanced Online Banking AuthenticationSystem Using One Time Passwords Embedded in Q-R Code” International Journal of Computer Science and Information Technologies(IJCSIT), Vol. 5 (2) , 2014.
3. O’Gorman, L. (2003), “Comparing Passwords, Tokens, and Biometrics for User Authentication” Proceedings of the IEEE.
4. Schneier, B. (2005), “Two-factor authentication: too little, too late” Communications of the ACM - Transforming China.
5. NayaniSateesh , “An Approach For Grid Based Authentication Mechanism To Counter Cyber Frauds With Reference To Credit CardPayments” Global Journal of Computer Science and Technology(GJCST), Volume 11 Issue 1 Version 1.0 February 2011
6. Starnberger, G., Froihofer, L. &Goeschka, K. M. (2009), “QR-TAN: Secure Mobile Transaction Authentication”, International Conference on Availability, Reliability andSecurity, IEEE Computer Society.
7. P. Schartner and S. B¨urger. (2011). Attacking mTAN-applicationslike e-banking andmobile signatures. Technical report, University of Klagenfurt.
8. Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2004), “Password memorability and security: Empirical results” IEEE Security and Privacy.
9. Tanaka, M., Teshigawara, Y. (2007), “A Method and Its Usability for User Authentication by Utilizing a Matrix Code Reader on Mobile Phones”, WISA 2006, Lecture Notes in Computer Science.
10. Mizuno, S., Yamada, K., Takahashi, K. (2005), “Authentication Using Multiple Communication Channels”, DIM’05, Fairfax, Virginia, USA.
11. Starnberger, G., Froihofer, L. &Goeschka, K. M. (2009), “QR-TAN: Secure Mobile Transaction Authentication”, International Conference on Availability, Reliability and Security, IEEE Computer Society.

ISSN 2348 – 7968

12. DillaSalama Abdul Minaam. Hatem M. Abdul Kadir, Mohily Mohamed Hadhoud. (2010)," Evaluating the effects of Symmetric Cryptographic algorithms on PowerConsumption for different data types‖, International Journal of Network Security.
13. Abhishek Gandhi, BhagwatSalunke, SnehalIthape, VarshaGawade, Prof. SwapnilChaudhari. (2014), "Advanced Online Banking Authentication System Using One Time Passwords Embedded in Q-R Code" International Journal of Computer Science and Information Technologies(IJCSIT).
14. C. Mulliner, R. Borgaonkar, P. Stewin, and J.-P. Seifert. (2013), "SMS-based one-time passwords: Attacks and defense (short paper)". In DIMVA.