Research Journal of

Information Technology

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 462-467, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.462.467

Secured Login System

N.R. Raajan, G. Shiva, P.V.M. Vijayabhaskar, P. Mithun and J. Peter Raj
Department of Electrical and Computer Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Corresponding Author: N.R. Raajan, Department of Electrical and Computer Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

ABSTRACT

User id and password is a key to secret certification of data and is most broadly used for safety purposes therefore it is vulnerable to attacks and this attacks steal private data, economic account credentials.etc. We generated the test template and establishes testing model of secure login and access control using encryption of login credentials. The mechanism we developed is encrypting the login credentials in another web based system which we called as Bluedot and this system is linked with the main login page. Whenever a user want to login in the main page, the user has to login in to Bluedot on selection of desired options on it will internally encrypts the login credentials of the user and displays it over the main login page, by this method no one can see login details and even if it is attacked also the third party gets only the encrypted form of user login credentials and this credentials are only valid to one time login.

Key words: Encryption algorithm, Bluedot model

INTRODUCTION

User credentials are the most frequently used type of validation on the net, but they have many usability troubles and security weaknesses. The security of user credentials depends on their uniqueness and it should be tough to guess, yet lengthy passwords can be hard to mark in mind and reenter properly. The passwords that are easiest to choose and remember tend to be susceptible to dictionary attacks, in which an invader tries to guess the password by constructing likelihood lists of words and familiar passwords (Hafizul Islam and Biswas, 2011). Altering passwords commonly helps to defy attack but makes the job of memorizing passwords even harder. Using the similar password or linked passwords at various sites compromises password concealment, yet memorizing an unusual password for each site imposes an idealistic huge on human users. Password login forms are also susceptible to phishing attacks, in which the user is fooled into entering a password at a fake site. Some of the more complicated phishing attacks (Goth, 2005) also corrupt or copy the parts of the browser's user interface to give the wrong impression about a site's true individuality. The proposed Bluedot software is being developed as a web based application. Initially user credentials are obtained and stored in a database. The user credentials includes first name, last name, user mail-id, password, mobile number, security questions etc. Each user is returned with an encrypted user name and password after registering by using blue-dot application (Gouda, 2008). The user id will be generated by automatic system (Bluedot) and password will be

chosen by a user and system is provided with a 16 digit code that user has to store and this code is divided into four sets each set consists of 4 digits. Whenever user logins into the Bluedot the system asks the user to type any 4 digits, one from each set. The one number from each set that user has type is decided by the system. This extra add on is for safe authentication of user. The encrypted data is generated by using blowfish algorithm.

If a user wishes to have a secure log-in, the user has to connect with blue dot application in a browser. Bluedot will get integrated in the same page of the website logins which the user wants to log-in. The user will type the automatic system generated user- id and password in the given field generated by Bluedot application. The blue dot application connects with the database, verifies the user credentials and sends back the website login page with original data.

The original user name and password is shared between the blue dot database and the website login. The visual data that can be seen in Bluedot and website login page will be in a encrypted version so even a person from behind or even a system is installed with keystroke software cant able to guess what the user is typing. The encrypted data will be valid for only one time login and it varies from one time to another.

STRUCTURAL DESIGN OF PLANNED SYSTEM

The structural design of the planed system is given away in above Fig. 1. The Bluedot web based system will be integrated with website login page. At first user creates a new account in the Bluedot were the user stores all website login information and gets registered with web based system. All the registered users are provided login id and password (chosen by user).When a user want to login into his account the user has to login in Bluedot and should provide all the

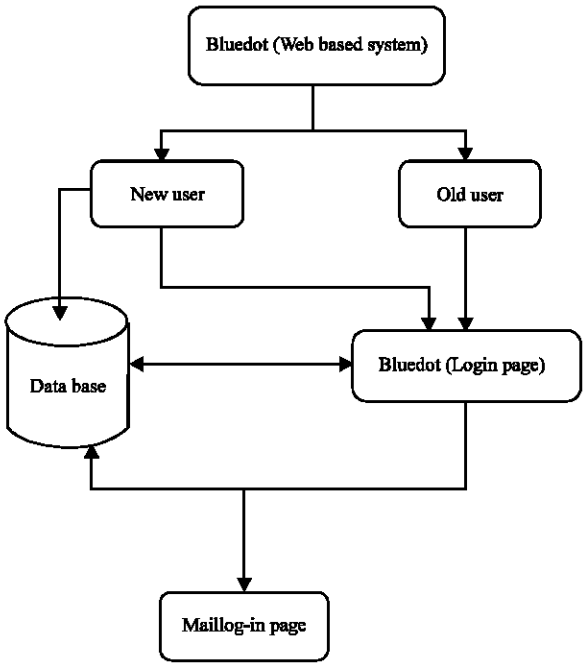

Fig. 1: Structural design of the planed system

information what the system asks. After getting all the information, when the given data matches with the database the encrypted user id and password gets displayed on website login page. The encryption is done by blowfish mechanism. It has a 64 bit block and a changeable key size from 1 bit to 448 bits. It has a 16 round Feistel cipher and uses huge key-dependent S-boxes. The user can safely login into website. When the user login in into the website, at backend the encrypted details are decrypted and the user can access his account safely.

We aim to get the following:

Achieve goals:

- Develop the ease of safe log in to websites
- Work with active websites and login forms
- Allow site-by-site relocation to the change scheme
- Permit the user to change passwords for individual sites
- Let the user only have to memorize one secret

Security goals:

- Use a distinctive password for all sites
- Defend against user-chosen secrets from offline dictionary attacks
- Keep away from storing passwords in long-term storage space
- Avoid establishing a centralized dependence
- Anti attacks based on fake website login forms
- Crack the tendency of entering passwords into WebPages

ENCRYPTION ALGORITHM

Blowfish was deliberate by Schneier (1994) as a fast, free substitute to existing encryption algorithms. Blowfish is license-free and is accessible free for all use. Blowfish is a symmetric block cipher which is used for encryption and safeguarding of data. Blowfish takes a variable-length key, which varies from 32 bits to 448 bits, making it ideal for securing data. Blowfish algorithm requires only about of 4KB memory. Running with a 32 bit processor can perform encryption/decryption with a message of 64 bit in roughly around aclock cycles of 12. For longer messages enhance in calculation time is in a linear way; let us consider, a 192 bit message acquires about (3×12) clocks. Then it works with keys from 32 bits to 448 bits in size. A pictorial illustration of Blowfish algorithm is shown in outline in Fig. 2 (Schneier, 1995). A 64 bit message (called as d) is classified into half's. Then perform XOR operation of 32 bits in left hand side and array of P to yield a value P', then it is going to a function F, next it should performed XOR operation to the 32 bits of right hand side message to create anew result of F'. F' is now replaced by left side and P'shifts to the right half of message and continue the process until 16 times with uninterrupted part of a P array. Then XOR of resultant P' and F' are performed with the Previous two entries in P array and again combined to make a 64 bit Cipher text. There is no successful cryptanalysis against blowfish. Although the differential attack performs against condensed round deviation; it is absolutely fruitless against 16 round blowfish.

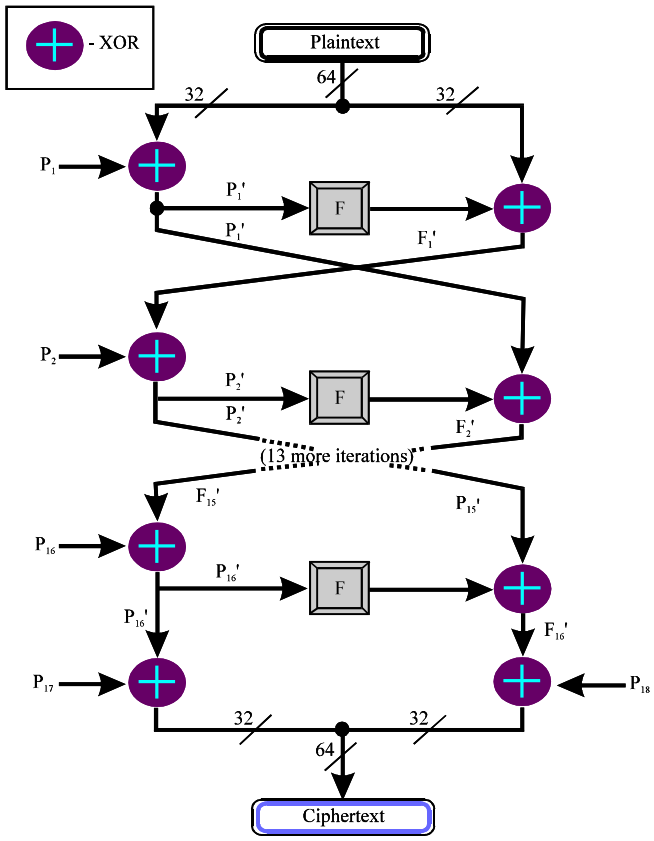

Fig. 2: Technique involved in blowfish algorithm

Blowfish encryption:

Blowfish has sixteen rounds

The input is a data element d of 64 bit as in Fig. 2

Divide x into two 32-bits of dL, dR

Then, for i = 1 to 16:

dL = dL XOR Pi

dR = F(dL) XOR dR

Exchange both dL,dR

Sub sequent to the 16th round, again exchange both dL, dR to undo the final exchange

Now, dR = dR XOR P17 and dL = dL XOR P18

At last, again combine both dL,dR to obtain the ciphertext

After logging into the Bluedot and entering the master key authentication will be done. Then key to encryption will be the master key After getting the master key the message to be encrypted will be taken from the database. Blow fish is block cipher, each element in the user credentials will be assigned to each block, the additional blocks which doesn't have any input element will be padded

BLUE DOT DEMO

Figure 3 is a graphical representation of a web based test model for secure login and access control where the Bluedot web based application is on left side which is integrated with website login page on right side. User had to enter the registered credentials which are provided by

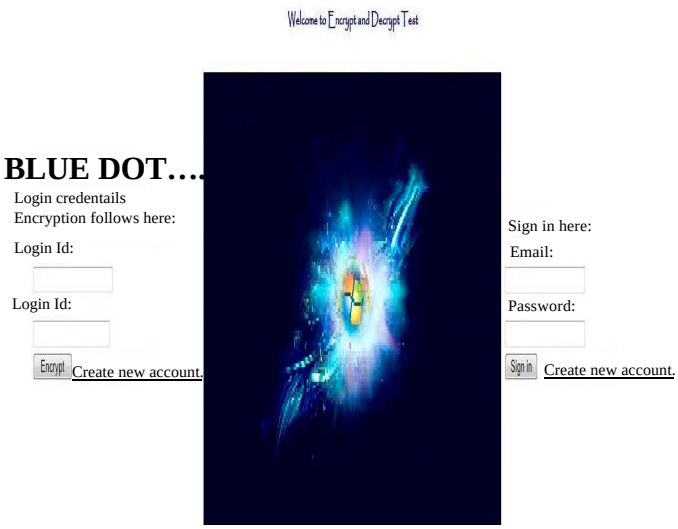

Fig. 3: Demo application

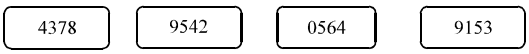

Fig. 4: Random secret key

Fig. 5: Website login page

automatic system(Liu *et al.*, 2009) on blue dot application. When the details has been accepted by the system the encrypted user id and password will be displayed on the website login page (right side).

After registering with user credentials in blue-dot, 16-bit random key is generated for the user and is notified to the user via mobile and E-mail. An example of such generated key is shown in Fig. 4.

While logging in to the blue-dot database, the user is requested to enter each number in specified position in each of the four blocks of the random secret key. The key is 16-digit number (64 bits) which is generated by pseudo random key generator (Luby, 1996; Luscher, 2002). The key which the user enters will be the key to encryption as well as decryption. A user can request a new key at any time after successfully logging in to the account with previous key. This is an extra add-on for user authentication and the feature can be enabled or disabled once the user is logged in.

In Fig. 5 we can see the website login pages where the user credentials are encrypted and it is displayed. You can observe that the password is encrypted which shown (just for demo). When a user press the sign in button these user credentials are passed into the database were these are decrypted using the master key, the resultant value will be checked in the database when it gets validated the user account of that particular user gets displayed.

CONCLUSION

We presented here web based application that helps in privacy of user login details while sharing them on an E-mail service provider. The proposed idea can be extended to other user accounts on the Internet like facebook, twitter, linked in etc. Wireless environment and Internet connection is the goal in every aspect of the technology trending now. In such an environment security and privacy plays an important role. A device connection is linked with a person by the data shared with the network. Blue dot is an application with such goals for privacy and security. It is presented as a basic idea to emphasize the need for encryption in the log-in fields.

REFERENCES

Goth, G., 2005. Phishing attacks rising, but dollar losses down. IEEE J. Secur. Privacy, 3: 7-8.

Gouda, M.G., 2008. Authentication by name or by registration. Proceedings of the 4th Workshop on Secure Network Protocols, October 19, 2008, Orlando, FL., pp: 1-2.

Hafizul Islam, S.K. and G.P. Biswas, 2011. Design of improved password authentication and update scheme based on elliptic curve cryptography. Math. Comput. Model., 10.1016/j.mcm.2011.07.001

Liu, Z., M. Huang and S. Zhu, 2009. The design and implementation of a pseudo random number generation algorithm. Comput. Intell. Nat. Comput., 2: 126-129.

Luby, M., 1996. Pseudorandomness and Cryptographic Applications. Princeton University Press, ISBN-13: 978-0691025469, New Jersey, Pages: 248.

Luscher, M., 2002. A portable high-quality random number generator for lattice field theory simulations. Comput. Phys. Commun., 79: 100-110.

Schneier, B., 1994. Description of a new variable-length key, 64-bit block cipher (Blowfish). Proceedings of the Cambridge Security Workshop, December 9-11, 1994, Cambridge, UK., pp: 191-204.

Schneier, B., 1995. The blowfish encryption algorithm-one year later. Dr. Dobb's J., 20: 137-137.