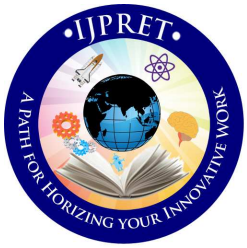
Research Article *ISSN: 2319-507X*
Sheetal Singh, IJPRET, 2013; Volume 1(8): 265-275 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURE WEB BROWSER

SHEETAL SINGH, SUMIT THAKKAR, DARSHAK SHAH, MANISH SINGH, MEDHA KULKARNI

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Browser

Secure Web Browser

Corresponding Author

Ms. Sheetal Singh

Abstract

Today's generation is engulfed by enormous presence of World Wide Web (WWW). They search, chat, shop, bank, read interesting articles, and keep in touch with their near and dear ones and do various other activities all with the help of a single browser. People are spending an increasing amount of time online and they are doing things never imagined when the web first appeared about 15 years ago. The web browser enables user to have all these features in one application. Few years ago, hacking emerged; people's accounts were no longer secure so there was a need to have a browser which also provided a secure environment to browse – a "secure web browser". A web browser or Internet browser is a software application for retrieving, presenting and traversing information resources on the World Wide Web. A Web browser is a software program that interprets the coding language of the World Wide Web in graphic form, displaying the translation rather than the coding. This allows anyone to "browse the web" by simple point and click navigation, bypassing the need to know commands used in software languages. In this report, we summarize our experiences in developing a secure web browser as desktop application. Architectures and features of various existing browsers were reviewed. For ensuring security aspect in the browser being developed, various security algorithms were studied and Triple Data Encryption Standard (TDES) algorithm was studied in detail. To prevent a user from remembering a password for each account owned by him/her, a master password facility was provided in the browser which would provide access to his/her accounts. Database stores usernames, passwords and master passwords of a user in encrypted form. Database can be copied to external device such as a pen-drive in XML form [1]. Design and implementation was done based on the paradigm of object-oriented technology using C# on dot net framework. Based on this work, we analyze the limitations, challenges and opportunities related to the web browser as an application platform. We also provide recommendations for possible future improvements.

INTRODUCTION

1.1 The ever-growing World Wide Web (WWW) and its impact

World Wide Web (www) is enormous. It finds its presence in almost all walks of human activities. Some of them are online payment of bills, online shopping, booking travelling tickets and even movie tickets online. It is also used for the vast sea of information it provides regarding any topic under the sun by students, professionals, housewives, etc.

1.2 Need of the hour – Secure and convenient web access

According to the individual requirements, some web users have multiple accounts and usually they end up struggling with a pile of passwords and face problems on securely storing and managing the passwords. Some users write

their passwords on a piece of paper or text file, which is not a secure way to store such sensitive data.

1.3 Secure Web browser comes to rescue

Our browser is developed to handle security threats arising out of above mentioned scenarios.

In the browser which we have developed, each user will have a master password. Through master password, user will be able to access all his/her accounts.

The encrypted usernames, passwords and master password may be stored in a pen-drive.

The browser has dynamic links to the database stored in the pen-drive.

When user enters master password, it is validated and accordingly access is granted to the user. For example, if the master password is tsec, its encrypted form will be something like *+!^.

Even if someone gets hold of the pen-drive having passwords, the accounts of user will not be hacked as the passwords are very well encrypted.

Decryption is very difficult as the algorithm used for encryption is not known to the intruder.

1.4 Problem Statement

To develop a secure web browser with sophisticated Graphical User Interface which can be used for normal browsing as well as for auto-login to various web-accounts? For using the auto-login facility, firstly, user will have to register on the browser through a unique master password, save the username(s) and password(s) of account(s) on his/her first visit and use pass card(s) for later visits. An authenticated user can view his/her account(s) information and delete them whenever user wants. The encrypted usernames, passwords, master password and URLs of accounts can be saved in an external hardware device like pen-drive. URLs are not encrypted and all the information is stored in XML form. Encryption is done using Triple Data Encryption Standard (TDES) algorithm. Web browser is developed in C# language using the dot net framework in Microsoft Visual Studio 2008.

1.5 Scope

Nowadays people usually have multiple accounts and have to take pains to remember one password for every account they own. The main objective of the project Secure Web Browser is to provide secure access to multiple accounts of an user through a single master password. The scope of our project can be summarized as follows:

It can be used as a normal browser just for surfing the web content.

Personal secure and convenient access to all the accounts through one master password.

Master password, usernames, passwords in encrypted form and URL(s) of accessed site(s) may be stored in pen-drive.

The data to be stored will be encrypted through Triple Data Encryption Standard (TDES) algorithm.

The browser, once installed can then be used anytime.

The setup for browser and user's data can be easily carried in a pen-drive which makes the system portable.

If need arises, a valid user can change his/her master password.

A user may delete his/her account information from the database.

User can navigate through next and previously visited web pages with the help of forward and back buttons.

2. REVIEW OF LITERATURE

2.1 Domain Explanation

Domain is a sphere of knowledge, influence, or activity. It is a set of related software systems that share common design features. The subject area to which the user applies a program is the domain of the software.

2.1.1 Networking

In information technology, networking is the construction, design, and use of a network, including the physical (cabling, hub, bridge, switch, router, and so forth), the selection and use of telecommunication protocol and computer software for using and managing the network, and the establishment of operation policies and procedures related to the network.

Our browser will access World Wide Web which is a network in itself. On the first visit of user, he/she has to create a master password, login through master password, access any website(s) and logout. The user information and accessed URL(s) may be stored in a pen-drive for convenient access in future.

Client-Server Architecture

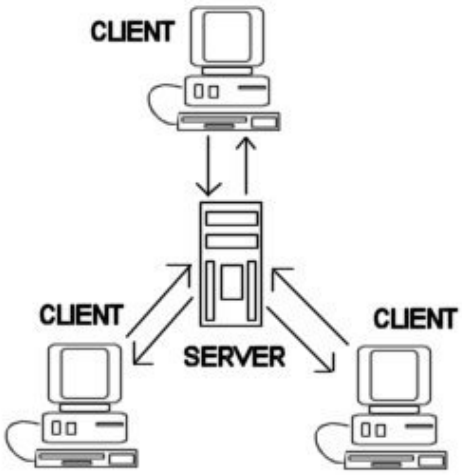


Figure 2.1 Client Server Architecture

- As shown in figure 2.1, we have implementeclient

server architecture where in the database would consist of Confidential User Information and details.

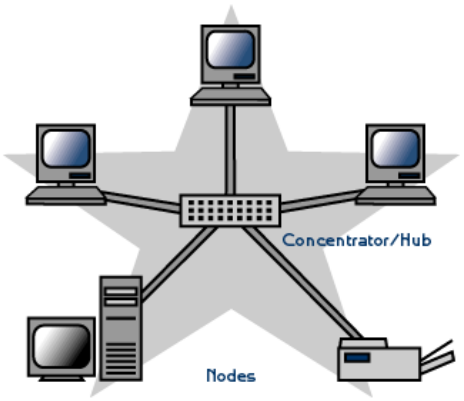


Figure 2.2 Hub network

2.1.2 Security

In present era, almost every person is web-friendly and possesses multiple web accounts for doing various activities like online payment of bills, online booking of tickets, online shopping, etc. But it is not convenient to remember a stack of passwords for accessing those accounts. If someone writes those passwords on a piece of paper or text file, the accounts may get hacked if passwords reach some evil hands. So there is a dire need of secure and convenient web access.

In our browser, the master password can be encrypted and stored in a pen-drive. The user may also save passwords for other websites and URL(s) of accessed website(s) in pen-drive. Everything will be encrypted using Triple Data Encryption Standard (TDES) algorithm and then stored in pen-drive. A valid user may change his/her master password when need arises.

2.2 State of the Current Methodology and Technology used

2.2.1 Prominent web browsers

Figure 2.3 Existing Web Browsers

Figure 2.3 shows various existing browsers like Internet Explorer, Google Chrome, Mozilla Firefox, Safari, Opera, Netscape, etc.

Web browser is software application that enables a user to display and interact with text, images, and other information typically located on a Web page at a website on the World Wide Web or a local area network.

Structure of a web page is actually not the way it is displayed in a Web browser. A web page is written in a coded form in HTML, PHP or any other language.

Web browser gets this information and formats into the display which we usually see when we visit a webpage. Because of inherent differences in browsers the displayed page might appear slightly different in different browsers.

If you wish to see how a webpage is actually written, do a right click and choose 'view source'. You will see a clutter commands and text which do not make any sense at all. The browser converts this clutter into understandable display.

Although browsers are typically used to access the World Wide Web, they can also be used to access information provided by Web servers in private networks. They can also be used to access content in file systems like eBooks etc.

Web browsers communicate with Web servers primarily using HTTP (hypertext transfer protocol) to fetch web pages. HTTP allows Web browsers to submit information to Web servers as well as fetch Web pages from them.

Web pages are located by means of a URL (uniform resource locator) which is treated as an address, beginning with HTTP access. Many browsers also support a variety of other protocols, such as FTP (file transfer protocol), RTSP (real-time streaming protocol- A protocol for use in streaming media systems), and HTTPS (an SSL encrypted version of HTTP- used to indicate a secure HTTP connection).

In addition to HTML, PHP and other languages, the Web browser also supports various image formats like JPEG, PNG and GIF. The combination of HTTP content type and URL protocol specification allows Web page designers to embed images, animations, video, sound, and streaming media into a Web page, or to make them accessible through the Web page.

Existing browsers do not provide a master password to access multiple accounts in one go. Firstly user has to login to our browser through master password and then access any web account and logout.

The provision for encrypting and storing user's data is also not provided by the existing browsers while the browser which is being developed is capable of providing above features [7].

2.2.2 DOT NET Framework

The Microsoft .NET Framework is a software framework that can be installed on computers running Microsoft Windows operating systems. It includes a large library of coded solutions to common programming problems and a virtual machine that manages the execution of programs written specifically for the framework.

2.2.4 Oracle

The Oracle Database (commonly referred to as Oracle RDBMS or simply as Oracle) is an object-relational database management system (ORDBMS) produced and marketed by Oracle Corporation. Larry Ellison and his friends, former co-workers Bob Miner and Ed Oates, started the consultancy Software Development Laboratories (SDL) in 1977. SDL developed the original version of the Oracle software. The name Oracle comes from the code name of a CIA-funded project Ellison had worked on while previously employed by Ampex.

2.3 METHODOLOGY AND TECHNOLOGY USED

2.3.1 Microsoft Visual Studio

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It can be used to develop console and graphical user interface applications along with Windows Forms applications, web sites, web applications, and web services in both native code together with managed code for all platforms supported by Microsoft Windows, Windows Mobile, Windows CE, .NET Framework, .NET Compact Framework and Microsoft

Silverlight.

2.3.2 Microsoft SQL Server

Microsoft SQL Server is a relational model database server produced by Microsoft. Its primary query languages are T-SQL and ANSI SQL. The code base for MS SQL server originated in Sybase SQL Server and was Microsoft's entry to the enterprise-level

database market, competing against Oracle, IBM and later Sybase itself.

2.3.3 C-Sharp (C#)

C# (pronounced as "see sharp") is a multi-paradigm programming language encompassing imperative, declarative, functional, generic, object-oriented (class-based), and component-oriented programming disciplines. It was developed by Microsoft within the .NET initiative and later approved as a standard by Ecma (ECMA-334) and ISO (ISO/IEC 23270). C# is one of the programming languages designed for the Common Language Infrastructure.

Its development team is led by Anders Hejlsberg. The most recent version is C# 4.0, which was released on April 12, 2010.

2.3.4 Extensible Markup Language (XML)

Extensible Markup Language (XML) is a set of rules for encoding documents in machine-readable form. It is defined in the XML 1.0 Specification produced by the W3C, and several other related specifications, all gratis open standards.

2.4 PROJECT OVERVIEW

In a nutshell, the overview of the project can be described as follows…

The browser provides an exclusive facility of master password to users. Users will just have to remember a master password to access all their accounts. On user's first visit to any web account through our browser, user will be asked "DO YOU WANT TO SAVE PASSWORD?" If user says "YES", the password's encrypted form will be stored in database. If user says "NO", the password won't be saved. But encrypted form of master password of user will be stored. The user may store URL(s) of visited web page(s) for convenient access in future. The data can be stored in pen-drive. It will be encrypted using Triple Data Encryption Standard (TDES) algorithm. For auto-login, user's master password is validated and user provides URL of account to be accessed. Accordingly user's username and password are retrieved from database or pen-drive. Thus the browser saves an user from remembering many passwords.

3 IMPLEMENTATION

3.1 Triple Data Encryption Standard (TDES) algorithm

It was found that a 56-bit key of DES is not enough to guard against brute force attacks so TDES was chosen as a simple way to enlarge the key space without a need to switch to a new algorithm.

In cryptography, Triple DES is a block cipher formed from the Data Encryption Standard (DES) cipher by using it three times [3]

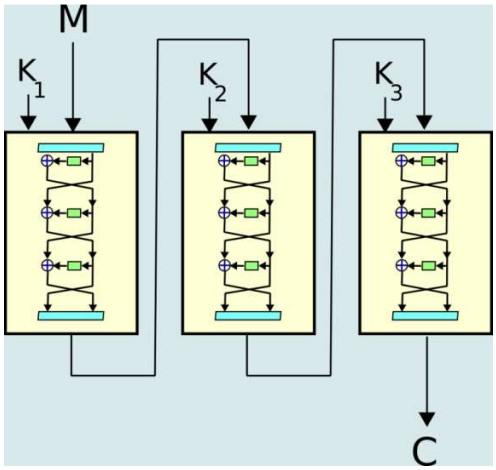


Figure 4.1 Encryption in TDES

As shown in figure 4.1, the use of three steps is essential to prevent meet-in-the-middle attacks that are effective against double DES encryption. Note that DES is not a group; if it were one; the TDES construction would be equivalent to a single DES operation and no more secure.

TDES can be operated with variations in two parameters: number of keys used and order of operations.

3.2 Order of operations

The simplest variant of TDES operates as follows:

DES (k3; DES (k2; DES (k1; M))), where M is the message block to be encrypted and k1, k2, and k3 are DES keys. This variant is commonly known as EEE because all three DES operations are encryptions.

In order to simplify interoperability between DES and TDES the middle step is usually replaced with decryption (EDE mode): DES (k3; DES-1(k2; DES (k1; M))) and so a single DES encryption with key k can be represented as TDES-EDE with k1 = k2 = k3 = k.

The choice of decryption for the middle step does not affect the security of the algorithm.

3.3 Number of keys

Since TDES has three cipher operations it allows for the use of one, two, or three keys.

The designation of the number of keys use is appended to the end of the order-of-operation notation (e.g. DES-EEE1, DES-EEE2, and DES-EEE3).

Using one key is the weakest implementation, especially if using an encrypt-decrypt-encrypt order of operation (DES-EDE1).This would effectively result in only one order of encryption since the first two operations are cancelled out, being encrypted and decrypted with the same key.

Using three distinct keys is the most secure operation and would be designated as DES-EEE3 or DES-EDE3 [3].

4 CONCLUSION

Web browsers today have progressed from being a mere internet-exploring tool to being a multi-purpose, multi-pronged application that brings several advantages to the web visitor. Our browser brings several advantages to the user. An user does not have to remember a password for every account he/she owns. Access to a web account is provided through a single master password. An user can view his/her account details. An user can add or delete account information from the database. An user can navigate to previous and next web pages. Encrypted account information can be carried securely in a pen-drive. All these things were kept in mind and then the browser was designed and implemented. This project has helped us to gain educational knowledge in terms of a new language C#.net and also helped us to learn Microsoft Visual Studio IDE.

4.1 Further Work

The browser was designed and implemented keeping in mind the current requirements of the user. But internet, as we all know is highly dynamic, so the user's requirements keep on changing all the time. So we look forward to accept challenges in terms of change of user's requirements and thereby improvise onto the work carried out so far.

Database storing master passwords and account information for multiple users on a

single machine can be implemented within the current project. With presence of multiple users on a single machine, security provisions may be upgraded. CAPTCHA can be implemented for secure registration by users.

REFERENCES

1.en.wikipedia.org/wiki/C_(programming_language)http://www.instructables.com/id/Make-a-web-browser-in-visual-basic/

2.en.wikipedia.org/wiki/Triple_DES

3.www.w3schools.com/php/php_mysql_intro.asp

4.http://www.codeproject.com/Articles/7580/Making-TripleDES-Simple-in-Visual-Basic-NET

5.www.csharp-station.com/Tutorial.aspx

6.www.referencedesigner.com/tutorials/csharp/csharp_1.phpen.wikipedia.org/wiki/.NET_Framework

7.vb.net-informations.com/framework/framework_tutorials.htm

8.www.tutorialspoint.com/java/index.htm

9.www.learnvisualstudio.net/