Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol 2, No.4, 2011

An Analysis of Text-Based Authentication using Images in Banking System

R. Sujatha (Corresponding author)
Research Associate, Smart and Secure Environment,
Department of Computer Science, Madurai Kamaraj University, Madurai, India.
E-mail: sujamurali72@gmail.com

G. Arumugam
Prof. and Head, Department of Computer Science,
Madurai Kamaraj University, Madurai, India.
E-mail: gurusamyarumugam@gmail.com

The research is financed by National Technical Research Organization, New Delhi.

Abstract

The stipulation of electronic services, such as Transactional, Non-transactional, Financial institution administration, Management of multiple users having varying levels of authority and Transaction approval process, by banking organizations evolves and spreads with the introduction of enhanced communication technologies. Though, this novel business occasion for the provision of banking products and services increases the need for security, especially due to the sensitive nature of the information exchanged. The specific nature of Internet banking systems creates the necessity for focused facts on security issues to be able to successfully demeanor an assessment or security evaluation process. More specifically, the information systems (IS) auditor should have the necessary technical and operational skills and knowledge to carry out the review of the technology employed and risks associated with Internet banking. Following this requirement, this paper presents a novel authentication approach to provide security to the end users. This proposed system, Analysis of Text-Based Authentication using Images in Banking System (ATBAIBS) provides great value in terms of convenience, customer intimacy, time saving, inexpensiveness and coherence in banking sectors.

Keywords: Authentication, Authentication using Images, Banking System, Security, Text-Based Password System, Internet Banking Server, Online User Authentication and ATM System.

1. Introduction

Online banking is a tremendous success for financial institutions and their customers. Customers enjoy the convenience and multiple services offered with online banking. In general, they are more active bankers; they have many more contacts with their financial institutions, representing greater opportunities for marketing and increased cross sell. This represents an opportunity for financial institutions to not only drastically reduce transaction costs when compared to branches or ATMs, but to provide a platform for additional services to offer customers.

However, due to the popularity and growth of online banking, it has become a target for online fraud. Internet criminals are taking advantage of weak password security for user authentication to conduct internet attacks such as phishing, man-in-the-middle, and keystroke logging. This increases risk for both banks and their customers which could inhibit the growth of online banking (Ca technologies 2011).

The online banking landscape is in the midst of a significant transition. Financial institutions who excel in providing security, convenience, and customer care will win the business of online consumers. Customers are demanding it. Consumers consider online security a top priority when choosing a financial association.

The banks implemented stringent physical security within the four walls of banking institution. Customers demand the same level of protection for online banking transactions. The Federal Financial Institutions Examination Council (FFIEC) has issued guidance for banks offering Internet-based financial services to enhance authentication methods and achieve compliance no later than year-end 2006. Leading banks are deploying it (SafeNet 2011).

In this networked world of the internet, the browser and e-mail are the ubiquitous software tools used for information exchange. When applied to the world of electronic banking, bill payment, and ecommerce, the internet is the haven for hackers to steal and commandeer the identity of others and perpetrate fraud (Online Banking Solutions 2011). With the advent of internet banking, customers are given the ability to do multiple financial tasks in just a few clicks of a button. While this may be fast and easy, security threats always exist causing worry among many consumers. Among the different fraudulent online activities that have been identified are the identity theft, pharming, hacking and spamming. In these criminal acts, it's often hard to identify perpetrators. Literally, billions of dollars are lost each year to these nefarious schemes, not to mention the impugned reputations of the masqueraded individuals and the legitimate companies with which they do business.

As providers of internet banking services, banks have the responsibility of ensuring a secure environment for customers notably as money is always being done, experts say that the end user of the public also have to their part and understand the risks involved in internet banking (Intenet Banking Security 2011).

To execute the guidelines provided by the standards, more precise harass and countermeasures should be considered. ATBAIBS provide a formal methodology for analyzing the security of systems and it provides the way of think about security, capture and re-uses expertise about security, and responds to changes in security.

In section 2 related works are discussed with their drawbacks.

Section 3 discusses the overview of Proposed Text-Based Authentication System using Images in Banking Application.

In section 4 implementation details related to the system are presented. Conclusion is given in section 5.

2. Related work and Problems

Despite the advent of a very tech-savvy and vast consumer class in recent years, a mix of industry issues and unique challenges continue to frustrate the expansion of net banking. Technology challenges, IT practices, certain cultural issues, industry lethargy, and workplace constraints have affected widespread acceptance of Internet banking. Some of the problems were discussed as:

2.1 Low Broadband Internet Diffusion

Some of the cities have low broadband connectivity penetration rates compared to Japan, Taiwan, Korea, Singapore etc. PC users in smaller cities and towns still use dial-up options to connect to the Internet. Slow connectivity speeds often dampen the online banking experience for many customers eager to use such services.

2.2 Bank's Diffident Assurance Levels

In the middle of this decade, multinational and domestic private banks started offering net banking services as a competitive differentiator. However, bank's diffident assurance levels and their reluctance to allocate huge budgets for net banking brand initiatives, as well as a lack of industry advocacy efforts, have resulted in poor acceptance levels of Internet banking by customers.

2.3 Fear of Online Threats / Scams

Ubiquitous and widespread online threats about hackers, identity theft, stolen passwords, viruses, worms and spy ware tend to make customers wary just like in any other country. Conservative bank customers used to years of saving in former mixed-collectivist economy are always fearful of losing hard-earned savings in online scams. These customers are also not sure about the value of banks' websites and their commitment to allocate funds for reliable encryption mechanisms and forceful back-end technologies and

systems.

2.4 Impersonal Transactions

Perform transactions in the internet can be very impersonal. No individual to receive and check the money or correct some wrong information that the user might have written on a certain form. Paper and money dealings made by people for personalized services are ideal compared to Internet banking.

2.5 Difficult for First Time Users

For a first time user, navigating through a website of an internet bank may be hard and may take some time. Due to numerous personal details queried the potential customer felt inconvenience in opening an account and make the customer discouraged in use of internet banking service. Friendly environment, tutorials and live customer support may be provided to help the users to perform their required tasks with dynamic environment (Ms Megha Jain et al. 2011).

2.6 Network Security Fraud

Many people introverted from internet banking because of the security threats. Users worry about the fraudulent bank transactions that pop up every now and then. This problem should be solved by banking sectors using the proper security technology in protecting their websites (Uppal R.K. 2007).

2.7 Regulation and Legalities

Internet banking makes it possible for banks and their customers to do business from anywhere in the world. This greatly increases the bank's potential client base. The global approach to banking that e-banking permit makes it extremely difficult for regulatory authorities to enforce finance laws. Additionally, regulations differ from nation to nation and banks are not always proficient in the financial laws for every nation in which they have business. This lack of proficiency opens banks and their users up to law violation and lawsuit.

2.8 Eminence and Database Security

More a bank relies on Internet banking; more the bank may gain an impersonal feel. Both of these problems may discourage clients from choosing a bank that relies on internet banking, regardless of how convenient internet banking may be. E-banking increases convenience, but it also opens a bank to security issues. A criminal might hack into the bank's server in order to acquire bank account data, or a software malfunction might cause the bank to unintentionally distribute personal data to the wrong person. Banks that use Internet banking have to constantly update their software and hardware to make sure that compatibility issues and increased knowledge of security systems do not increase their security risks (Wanda Thibodeaux 2011).

The technology has the potential to change methods of marketing, advertising, designing, pricing and distributing financial products and services and cost savings in the form of an electronic, self-service product delivery channel. The technology holds the key to the future success of banks. Thus, internet banking is the need of the hour, which cannot be lost prospect of except at the cost of elimination from the competition. The existence of internet banking also becomes predictable due to the standards required to be matched at the international level. Therefore the domestic as well as the international standards authorize the adoption of internet banking at the earliest possible moment. To overcome the several drawbacks reported in internet banking about authentication schemes in lieu of the traditional password based system, a method is proposed as Text-Based Authentication System using Images for Banking Applications.

3. Text-Based Authentication System using Images in Banking Applications

This system involves the use of authentication mechanism and a server that minimizes the hacking by the attackers. In Text-Based Authentication System using Images for Banking Applications, a Secured Authentication Protocol System using Images (SAPSI) Protocol (Arumugam G., Sujatha R., 2010) is used for authenticating the Online and ATM users.

Two processes are involved in this system. They are i) Online user authentication ii) ATM user

authentication.

3.1 Online User Authentication

The fundamental idea of ATBAIBS is based on the hypothesis that 'humans are good at identifying, remembering and recollecting graphical patterns than text patterns' (Shepard R.N., 1967; Arumugam G., Sujatha R., 2011).

The core conceive of ATBAIBS is that, 'Instead of remembering a sequence of characters as password, users have to remember a sequence of images as their password'.

Whenever the user wants to access the online user authentication system, the ATBAIBS displays an N x N matrix of cells, which is known as graphical image patterns. In each cell of the image pattern an index number is displayed, that is used to enter the passwords. The typical 8 x 8 graphical image pattern is represented in Figure 1.

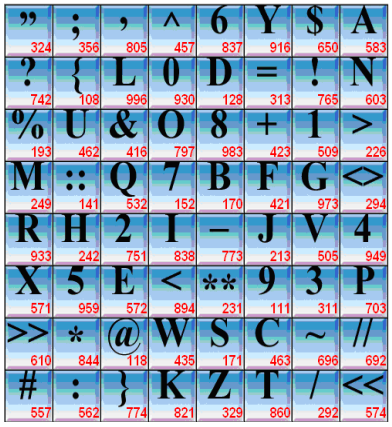


Fig. 1

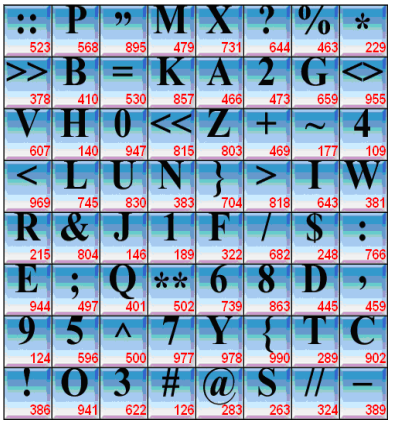


Fig. 1.a

Figure 1: A typical 8 x 8 SAPSI is represented. 1.a: SAPSI in shuffled view.

For providing password the user has to enter the index numbers provided at the images. While entering index numbers in the password area, the numbers will be replaced by bullet marks. For example, if the user chooses images PASS2@~* then the index numbers 703, 583, 171, 171, 751, 118, 696 and 844 should be entered in a selected order. While confirming password, images and index numbers were shuffled, so user has to re-enter the password by giving different index numbers according to the images chosen. According to the user's choice now the user has to enter 568, 466, 263, 263, 473, 283, 177, 229 as index numbers while confirming password. It is represented in Figure 1.a. Here both image patterns and index numbers are represented in a shuffled and varied manner for every login attempt. Due to this dynamic setup no one would be able to read or guess the password mechanism involved in the network.

In this online user authentication process a malicious user cannot attain the end-user password from the network plane. If the malicious user tries to hack the password he / she will get only the index numbers from the network plane. Using that index numbers the malicious user cannot enter into the authentication system because the malicious user will have only index numbers which should not matched with the index numbers present in the login session. During entry of password, only bullets appear in the password area which avoids the shoulder surfing attacks. When sending index numbers in the network plane, it will be converted into a computed Ascii value, so that Man-In-The-Middle attack is prohibited.

The user can select the images on some sequences familiar to him / her. Due to shuffling system, this method reduces the guess ability of the persons who are related to the users. Each image will be mapped with a corresponding number which is stored in the Image-Map table. Instead of comparing the images, the mapped numbers were compared for password verification. It serves as user friendly for the end-user and machine friendly for the system by reducing the comparison time by using numbers rather than images.

A mapping mechanism which validates the index numbers with hidden numbers is represented in Table I.

Using this mapping mechanism the shuffling process of images and index numbers are generated. The images are validated only by using the hidden characters and index numbers along with iterations to reduce the time complexity of comparing the images.

Table I. A Sample Image Map Mechanism for ATBAIBS

Image Numbers	Const Hidden Characters	Index Numbers			
		Iteration 1	Iteration 2	…	Iteration N!
BI1	1A	761	509	…	084
BI2	2G	329	789	…	145
BI3	25	430	890	…	098
BI4	1C	589	342	…	123
BI5	2P	990	111	…	543
BI6	37	546	253	…	234
BI7	9L	223	687	…	345
:	:	:	:	…	:
BIN	5P	567	008	…	675

The image positions are generated using permutation sequences. Let B = {BI1, BI2, BI3}, this set can be arranged in 3! Ways as,

{BI1} {BI2} {BI3}

{BI1} {BI3} {BI2}

{BI2} {BI1} {BI3}

{BI2} {BI3} {BI1}

{BI3} {BI1} {BI2}

{BI3} {BI2} {BI1}

Therefore for N images N! Sequences were generated and it will be used randomly for every attempt of user registration or login.

3.1.1 User Registration Phase

In user registration phase first the user wants to create a new Image password by making a request to online banking system. The system will provide a user name and pre-kit password. Using these details the end-user selects the image password from SAPSI Protocol. After creation of image password the end-user will get the user ID for further transactions. It is represented in the flow diagram Figure 2.

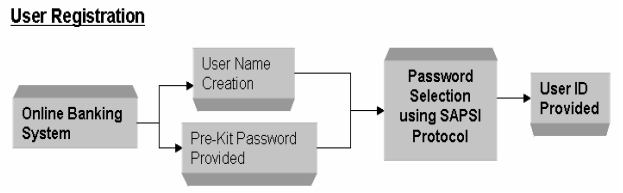
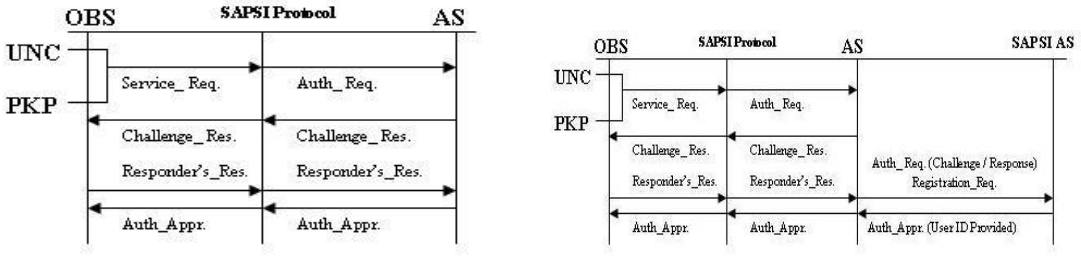


Figure 2. User Registration in Online Banking System

If the user chooses eight images as the Image password from 8 x 8 Graphical Image Pattern matrix, he / she has to confirm the password from the 2nd set of Image patterns and index numbers. This makes the end-user to get proficient with the Image patterns.



(a) (b)

OBS: Online Banking System, UNC: User Name Created, PKP: Pre-Kit Password, AS: Authentication Server, SAPSI AS: Secured Authentication Protocol System using Images Authentication Server

Figure 3. (a). OBS makes a request to AS using SAPSI Protocol (b) OBS makes a request to SAPSI AS for User Registration

User gets the online bank user name along with pre-kit password from the bank in person. With these details now the user makes a service request to AS and AS responded to that request as challenge response. According to the challenge response user will provide the response and also confirm the response. After getting confirmation from user side the registration request made for user authentication is approved from the SAPSI AS and user ID is provided. Timing sequence is represented in Figure 3.

User password chosen using SAPSI protocol is encrypted at the time of registration using MD5 (one way hash function). An encrypted password will be stored in the database server for validation.

3.1.2 User Login Phase

Users get their login by providing the user ID into the OBS and gets authentication using SAPSI protocol. If the user provides valid user ID and password then the user gets authenticated otherwise denied. The flow diagram represented in Figure 4.

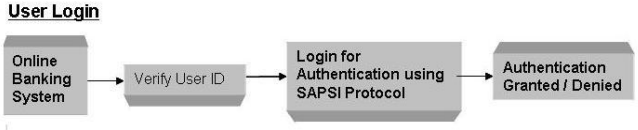
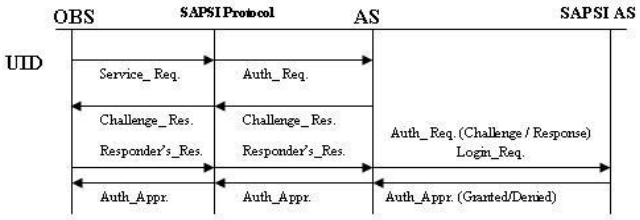


Figure 4. User Login in Online Banking System

User gets authenticated in login phase, by issuing the user ID to the OBS and makes a service request to SAPSI protocol. Now AS issue the challenge response to OBS and gets the response from user. Using the password chosen by SAPSI protocol authentication request made to SAPSI AS. Authentication approval being issued to user by providing valid password otherwise authentication request was denied.

Timing sequence is symbolized in Figure 5.



UID: User Identification

Figure 5. OBS makes a request to SAPSI AS for user login

The encrypted password using SAPSI protocol during registration phase was verified with the encrypted (same MD5 algorithm) password during login phase. If both the encrypted values are same then authentication will be provided to the end-users.

3.2 ATM User Authentication

The precise nature of ATM user authentication deals with trouble-free way of entering secret code by choosing images as password. Normally the end-users try to bring to mind and enter the secret code in ATM's; this could be avoided due to screening the secret code in the form of images. Every end-user easily enters their passwords by screening the images on the ATM screen. This makes any kind of end-users not to forget passwords at any moments, because images or pictures make human beings in better commemoration.

3.2.1 User Registration Phase

In ATM user registration, user makes a request to ATM system to get the PIN number. The PIN number provided by the ATM system to end-user and user has to choose their password using SAPSI protocol. It is represented in Figure 6.

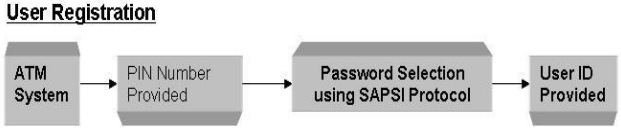
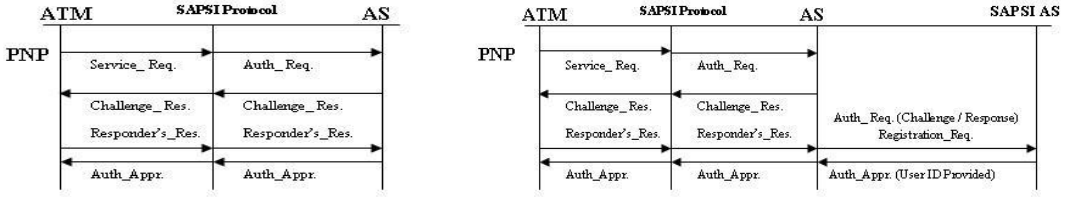


Figure 6. User Registration in ATM System

After getting the password from the system user ID is provided to the end-users.



(a) (b)

ATM: Automatic Teller Machine PNP: PIN Number Provided

Figure 7. (a) ATM makes a request to AS using SAPSI Protocol. (b) ATM makes a request to SAPSI AS for User Registration.

After getting the PIN number from the bank in person end-user makes a service request to the ATM system to acquire the image password from the SAPSI protocol. Challenge response issued to the user from AS and get the response from user. Then user makes an authentication request to SAPSI AS and enters the

text password as images. According to the confirmed registration request made to SAPSI AS, user ID is provided to the end-users. Timing sequence is represented in Figure 7.

User password chosen by the end-users is encrypted using MD5 (one way hash function) algorithm and stored in the database server.

3.2.2 User Login Phase

In ATM system user login is get through SAPSI protocol. End-user has to give PIN password to enter into the authentication system and using SAPSI protocol, authentication is granted. It is represented in Figure 8.

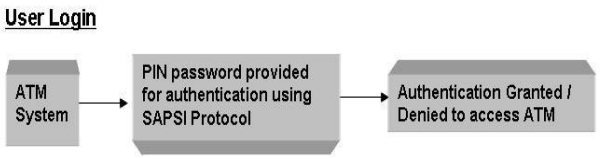
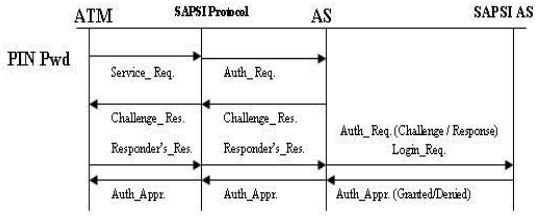


Figure 8. User Login in ATM System

If end-user provides valid user ID and password images then the user gets authenticated otherwise denied to access the ATM system.



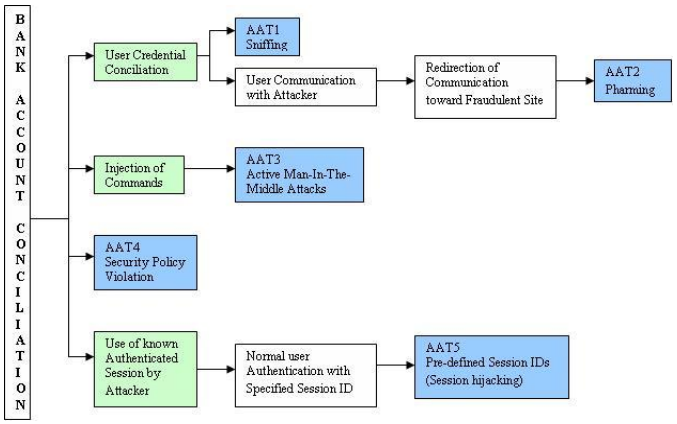
PIN Pwd: PIN Password

Figure 9. ATM System makes a request to SAPSI AS for User Login

End-user makes a service request to AS to get challenge response. After getting response from AS user make a response to SAPSI AS for login request. Then SAPSI AS makes authentication approval according to the valid password provided by the end-user otherwise authentication denied. Timing sequence symbolize in Figure 9. End-users encrypted password will be verified at the login phase according to the encrypted password stored at the time of registration.

4. Security Analysis of ATBAIBS

To implement the guidelines provided by the standards, more specific attacks and countermeasures should be studied (Christos K. Dimitriadis 2007). Analyzing the security system and its subsystems kind of attacks identified to compromise the banking system is represented in Figure 10. In this new system all the existing drawbacks are overcome with the new Text Based Authentication using Images in Banking System. Normal kind of attacks in the network security like, brute-force attack, dictionary attack, man-in-the-middle attack, shoulder surfing attack, database compromise attack and key loggers attack are conquer using SAPSI protocol.



AAT: Authentication Attack

Figure 10. Applicability of attacks identified to Compromise the Banking System.

Some of the banks web addresses were compromised for certain period of time to hack the end-users information is represented in Figure 11 (db.aa419.org web link).

Url	Site Name	Status	Date Added (down)	Updated
http://www.reservebind.com	Reserve Bank of India	active	2011-06-07 19:45	2011-06-07 19:45
http://www.reserveb-ind.com	Reserve Bank of India.	active	2011-06-07 10:02	2011-06-07 10:02
http://www.indonlinerb.in	Reserve Bank of India	dead	2011-06-07 09:23	2011-06-07 16:57
http://www.myrbionlineindia.com	Reserve Bank of India	active	2011-06-07 09:15	2011-06-07 14:53
http://www.rbind.org	Reserve Bank of India	dead	2011-06-07 03:46	2011-06-07 16:28
http://www.reservindiaonline-in.co.cc	Reserve Bank of India	dead	2011-05-30 19:01	2011-06-03 19:58
http://www.net-rbi-online.co.cc	Reserve Bank of India	dead	2011-05-30 18:58	2011-06-03 20:01
http://www.rbimbr.com	Reserve Bank of India	dead	2011-05-27 15:53	2011-06-11 15:21
http://www.rbnki-in.com	Reserve Bank of India	dead	2011-05-22 19:01	2011-06-03 20:26
http://www.rbiol-in.co.cc	Reserve Bank of India	dead	2011-05-22 08:21	2011-05-24 20:38
http://www.reserveindonline-in.co.cc	Reserve Bank of India	dead	2011-05-22 07:54	2011-05-24 20:42
http://www.rbifunds.co.cc	Reserve Bank of India	dead	2011-05-19 08:06	2011-05-20 07:58
http://www.hsbconlineb-uk.com	Reserve Bank of India	active	2011-05-15 10:29	2011-05-15 10:29
http://www.rbionlinebnk-in.com	Reserve Bank of India	active	2011-05-15 10:26	2011-05-15 10:26
http://www.rbetran.com	Reserve Bank of India	dead	2011-05-13 11:50	2011-05-22 20:41
http://www.rbinplc-in.com	Reserve Bank of India	active	2011-05-08 10:25	2011-05-08 10:25
http://www.rbiindiaplc.com	Reserve Bank of India	active	2011-05-08 10:22	2011-05-08 10:22
http://www.reservebkofindia.co.cc	Reserve Bank of India	dead	2011-05-05 17:23	2011-05-06 15:26

Figure 11. Duplicate Bank Web Addresses to hack end-users information.

The identified attacks have the target of compromising the challenge-response protocol in the banking system. The following types of attacks focuses on communication links are identified:

4.1 AAT1 attack: Sniffing

Active sniffing attacks masquerade the two communicating entities to each other (user client and the Internet banking server) to capture information, such as username and password. Passive sniffing captures information from the communication medium, without interception. This attack is not feasible in the ATBAIBS due to dynamic entry of passwords at every login attempts.

4.2 AAT2 attack: Pharming

These involve compromising domain name servers (DNSs), altering DNS tables and connecting the user to fraudulent sites, instead of the official bank's site, where information regarding the user's account may be derived. In ATBAIBS the web page was shuffled and varied every time makes the malicious users unable to associate the images and index numbers to get into the system.

4.3 AAT3 attack: Active Man-In-The-Middle Attacks

This type of attack regards a schema where the attacker receives and forwards information between the User Terminal and Internet Banking Server (IBS). The attacker sends malformed user packets or injects new traffic, such as transfer commands, from one account to another. Getting proper authentication from ATBAIBS end-user will get user ID and encrypted password using one-time hash function, which is stored in the attack confined IBS.

4.4 AAT4 attack: Security Policy Violation

Violating the bank's security policy in combination with weak access control and logging mechanisms, and employee may cause an internal security incident and expose a customer's account. Due to choice of images as password in ATBAIBS end-user remember their passwords in a fine manner. In login sessions shuffling mechanisms involved, so malicious users unable to hack end-users information from network path.

4.5 AAT5 attack: Predefined Session IDs (Session hijacking)

Attacks that force the user to connect to the IBS with a present session ID. Once the user authenticates to the server, the attacker may utilize the known session ID to send packets to the IBS, spoofing the user's identity. In ATBAIBS the IBS considered as confined, so attackers' entry towards session ID will not affect the system.

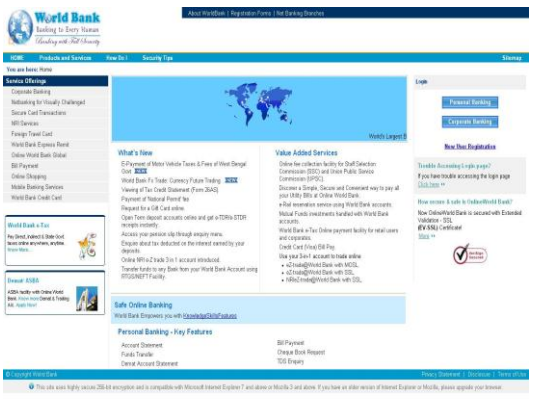
Thus ATBAIBS makes the end-users easy to enter their passwords with secured authentication. Malicious users unable to hack information of end-users from network plane due to shuffling and dynamic mechanisms involved in the system.

5. Implementation of ATBAIBS

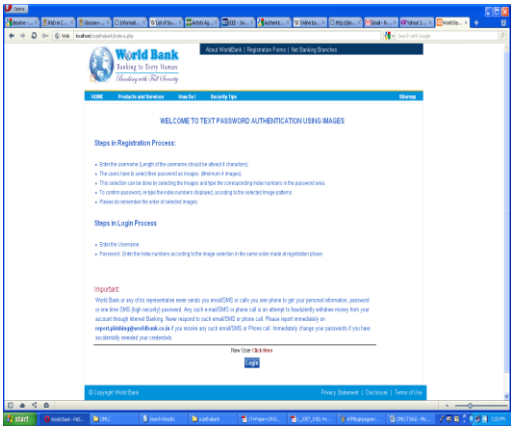
The identified attacks is used to gain a comprehensive view on the different types of attacks, the analysis of which should facilitate the process of studying the adequacy of existing countermeasures used by banks.

5.1 Online Banking System

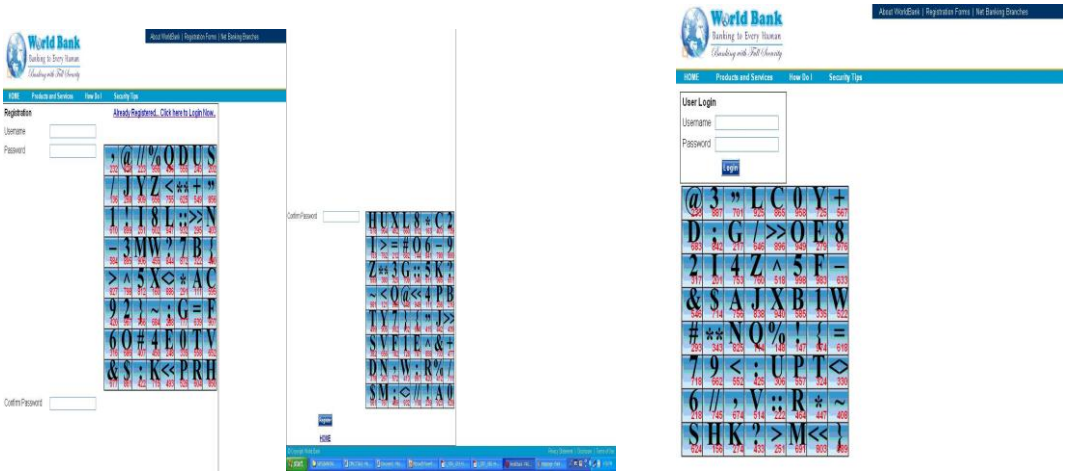
End-users getting valid data from bank to access their account have to enter into this ATBAIB System. It is implemented and represented in Figure 12.



(a)



(b)



(c) (d)

Figure 12. (a) Online Bank Home Page (b) Method of choosing the password from ATBAIB System (c) Online Banking User Registration Page (d) Online Banking User Login Page.

With the help of bank account information end-users get their authentication using ATBAIBS by following the rules of image password authentication in SAPSI protocol. End-users password information provided at the time of user registration should be confirmed with shuffled and dynamic mechanism. During login time again the shuffle and dynamic mechanism involved to the end-users to provide the password.

5.2 ATM System

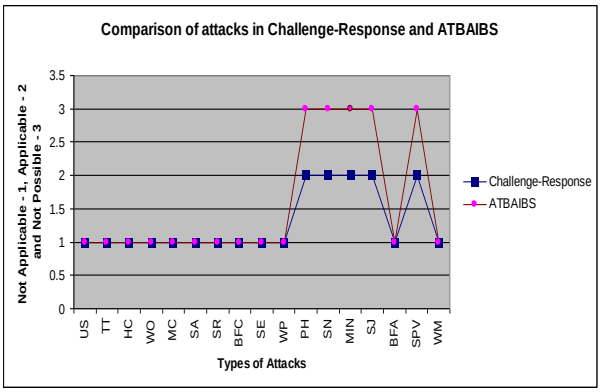
Normally end-users provide their PIN numbers in the form of numbers in the ATM System. According to the ATBAIBS end-users first provide their PIN number and enter into the system to give their text password using images. It is represented in Figure 13.

(a) (b)

Figure 13. ATM System (a) User login into the ATBAIB System (b) Shuffled and Dynamic view of ATBAIB System

In ATM System the end-user gets authenticated using the ATBAIBS method. Due to shuffling and dynamic mechanism involved every attempt of ATM System shows shuffled images with new set of index

numbers. Compared to challenge-response mechanism some of the attacks were not possible in ATBAIBS is represented in Figure 14.



Not Applicable in Challenge-Response but in other Authentication Mechanisms:

US: User Surveillance, TT: Token/notes Theft, HC: Hidden Code, WO: Worms, MC: E-mails with Malicious Code, SA: Smartcard Analyzers, SR: Smartcard Reader manipulator, BFC: Brute-force attacks with PIN Calculators, SE: Social Engineering, WP: Web Page obfuscation, BFA: Brute-Force Attacks and WM: Web site Manipulation.

Applicable of attacks in Challenge-Response and ATBAIBS:

PH: Pharming, SN: Sniffing, MIN: Active Man-In-The-Middle attacks, SJ: Session Hijacking and SPV: Security Policy Violation.

Figure 14. Comparison of Attacks in Challenge-Response and ATBAIB System.

Some of the attacks specified were not applicable in challenge-response mechanism but it comes under the authentication system. Applicability of attacks were discussed in security analysis of ATBAIBS and exemplify that, those attacks are not possible in the ATBAIBS method.

5. Conclusion

A novel method presented using ATBAIBS for banking applications. ATBAIBS is systematizing both in online and ATM banking systems. This system is more simple and easy for all kind of end-users to remember the passwords, even when the user has more number of passwords. We have shown that ATBAIBS endure all known attacks in the challenge-response mechanism. Shuffling and dynamic system involved in ATBAIBS makes the malicious users unable to hack the information from the network plane. Thus our system overcomes the problem encountered in existing systems and ensures the confidentiality and authentication in Text-Based Authentication using Images in Banking System.

References

Atul Kahate, Cryptography and network security, The Tata Mc-Graw Hill publications.

Arumugam, G. and Sujatha, R. (2010), "Secured Authentication Protocol System using Images", International Journal of Computer Science and Information Security, Vol. 8, No. 8, pp 110-116, November 2010, ISSN 1947 – 5500.

Arumugam, G. and Sujatha, R. (2011), "Secured Authentication Protocol System using Images for Mobile", International Journal of Advanced Research in Computer Science, Vol. 2, No. 3, May-June 2011, ISSN No. 0976-5697.

Bruice Schneier (2007), Applied Cryptography, Protocols, Alogrithms and Source Code in C, Second Edition, Published by JOHN WILEY and SONS, Reprint.

Christos K. Dimitriadis, (2007), "Analyzing the Security of Internet Banking Authentication Mechanisms", Information Systems Control Journal, vol. 3.

Ms Megha Jain, Ms Rashmi Tiwari, Ms Namrata Jain, (2011), "Internet banking in India: Problems and Prospects", International Journal of Advanced Research in Computer Science, Vol. 2, No. 3, May-June 2011.

Shepard, R.N., (1967), "Recognition memory for words, sentences, and pictures", Journal of verbal Learning and verbal Behavior 6, Pages 153-163.

Uppal, R.K. Rimpi Kaur, (2007), "Internet banking in India – Challenges and Opportunities", ISBN 8177081373.

Wanda Thibodeaux (2011), "Challenges of Electronic Banking", eHow Contributor, online at http://www.ehow.com/list_6603416_challenges-electronic-banking.html, accessed 11 August 2011.

William Stallings, (2006), Cryptography and network Security principles and practices, by pearson education, Inc.

Ca technologies (2011), online at http://www.arcot.com/solutions/secure-online-banking.html, accessed 08 August 2011.

Artists against 419, 100% risk free (2011), online at http://db.aa419.org/fakebankslist.php?psearch=uco+bank&Submit=GO&psearchtype, accessed 10 August 2011.

SafeNet (2011), online at http://www.esafe.com/safeword/online-banking.aspx, accessed 10 August 2011.

SyndicateBank (2011), online at https://netbanking.syndicatebank.in/netbanking, accessed 11 August 2011.

Online Banking Solutions(2011), online at http://www.onlinebankingsolutions.com/solutions/solutions.html, accessed 10 August 2011.

Internet Banking Security – Internet Banking (2011), "A guide to Internet Banking Security", online at http://webinternetbanking.com/internetbankingsecurity.html, accessed 10 August 2011.

Wikipedia (2011), "The Free Encyclopedia", online at http://en.wikipedia.org/wiki/Online_banking, accessed 11 August 2011.

Wikipedia (2011),"The Free Encyclopedia", *The list of banks in India*, online at http://en.wikipedia.org/wiki/List_of_banks_in_India#Nationalised_banks, accessed 11 August 2011.