Secure Socket Layer (SSL) in the Network and Web Security

Roza Dastres, Mohsen Soori

World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:10, 2020

Secure Socket Layer in the Network and Web Security

Roza Dastres, Mohsen Soori

***Abstract*—**In order to electronically exchange information between network users in the web of data, different software such as outlook is presented. So, the traffic of users on a site or even the floors of a building can be decreased as a result of applying a secure and reliable data sharing software. It is essential to provide a fast, secure and reliable network system in the data sharing webs to create an advanced communication systems in the users of network. In the present research work, different encoding methods and algorithms in data sharing systems is studied in order to increase security of data sharing systems by preventing the access of hackers to the transferred data. To increase security in the networks, the possibility of textual conversation between customers of a local network is studied. Application of the encryption and decryption algorithms is studied in order to increase security in networks by preventing hackers from infiltrating. As a result, a reliable and secure communication system between members of a network can be provided by preventing additional traffic in the website environment in order to increase speed, accuracy and security in the network and web systems of data sharing.

***Keywords*—**Secure Socket Layer, Security of networks.

I. Introduction

THE software such as Outlook Software are presented in order to provide the electronically exchanging information between users in the web. The need to use this new connection reduces the traffic of users on a site or even the floors of a building. In the meantime, an example such as face, security, and reliability is very important. Security and reliability are important issues that messages are sent to the destination with the least error.

Encryption is the science of codes and codes. It is an ancient art and has been used for centuries to protect messages exchanged between commanders, spies, lovers, and others in order to keep their messages confidential. When dealing with data security, it is essential to prove the identity of the sender and receiver of the message. Also, it is necessary to make sure that the content of the message does not change in the data transferring process. These three issues, privacy, authentication, and comprehensiveness, are at the heart of modern data security and can be used for encryption.

In this paper, various encryption algorithms are presented in order to prevent hackers from infiltrating. The aim is to provide a complete and coherent defense model that can be exploited according to the organization's capabilities. Application of the Secure Socket Layer (SSL) in increasing the security of the data sharing via the web is studied and an advanced system of secured data sharing is also developed. As a result, security and reliability of the network systems can be increased in order to increase benefits of information technology in human life.

Review of research works is presented in Section II. Application of the SSL in the network and web security is presented in Section II. The developed software in the study is presented in Section IV. Finally, the obtained results are presented in Section V.

R. D. is with the Department of Computer Engineering, Cyprus International University, North Cyprus, Turkey (e-mail: roza.dastres@yahoo.com).

M. S. is with the Department of Mechanical Engineering, Eastern Mediterranean University, Famagusta, Via Mersin 10, North Cyprus, Turkey (corresponding author, e-mail: Mohsen.soori@emu.edu.tr).

II. Review of Research Works in Application of the SSL in the Network and Web Security

To provide public key certificate based authentication, secure session key establishment, and symmetric key based traffic confidentiality, on the security of Secure Socket Layer/Transport Layer Security (SSL/TLS)-enabled applications is presented by [1]. Secure communication using DNA cryptography with SSL protocol in wireless sensor networks is presented by [2] to provide a secure channel with more secure exchange of information in wireless sensor networks. To provide an advanced Network Security Processor in the webs of data, A Gbps IPSec SSL security processor design is investigated by [3]. A usability analysis of Java Secure Socket Extension API is presented by [4] to prevent the security vulnerabilities in software development applications. SSL certificate verification is investigated by [5] to verify SSL certificates using the concepts of learning automata (LA). To increase security in the data sharing systems in the networks, the most recent SSL security attacks is analyzed by [6]. Design and implementation of a high performance network security processor is presented by [7] to develop network security processors (NSPs) in data sharing systems. A combined approach to ensure data security in cloud computing is presented by [8] to increase security in data sharing networks.

III. SSL

SSL is a standard, registered technology for secure communication between a web server and an Internet browser or a mail server and a mail client (e.g., Outlook). This secure connection protects all the information that we transfer between the web server and the Internet browser (user) so that it remains confidential and intact. SSL is an industry standard and is used by millions of websites around the world to ensure data security. The SSL is a solution for secure communication between a server and a service provider, provided by Netscape. In fact, SSL is a protocol that is lower than the application layer (TCP/IP layer 4 in the TCP/IP model). The advantage of using this protocol is the use of its embedded

security features to secure insecure application layer protocols such as HTTP and HTTPS. Based on that, cryptographic algorithms are applied to plain text that is supposed to pass through an insecure communication channel such as the Internet, and ensures that data are kept confidential throughout the transmission channel. An SSL certificate is required for a website to have a secure SSL connection. The connection between the web browser and webserver using the SSL system is shown in Fig. 1 [9].

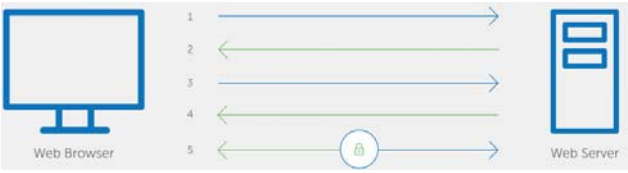

Fig. 1 The connection between the web browser and webserver using the SSL system [9]

To create security in the websites, the https security level is provided by using the server identification system. The server's public key is sent to the browser in order to secure the content of the website. Then, it is controlled by the browser to check the validation of the used certificate. So, the authentication and validation of the considered certificate is approved by the browser in order to get a feedback from the used key in the server of the website [9].

To authenticated clients and server, the SSL operates by authenticating clients and servers using digital certificates, and by encrypting/decrypting correspondence using specific keys which needs to be validated in the Cortication Authority (CA) certification center. The CA's job is to identify the parties to the relationship, the addresses, the bank accounts and the expiration date of the certificate, and to determine the identities based on them. By using the developed feature in SSL, a user is assured of the authenticity of a server.

SSL-based software on the receiving side (for example, a web browser such as Internet Explorer) of a standard key-based encryption technique and comparing the public keys of a server (such as a web service provider such as IIS) can be used in order to identify the user in the website. Then, the user can enter their information such as credit card numbers or passwords with a high level of security and reliability.

The SSL system can use a combination of symmetrical and asymmetric encryption. Symmetric key encryption is faster than public key encryption, and on the other hand, public key encryption offers more robust authentication techniques. A secured SSL connection as "SSL Handshake" is generated when the users are trying to access to the secured content in the website. The process and the generated keys in the security operations are not visible to the user. In order to encrypt all transmitted data, anything encrypted with the public key can only be decrypted with the private key, and vice versa [9].

IV. The Developed Network System

In the developed software in the study, a small sample of 2 computer conversations on the network is examined. All exchanged information between the server and the receiver will be encrypted by the developed software in the study. Then, the sent data will be decrypted on the opposite side in order to maximize confidentiality in data sending systems via the webs of data. The developed algorithm of the presented software is described in this section.

```
unit unfrmMain;
interface
uses
Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls,
forms,
  Dialogs, StdCtrls, ExtCtrls, Sockets, IdBaseComponent,
IdComponent,
  IdIPWatch, Menus, ScktComp;
type
  TfrmClientSocket = class(TForm)
    Panel1: TPanel;
    Panel2: TPanel;
    btnSendText: TButton;
    Label3: TLabel;
    edPortNo: TEdit;
    btnChangeServer: TButton;
    Panel3: TPanel;
    Memo1: TMemo;
    edSendText: TEdit;
    edHostName: TEdit;
    Label1: TLabel;
    TcpClient: TTcpClient;
    TcpServer: TTcpServer;
    procedure btnChangeServerClick(Sender: TObject;)
    procedure btnSendTextClick(Sender: TObject;)
    procedure FormShow(Sender: TObject;)
    procedure TcpServerAccept(Sender: TObject;
      ClientSocket: TCustomIpClient;)
  private
   {  Private declarations }
   Function Encode(InParam:String): String;
    function Decode(InParam:String): String;
  public
   {  Public declarations}
  End;
var
  frmClientSocket: TfrmClientSocket;
Implementation
Uses ConvUtils;
```

The main dialogue box of the developed software is shown in Fig. 2. Then, the port number of the server will be entered by the user as is shown in Fig. 3.

```
    TcpServer.LocalPort:= edPortNo.Text;
```

Then, the server will be activated.

```
    TcpServer.Active:= True;
  Finally
Show Message (The connection to the server is established.)
```

Next, the name of the server will be entered as is shown in Fig. 4. So, it will be defined that the user is connected to the server in the web.

After that, the files and text will be sent by the user as is shown in Figs. 5 and 6 respectively. The sent data will be encoded by the developed system in order to be secured in the data transferring process via the web.

```
Procedure TfrmClientSocket.TcpServerAccept (Sender:
```

TObject;ClientSocket: TCustomIpClient;)
Begin

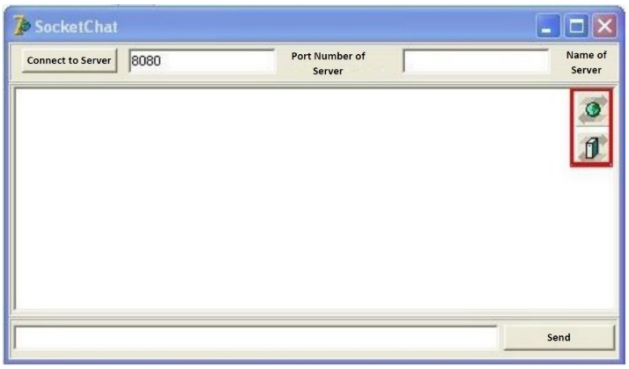

Fig. 2 The main dialogue box of the developed software

Fig. 3 The port number of the server

Fig. 4 The name of the server

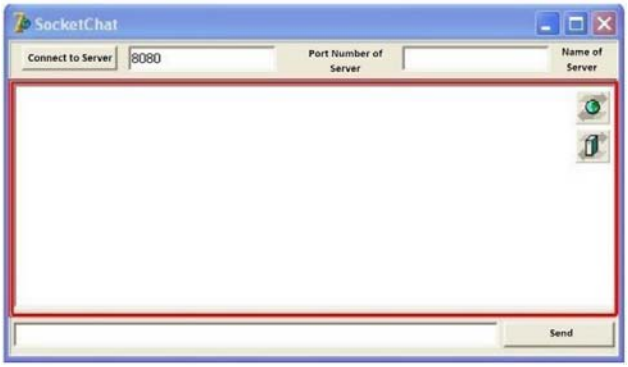

Fig. 5 File sending by the user

TcpClient.Sendln (Encode (edSendText.Text);)

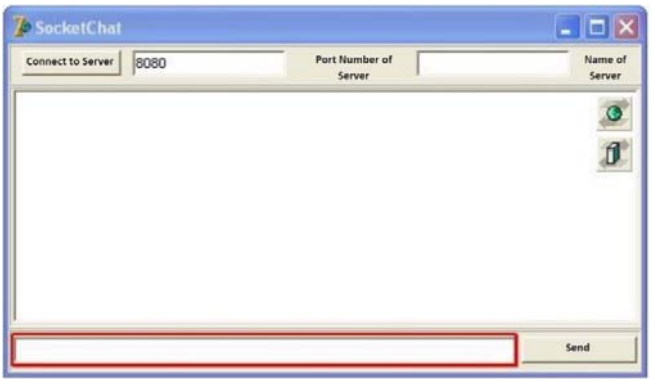

Fig. 6 Text sending by the user

Next, the user will be disconnected to the network and the field of the text sending will be cleared for the next data sending process.

```
  TcpClient.Disconnect;
edSendText.Text;:= "
 End;
End;
```

Finally, the received text by the user will be decoded by the developed system in order to be understood.

```
Function TfrmClientSocket.Encode (InParam: String): String;
Var i: Integer;
Begin
 Result: =InParam;
 For i: = 1 to length (InParam) do
  Result[i]:= chr(ord(InParam[i]) + 110;)
End;
Function TfrmClientSocket.Decode (InParam: String): Strin;
Var i: Integer;
Begin
 Result: =InParam;
 For i:= 1 to length(InParam)  do
  Result[i]:= Chr (ord (InParam[i]) – 10;)
End;
End.
```

V. Conclusion

Advanced data sharing systems are recently presented due to information exchange requirements between webs of data. In this study, various encryption algorithms is presented to prevent hackers from infiltrating. The aim of the present research work is providing a complete and coherent defense model which can be exploited according to the organization's capabilities. The developed software in the study is presented and algorithm of the system is described. By connecting between two computers, the user can consider features such as sending various files and voice calls and voicemail, etc., in addition to text conversation. So, an advanced secured communication system in the webs of data can be provided using the developed system in the study. The obtained results proved the reliability and capabilities of the developed software in the study which can be used in the internet (Like yahoo messenger software).

In designing security patterns, the fit between the user and

the security plan is very important. Moreover, the process of changing and updating security technology must be anticipated in accordance with new standards and threats.

The security system buyers are still struggling with countless security issues. Some organizations buy expensive security equipment in order to ensure their security in the web of data, which is much more than the organization's capacities. A security plan which is more than the capacity of an organization is a waste of money. Also, a security plan which is flawed will have a small impact on the organization's performance, and it is the erosion of forces time and energy. As a result, it is important to provide an advanced connection system in the web of data by considering the demands and threats in order to increase benefits of information technology in the human life.

REFERENCES

[1] M.L. Das, N. Samdaria, "On the security of SSL/TLS-enabled applications" *Appl. Comput. Inform*. 2014, 10(1-2), pp.68-81.

[2] S. Upadhyaya, "Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks" *Proced. Comput. Sci*. 2015, 70, pp.808-813.

[3] H.Wang, G. Bai, and H. Chen, "A gbps ipsec ssl security processor design and implementation in an fpga prototyping platform" *J. Signal Process. Syst*. 2010, 58(3), pp.311-324.

[4] C. Wijayarathna, N.A.G. Arachchilage, "Why Johnny can't develop a secure application? A usability analysis of Java Secure Socket Extension API" *Comput. Secur*. 2019, 80, pp.54-73.

[5] P.V Krishna, S.Misra, D. Joshi, A. Gupta and M.S. Obaidat, "Secure socket layer certificate verification: a learning automata approach" *Secur. Commun. Networ*. 2014, 7(11), pp.1712-1718.

[6] W.El-Hajj, "The most recent SSL security attacks: origins, implementation, evaluation, and suggested countermeasures" *Secur. Commun. Networ*. 2012, 5(1), pp.113-124.

[7] H. Wang, G. Bai and H. Chen, "Design and implementation of a high performance network security processor" *Int. J. Electron*. 2010, 97(3), pp.309-325.

[8] S.K. Sood, "A combined approach to ensure data security in cloud computing*" J. Networ. Comput. Appl*., 2012, 35(6), pp.1831-1838.

[9] https://www.digicert.com/ssl/