URL ANALYSIS AND CROSS SITE SCRIPTING WITH SECURED AUTHENTICATION PROTOCOL SYSTEM IN FINANCIAL SERVICES

R. Sujatha[1] and G. Arumugam[2]

[1]Research Associate, SSE Project, Department of Computer Science,
Madurai Kamaraj University, Madurai, TamilNadu.
sujamurali72@gmail.com
[2]Professor and Head, Department of Computer Science, Madurai Kamaraj University,
Madurai, TamilNadu.
gurusamyarumugam@gmail.com

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. 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, Financial services etc. Following this necessity an approach made by URL Analysis and Cross Site Scripting with Secured Authentication Protocol System in Financial Services [URL-SAP] is presented to provide security to the end users.

KEYWORDS

URL, Authentication, Authentication Protocol, Financial Services, Security, Cross Site Scripting, Password Patterns, Random Numbers, Online Banking, URL-SAP, Internet Banking.

1. INTRODUCTION

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. 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

DOI : 10.5121/ijsptm.2012.1301

increases risk for both banks and their customers which could inhibit the growth of online banking. [1].

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 [2]. 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 [3]. To execute the guidelines provided by the standards, more precise harass and countermeasures should be considered. URL-SAP provide a formal methodology for analysing 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. URL-SAP affords security in the password system by the way of dynamic mechanism involved in it. Thus it provides network security in the network plane.

In section 2 related works are discussed with their drawbacks.

Section 3 discusses the overview of Proposed URL Analysis and Cross Site Scripting with Secured Authentication Protocol System in Financial Services.

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 and all kinds of financial services. Some of the problems were faced in the internet banking and all kinds of financial services are 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 **u**sers 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. Fear of Online Threats / Scams and Impersonal Transactions

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.

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.

2.3. 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.[4].

2.4. Network Security Fraud, Black-Listed Domain and Scripts

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.[5].
The URLs' in the email are checked with the phishing websites which are put up in the Phish Tank website (anti phishing sites are reported in this site).

If the URL in the e-mail contains any type of scripts, then the scripting part is excluded from the link.

2.5. More Number of Dots in the Web Link

Some of the web links are malicious. The web links are verified before it is being displayed to the user. If the web links present in the mail contains more than 4 dots alert is given.

2.6. Encoded, @ Symbol and Sensitive Keywords

If the web link is suspiciously encoded then it will transferred to malicious web address.
If the symbol @ is present in web link, then the control will be transferred or redirected to hacker browser.

If the URL contains keywords then it is predefined by the service providers. If the attacker wants to get information about bank details he / she may get it through similar type of keywords present in web link address as well as the terms used for the financial websites.

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. Therefore the domestic as well as the international standards authorize the adoption of internet banking as well as the financial sectors at the earliest possible moment. To overcome the several drawbacks reported in all financial services about authentication schemes in lieu of the traditional password based system, a method is proposed as URL Analysis and Cross Site Scripting with Secured Authentication Protocol System in Financial Services.

3. URL ANALYSIS AND CROSS SITE SCRIPTING WITH SECURED AUTHENTICATION PROTOCOL SYSTEM IN FINANCIAL SERVICES

This system involves the use of authentication mechanism and a URL analysis that minimizes the hacking by the attackers. In URL-SAP, an ATBAIBS [6] system is used for authenticating the Online users.

The core conceive of URL-SAP is that, 'Instead of remembering a sequence of characters as password, users have to remember a sequence of patterns as their password'.

Normally the users practiced with password system as the easy access for authentication. But considering the security in the password system, more kind of techniques, tools, methodologies etc. were used to hack and break the design involved in the system. To perceive security as the most needed one this dynamic nature mechanism of URL-SAP provides the same to the authentication process.

3.1. Authentication Process using ATBAIBS

Whenever the user wants to access the secured authentication protocol system, the URL-SAP displays an N x N matrix of cells, which is known as flexible user interface patterns. In each cell of the flexible user interface pattern a random number is displayed, that is the key used to enter the passwords. The typical 8 x 8 flexible user interface pattern is represented in Figure 1.

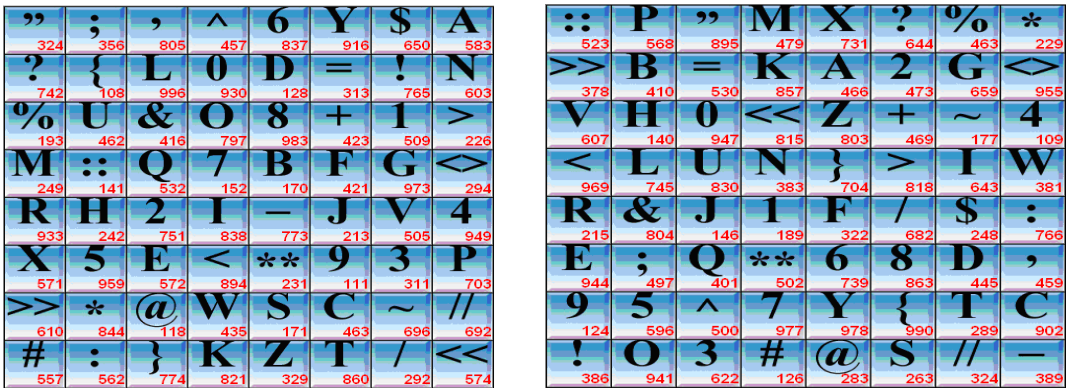


Figure 1.a Figure 1.b

Figure 1: 1.a) A Typical 8 x 8 ATBAIBS is represented 1.b) ATBAIBS in shuffled view.

For providing password the user has to enter the random numbers provided at the flexible user interface patterns. While entering random numbers in the password area, the numbers will be replaced by bullet marks. Thus entering numbers differently at every accession avoids the dictionary attack in the system. For example, if the user chooses image patterns PASS2@~* then the index numbers 703, 583, 171, 171, 751, 118, 696 and 844 should be entered in a selected order. While confirming password, flexible user interface patterns and random numbers were shuffled, so user has to re-enter the password by giving different random numbers according to the flexible user interface patterns chosen. According to the user's choice now the user has to enter 568, 466, 263, 263, 473, 283, 177, 229 as random numbers while confirming password. It is represented in Figure 1.a. Here both flexible user interface patterns and random 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 random numbers from the network plane. Using that random numbers the malicious user cannot enter into the authentication system because the malicious user will have only random numbers which should not matched with the random 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 flexible user interface patterns 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 pattern will be mapped with a corresponding number which is stored in the Image-Map table. Instead of comparing the flexible user interface patterns, 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 flexible user interface patterns. A mapping mechanism which validates the random numbers with hidden numbers is represented in Table 1.

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

Table 1: A Sample Flexible User Interface Pattern Map Mechanism for URL-SAP

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.

3.2. URL Analysis in Cross-Site Scripting

URL Analysis is used to check whether the links present in the email is malicious or not. The links are verified before it is being displayed to the user. Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. The Taxonomy of Phishing attacks were listed in Table 2.

Different types of Phishing attacks were considered and the overall solution be provided through authentication mechanism in a dynamic manner.

Medium of Attack	Setup	Type of Attacks	Target Activity
E-Mail	a)Embedded Forms b)Attachments c)URLs	a)Phisher uses Credentials b)Money Laundering	a)Login credentials b)Banking credentials
Message Boards	a)URLs	a)Malware requests / sends credentials	c)Credit card details d)Address information
Advertise-ments / Pop-ups	a)URLs	a)Urges to enter personal identity details b)Cross-Site scripting attacks	e)Personal information f)Confidential documents g)Attack Propagation
Instant Chat	a)URL b)Pre-recorded message	a)Man-in-the-middle attacks	h)Botnets

Types of Phishing attacks were illustrate as,

- ***Deceptive Phishing Attacks***

  - ✓ Phisher sends a bulk of deceptive emails which command the user to click on the link provided "Call to Action" link.
  - ✓ Phisher's call to action contains daunting information about the recipient's account.
  - ✓ Phisher then collects the confidential information given by the user.

- ***URL Obfuscation Attacks***

  - ✓ The user is made to follow a URL by sending a message which navigates them to the attacker's server. Different methods include:
  - ✓ Making few changes to the authorized URL's which makes difficult identify it as a phishing site.
    - Dotted representation of IP address URL
      - Decimal: http://202.81.255.242
      - Hexadecimal: http://0xca.0x51.0xff.0xf2
      - Octal : http://0312.0121.0377.0362

- Dot-less representation of IP address URL
  - Decimal: http://3639552355 http://7689338866...
- Valid Use of @

Malicious Use of @ to hide bogus host

  - http://www.microsoft.com@www.pisa.org.hk
  - http://www.microsoft.com@202.81.255.242 (IP address)
  - http://www.microsoft.com@3394371570 (decimal representation)

- Use domain names such as:
  - www.ebay.com.badguy.com (use of more dots)
- Use URLs with multiple redirections
  - http://www.chase.com/url.php?url="http://www.phish.com"

➢ ***Man-In-The-Middle Attacks***

✓ Attacker traces the communication between the systems.

✓ Direct the customer details to proxy server rather than the real server. It is represented in Figure 2.

Figure 2 : Man-In-The-Middle Attack Representation

✓ Phisher watches traffic changes values passed around or skims.

Counter measures to be undertaken whenever the IP addresses are considered in the Internet. URL based filtering to be made with every IP addresses. Normally the URL filtering made with the following:

✓ Dot-less representation of IP address URL – Decimal: http://3639552355 http://7689338866 ... – Hexadecimal: http://0xCA51FFF2

- Query the WHOIS Domain
- Obtain the respective URL
- Detect whether the URL is in the blacklist or validate its contents.

Phishing is prevented in validating a mail while retrieving it as:

- Content is parsed and checked for forms lifetime of the URL is checked.
- Links in the web page are checked for the presence of, Sensitive keywords, more Number of dots, Black-listed URL, Encoded, @ Symbol and Scripts.

Thus counter measures [8-16] are considered and the design of this URL-SAP is devised. In this system both the URL analysis and authentication to the system is provided. URL-SAP is defined to obtain the analysis results by,

- First the client / end-user have to check the URL link.
- If the given URL link is valid then next step of authentication will be proceeded.
- After getting authentication the client / end-user can enter into the derived system.

4. IMPLEMENTATION DETAILS

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 financial sectors.

Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. End-users enter into the web link using the URL. But the given URL proceed in many ways as, URL multiplexed by more number of dots, URL sent to black-listed domain, URL encoded with more text, URL redirected using @ symbol and URL encoded with Java Script (DOM based vulnerability). Thus using URL an attacker can obtain the details of Client / End-user. The process of URL implementation with various attack generation in e-mail is represented in Figure 3.

To avoid the conflict arise in this scenario the URL-SAP is designed and implemented. Now the end-users first validate the given URL and can enter into the authentication process. Only registered valid URLs will be available to enter into the system. Thus it avoids the data capturing by hackers through URL. More devise thing followed in this URL-SAP is whatever URL an end-user can get through, but in authentication process the given details cannot be attain by hacking. Because of dynamic mechanism involved in authentication process no such malicious person capture the data given by the end-users.

Figure 3.a

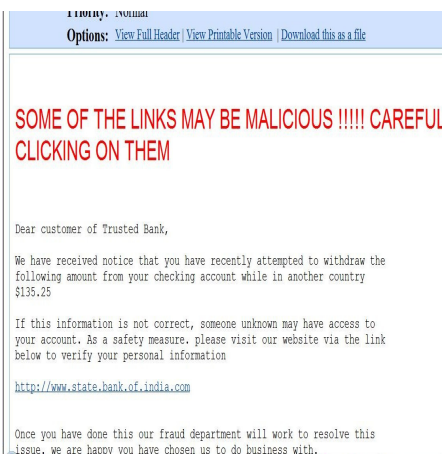


Figure 3.b

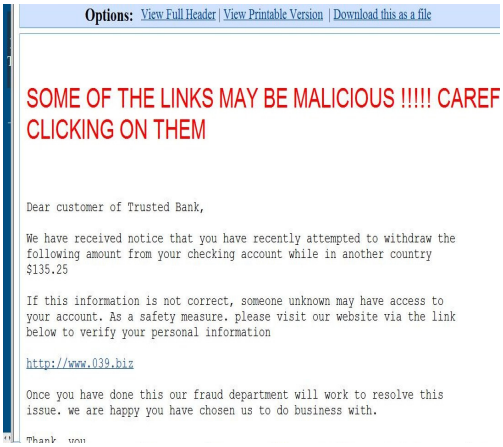


Figure 3.c

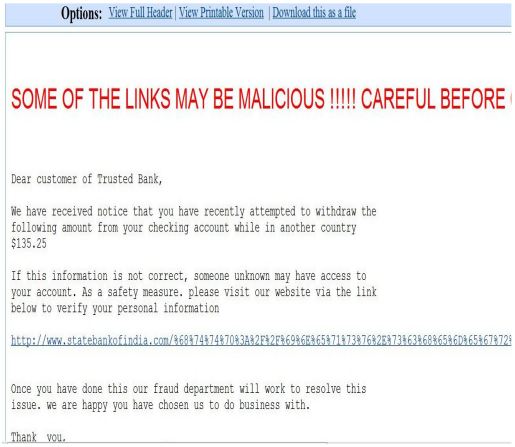


Figure 3.d

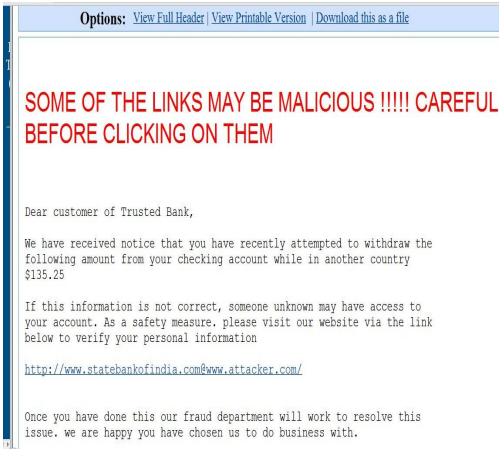


Figure 3.e

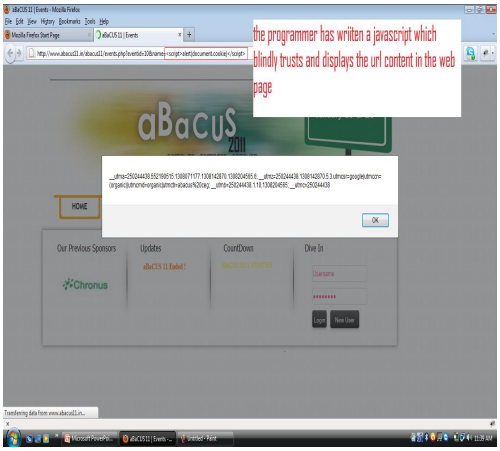


Figure 3.f

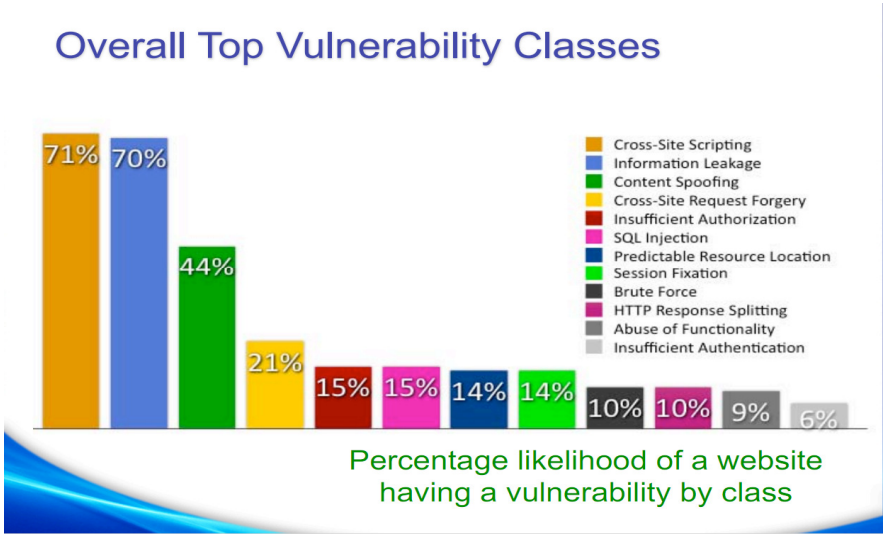
Figure 3: URL Obfuscation Attacks and Cross-Site Scripting Attacks Representation in Different Views : 3.a) Normal Mail Representation 3.b) URL with more number of dots 3.c) Black-listed URL 3.d) Encoded URL 3.e) @ symbol 3.f) DOM-based vulnerabilities

URL Obfuscation attacks and Cross-Site Scripting attacks are prevented by entering the web link and able to find the given web link is original or not.

After getting proper alert message the user can get into the secured authentication protocol system. This authentication process is implemented in banking sector.

4.1. Cross-Site Scripting Attack

Cross-Site Scripting is the act of loading the attack, third-party web application from an unrelated attack site, in a manner that executes a fragment of JavaScript prepared by the attacker in the security context of the targeted domain is represented in Graph 1.



Graph 1: Overall Top Vulnerability Classes

In Graph 1, the top most vulnerability is considered and evaluated its functioning practice in the world scenario. Thus cross-site scripting possesses the top most ratios among other vulnerabilities. Hence before entering into the URL process proper authentication mechanism is required, this provides by the ATBAIB system.

4.2. DOM Based Vulnerability Attack

DOM based vulnerability attack is stand on the Cross-Site Scripting attack. DOM based vulnerabilities occur in the content processing stages performed by the client, typically in client-side JavaScript. JavaScript programs manipulate the state of a web page and populate it with dynamically computed data primarily by acting upon the DOM.

These URL Obfuscation attacks and Cross-Site Scripting attacks are the main kind of attacks in the URL analysis and are to be overcome with the help of URL validation and dynamic system involved.

The process of getting into the URL-SAP is as follows: End-users should access the bank account through the ATBAIB System. End-users first register their details and have to get the 10-digit Identification Number. Along with this 10-digit Identification Number the end-user has to enter the web link for verification. If the given web link is valid then end-user can enter into the authentication system otherwise he/she have to try for right web link. The process of web link validation and authentication system is implemented in banking sector and is represented in Figure 4.

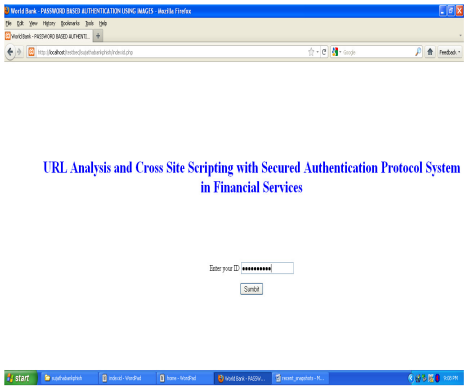


Figure 4.a

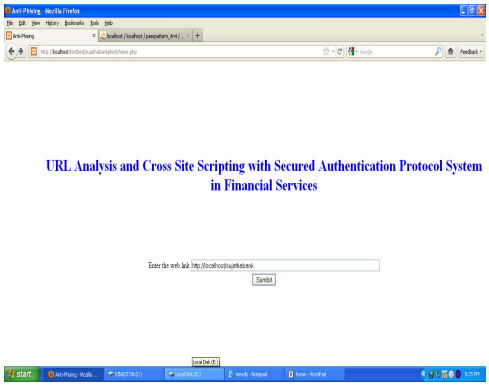


Figure 4.b

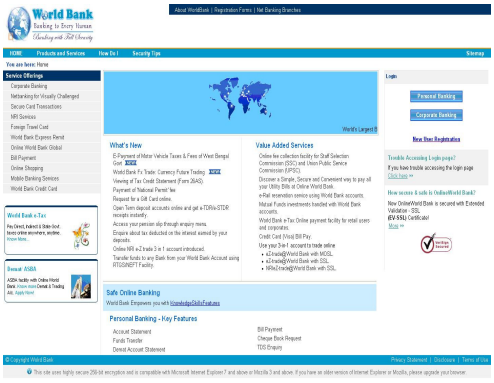


Figure 4.c

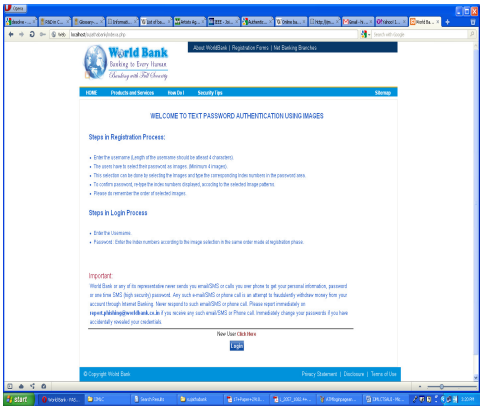


Figure 4.d

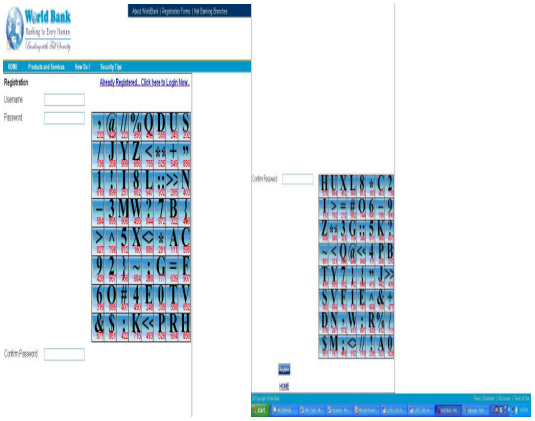


Figure 4.e

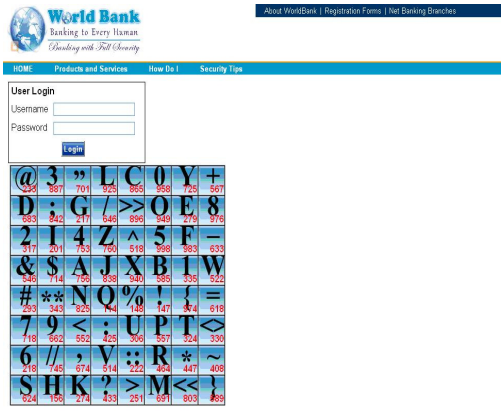


Figure 4.f

Figure 4: URL-SAP Implementation Details: 4.a) URL-SAP Home page with Client / End-user Identification Number 4.b) URL Link verification web page 4.c) Online Bank Home Page 4.d) Method of choosing the password from URL-SAP System 4.e) Online Banking User Registration Page 4.f) Online Banking User Login Page.

URL-SAP is the system provided to end-users to protect their data and to communicate in a secured manner. This gives the full optimism to transact their valid data from one place to another place.

5. CONCLUSIONS

A novel method presented using URL-SAP for financial services. URL-SAP is systematizing both in online and individual 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 URL-SAP endure all known attacks in the challenge-response mechanism. Shuffling and dynamic system involved in URL-SAP 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 URL Analysis and Cross-Site Scripting Secured Authentication Protocol System in Financial Services.

ACKNOWLEDGEMENTS

This paper is part of SSE Project funded through a National Technical Research Organization, New Delhi and is gratefully acknowledged.

REFERENCES

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

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

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

[4] 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.

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

[6] R. Sujatha and G. Arumugam (2011), "An Analysis of Text-Based Authentication using Images in Banking System", IISTE – Computer Engineering and Intelligent Systems, ISSN 2222 – 1719 (Paper) ISSN 2222 – 2863 (Online), Vol. 2, No. 4, 2011, www.iiste.org.

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

[8] A. Bergholz, J. H. Chang, G. Paab, F. Reichartz and S. Strobel, "Improved Phishing Detection using Model-Based Features". In Proceedings of the Conference on Email and Anti-Spam(CEAS), Mountain View, CA, Aug. 2008.

[9] I. Fette, N. Sadeh, and A. Tomasic, "Learning to Detect Phishing Emails". In Proceedings of the International World Wide Web Conference (WWW), Banff, Alberta, Canada, May 2007.

[10] S. Garera, N. Provos, M. Chew, and A. D. Rubin, "A Framework for Detection and Measurement of Phising Attacks". In Proceedings of the ACM Workshop on Rapid Malcode (WORM), Alexandria, VA, Nov. 2007.

[11] IronPort, "IronPort Web Reputation: Protect and Defend Against URL-Based Threat", IronPort White Paper, 2008.

[12] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Identifying Suspicious URLs: An Application of Large-Scale Online Learning".In Proceedings of the International Conference on Machine Learning (ICML), Montreal, Quebec, June 2009.

[13] J. Zhang, P. Porras, and J. Ullrich, "Highly Predictive Blacklisting", In Proceedings of the USENIX Security Symposium, San Jose, CA, July 2008.

[14] Y. Zhang, J. Hong, and L. Cranor, "CANTINA: A Content-Based Approach to Detecting Phishing Web Sites", In Proceedings of the International World Wide Web Conference (WWW), Banff, Alberta, Canada, May 2007.
[15] Le, A. Markopoulou, and M. Faloutsos, "Technical Report: PhishDef: URL Names Say it All", http://www.ics.uci.edu/ahhml/publications. html, also on arxiv:1009.2275, Sep 2010.
[16] OpenDNS. PhishTank. http://www.phishtank.com.

Authors

Dr. G. Arumugam received his post-graduate degree in Applied mathematics from PSG College of Technology, Coimbatore and Ph.D degree from University of Piere and Marie curie, Paris, France in 1987. He is now the Professor and Head of Computer Science department at Madurai Kamaraj University, Madurai,TamilNadu, South India. He is an active researcher in databases, data mining,Bioinformatics and mobile computing and has published more than 50 papers in International Journals and conference proceedings.Email: gurusamyarumgam@gmail.com

Ms. R. Sujatha received her post-graduate degree in Computer Science from Madurai Kamaraj University, Madurai and M.Phil degree from Alagappa University, Karaikudi. She is now working as Research Associate in a SSE Project in Department of Computer Science at Madurai Kamaraj University, Madurai, TamilNadu, India. She is a researcher in the area of Authentication and Network Security and has published papers in International Journals and presented in various workshops. Email: sujamurali72@gmail.com