ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 6, June 2018

IPS: Inkblot Password Security

[1] Monika N, [2] S Shree BN Kavitha, [3] Pallavi V Reddy

Abstract- **Many security Primitives are based on text-based passwords which can be hacked using brute force attack and dictionary attack. To overcome this problem we present a new security primitive based on graphical image authentication system using inkblot images. This type of system avoids the phishing attack. Since the user can able to understand the inkblot image which he saw during password setting is differ while login process they can able to understand this is a phishing site. To improve the system we implemented this security measure on the banking application.**

Index Terms: - IRIS, Inkblot images, Phishing attack.

I. INTRODUCTION

The new approach is straight forward and relies on a user answering a number of questions when he or she first signs up for access to a website. It begins by picking a set of simple inkblot pictures by randomly positioning different inkblot images in a small area of the screen. During the signup procedure, the user is requested to transcribe a short phrase that defines each of these pictures. Once the users return to access the site with a password, they are presented the inkblot patterns and the set phrases that define them. Their task is then to allocate the correct phrase each pattern.& quot;These are puzzles that are easy for a human to solve, but hard for a computer to solve, even if it has the random bits used to generate the puzzle& quot; They call their new test is IPS (Inkblot Password Security System). Network security is a leading link in the security chain. The three main networks Components of an E-Bank security solution include:

•Extended Access Control Lists (ACL) on routers
• IOS Firewall Feature Set (FFS)
• Secure Stateful Firewalls

Routers provide in initial line of defense against extraneous traffic entering the E-Bank network. Tight Extended ACLs are applied to the inbound interfaces to the routers. These ACLs need only to allow traffic that is relevant to the E-Bank center. Although several TCP/UDP ports may need to be permitted using ACLs, other traffic such as PING, Telnet, and FTP are not required and should be denied. No login ability to router from the 'outside' network should be allowed and one should use security technologies like SSL/Kerberos and others to secure and account for access to the router consoles. Firewalls provide a high level of stateful aware security between the front-end servers and the back-end database and application servers. Specific policies are installed to only allow communication between the front-end servers and the back-end database and application servers. Using address translation (NAT), the addresses of the back-end servers are hidden from the outside world. Only trusted stations known by the stateful firewall and authorized through a rule set to access the firewall's console. The data integrity ensures an exchange of financial and other sensitive data between the bank and the customer in authorized and protected manner. Depending on the choice of the channel for data exchange, different levels of security are to be implemented. For instance, the Web channel is mostly exposed and the highest level of protection should be applied.

The employed security models in E-Bank solution are:
• Secure Socket Layer (SSL)
• Public Key Infrastructure (PKI)
• Identity Authentication

The current mainstay for securing web transactions is the Secure Socket Layer, Or SSL. Secure Web Servers use the SSL protocol to create an encrypted communications channel between the client and server on the transport layer. SSL is a generic "pipeline" that secures data. It allows the client and the server, to negotiate cryptographic algorithms to use, provides a
protocol for them to do the negotiation ("SSLhandshake") and then exchanges data using the algorithms. Additionally, the server is authenticated to the client during the handshake.

The main steps in the SSL handshake are • To determine the set of algorithms to use for the new connection;
• Validate the server to the client and to exchange casual data to be used later for symmetric cipher keys, using the asymmetric cipher that was negotiated in previous step;
• Start sending data encrypted in the symmetric cipher..

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 6, June 2018

II. LITERATURE REVIEW

USABLE SECURITY AND E-BANKING: EASE OF USE VIS-À-VIS SECURITY

Electronic banking should be safe and informal to use. An assessment of six Danish web-based electronic banking systems designates that the systems have thoughtful weaknesses with respect to comfort of use. Our study of the weaknesses proposes that security necessities are among their causes and that the weaknesses may in turn cause reduced security. We outlook the struggle among ease of use and security in the context of usable security, a concept that is planned to match security principles and demands against user information and inspiration. Instruction, Automation, and understanding can be recognised as different methods to practical security. Instruction is the main approach of the systems evaluated; automation relieves the user from involvement in security, as far as possible; and understanding goes beyond stepby-step instructions, to enable users to act competently and safely in situations that transcend preconceived instructions. We deliberate the pros and cons of mechanisation and considerate as another methods to the design of web-based e-banking systems.

E-BANKING – DEVELOPING FUTURE WITH ADVANCED TECHNOLOGIES

Internet forces are affecting the banking sector transition more than any other financial provider group. E-Bank solution should deliver three key requirements: High Availability, Scalability and Security. End-toend security consideration includes network security, data integrity and identity authentication security. Framework architecture for multichannel B2C solution enforced by reliable Network and N-Tier architecture is proposed. The architecture is designed to fulfil the key requirements.

PASSWORD MEMORABILITY AND SECURITY: EMPIRICAL RESULTS

Many of the deficiencies of password authentication systems arise from human memory limitations. If humans didn't have to remember their passwords, a maximally secure password would have maximum entropy: it would consist of a string as long as the system allows with characters selected from those the system permits in a manner that provides no redundancy—that is, totally random selection. These requirements run contrary to the properties of human memory, however. Human memory for sequences of items is temporally limited, with a short-term capacity of around seven plus or minus two items. In addition, when humans do remember a sequence of items, those items must be familiar chunks such as words or familiar symbols. Finally, human memory thrives on redundancy we're much better at remembering information we can encode in multiple ways. Password authentication therefore involves a tradeoff. Some passwords are easy to remember (for example, single words in a user's native language), but also easy to guess through dictionary searches. Other passwords are secure against guessing but difficult to remember. In this case, human limitations can compromise the password's security because the user might keep an insecure written record of it or resort to insecure backup authentication procedures after forgetting it. This doesn't mean we accept the common doctrine that writing passwords down is always wrong. If your machine isn't in a publicly accessible area, writing down a long, random boot password and taping it to the machine can be worthwhile because you can then have a strict policy against disclosing passwords over the phone.

INTRODUCTION TO SYSTEM ANALYSIS

System.

A system is an orderly group of interdependent components connected together according to a strategy to realize a detailed objective. Its main characteristics are organization, interaction, interdependence, integration and a central objective.

System Analysis

System analysis and design are the application of the system approach to problem solving generally using computers. To reconstruct a system the analyst must consider its elements output and inputs, processors, controls, feedback and environment.

Analysis

Analysis is a detailed study of the various operations performed by a system and their relationships within and outside of the system. One feature of exploration is major the restrictions of the system and determining whether or not an applicant system must consider other connected systems. During analysis data are collected on the available files decision points and transactions handled by the present system. This involves gathering information and using structured tools for analysis.

EXISTING SYSTEMS

• At present the security system is CAPTCHA-Completely Automated Public Turing test to tell Computers and Human Apart.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 6, June 2018

• It is a computer program or system intended to distinguish human from machine input, typically s a way of thwarting spam and automated extraction of data from websites.
• It is a type of challenge response test used in computing to determine whether or not the user is human.
• But it is also less secured. Disadvantages of existing system:
• It is unable to prevent spam completely
• It is less secured and easily can be attacked by:
• Brute force attack

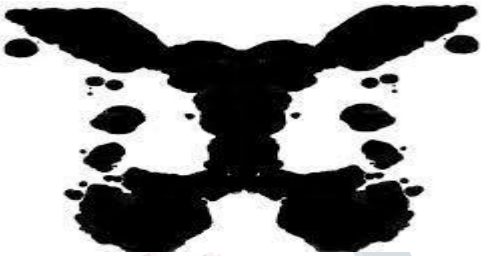

Figure 1: Inkblot image

PROPOSED SYSTEM:

• Now to overcome those problems of captcha we introduce a system called IPS(IPS - Inkblot Password Security)
• It is a graphical password authentication scheme; here we make use of images instead of numbers and text.
• Like CAPTCHA, IPS aims to stymie hackers and trolls by adding a step that's easy for human but difficult for a computer.
• The inkblot pictures.
• The image will be saved previously in the data base
• While creating the account each image is saved with different name and while registering in to the account the users are asked to give the description about the pictures
• Next time when they want to login then they are asked to give the same description what they gave while registration.
• If those descriptions match then only users can able to login otherwise they cannot login to the account.

SYSTEM ARCHITECTURE

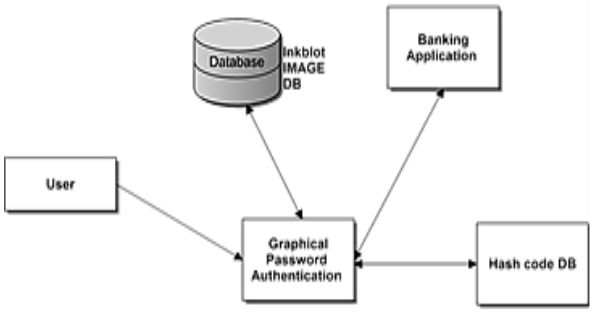

Figure 2: System architecture

SYSTEM DESIGN

Design for WebApps encompasses technical and non-technical activities. The appearance and feel of content is established as part of graphic design; the aesthetic layout of the user interface is created as part of interface design; and the technical structure of the WebApp is modeled as part of architectural and navigational design.

Design goals – the succeeding are the scheme goals that are valid to almost every WebApp irrespective of application area, size, or difficulty. 1. Simplicity
2. Consistency
3. Identity
4. Visual appeal

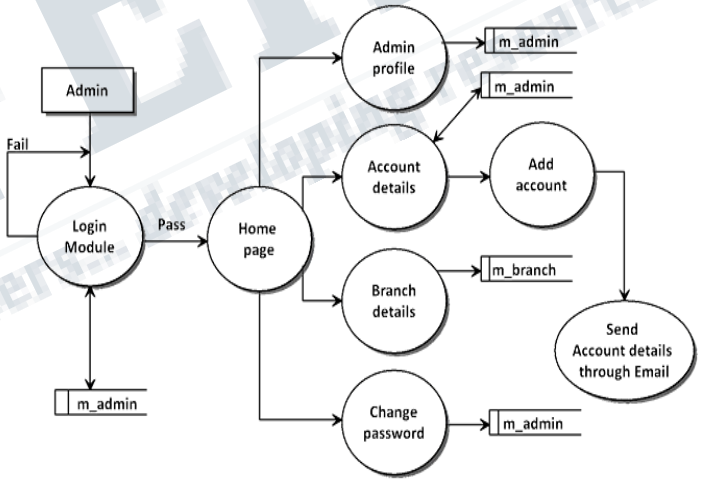

Figure 3: Admin login

DURING REGISTRATION

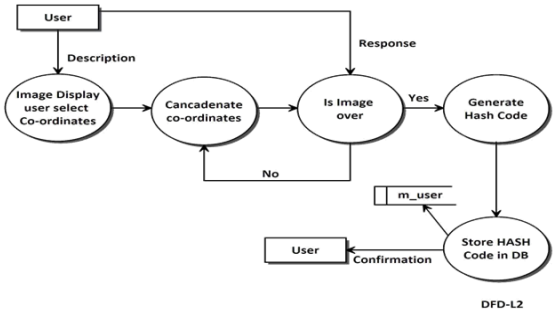

Figure 4: User registration

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 6, June 2018

DURING LOGIN

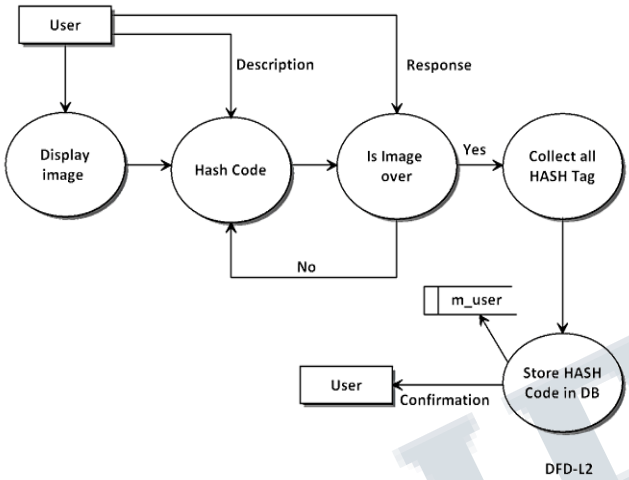

Figure 5: User login

SYSTEM REQUIREMENT

Software Requirements

- Operating system: Windows XP / 7
- Coding Language: Java (Jdk 1.7)
- Web Technology: Servlet, JSP
- Web Server: Tomcat 6.0
- IDE: Eclipse Galileo
- Database: My-SQL 5.0
- UGI for DB: SQLyog
- JDBC Connection: Type 4

III. CONCLUSION

In this paper, we presented and analysed inkblot, a simple, highly scalable and strong authentication system, which is simple enough for users to use and strong enough to keep malicious users away. Its strength lies in its simplicity and unique perception of each individual. This work contributes design and evaluation of a new graphical password authentication system that extends the challengeresponse paradigm to resist various active and passive attacks. We designed and tested a prototype of inkblot.

REFERENCE

[1] Adams, A., Sasse, M.A., and Lunt, P. (1997) "Making passwords secure and usable" in People and Computers XII: Proceedings of HCI'97, Springer, Berlin, pp. 1-19.

[2] Beyer, H., and Holtzblatt, K. (1998) Contextual Design: Defining Customer Centered Systems, Morgan Kaufmann, San Francisco, CA.

[3] Claessens, J., Dem, V., Cock, D.D., Preneel, B., and Vandewalle, J. (2002) on the security of todays electronic banking systems, Computers & Security, 21(3), 257-269.

[4] Dewan, R., and Seidmann, A. (eds.) (2001) Current issues in ebanking (Special section), Communications of the ACM, 44 (6), 31-57.

[5] Dourish, P., and Red miles, D. (2002) "An approach to usable security based on event monitoring and visualization" in Proceedings of the 2002 Workshop on New Security Paradigms,ACM Press, New York, pp. 75-81.

[6] Hertzum, M., Juul, N.C., Jørgensen, N., and Nørgaard, M. (2004) Usable Security and EBanking: Ease of Use vis-à-vis Security. Technical Report. URL:http://www. ruc. Dk /~nielsj/research/papers/ebanking-tr.pdf.

[7] IDC (2003) Total IT security market – including software, hardware, and services – to reach $45 billion by 2006, according to IDC (press release), IDC, Framingham, MA. Available at:www.idc.com /getdoc. jhtml?con tainerId=pr2003_01_28_085549.
Consulted: September 19, 2003.

[8] ISO 9241-11 (1998) Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) - Part 11: Guidance on Usability, International Organization for Standardization, Geneva.

[9] ISO/IEC 9126-1 (2001) Software Engineering – Product Quality – Part 1: Quality Model, International Organization for Standardization, Geneva.

[10] ITU (1991) Security 9Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800, International Telecommunication Union, Geneva.