Securing Website by Secure Sockets Layer in Wireless Network using Windows Server 2008

Athraa Juhi Jani and Worood Abdalkareem Jbara

***Abstract*—Internet security is a branch of computer security specifically related to the Internet. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as hackers. Different methods have been used to protect the transfer of data, including encryption. The main goal of this paper is to establish the authenticity of website by SSL in wireless network, through applying SSL to establish encryption and identity assurance. It would create an encrypted link between a web server and a web browser. The link ensures that all data passed between the web server and browser remains private and secure.**

***Index Terms*—SSL Layer, Web security, Windows server 2008, Wireless Network**

I. Introduction

Over 700 million people, world wide banks, shops, are buying airlines tickets and perform research using World Wide Web. Privet information including names, addresses, phone numbers, credit card numbers, and passwords, are routinely transferred and stored in a variety of locations with each transaction. Billion of dollars and million of personal identities are at risk everyday. In the past, security professionals thought firewalls, patching, and privacy policies were enough to protect websites from hackers [1].

With major Web attacks taking place frequently. Secure Socket Layer (SSL) is seems to be the most secure solution. SSL is an efficient method of protecting data which is sent over a local or wide area network. It works by encrypting data sent over a network, i.e. a print job, so anyone trying to capture it will not able to read it as all the data will be encrypted. SSL can be configured on both wired and wireless networks [2]. Originally SSL was created to secure web traffic information, in specific data sent between web browsers and servers. For example, using Internet Banking when we see https:// and the little padlock in bottom right hand corner of the web browser, it means you are using SSL. After that SSL grew to work with other application such as telnet, printers and FTP software in order to become a universal solution for online security [3]. The goal of this paper is to be an easy to follow guide for establishing the authenticity of website by SSL in wireless network, through simulating a mini Internet between two laptops to implement the several transactions among website, server, and other websites.

Manuscript received August 27, 2012; revised September 24, 2012.

The authors are with Computer Science Department at Al-Mustansiriya University, Baghdad, Iraq (e-mail: athraa.jj@gmail.com,wor81@yahoo.com).

II. Related Works

Researchers turned to study ways to secure websites over networks. In [4] Sameer Verma, claimed wireless networks are not secure at the physical layer, because unauthorized users do not need access to an Ethernet jack. He proposed approach to a secure service which is based on an open source solution called NoCatAuth. This solution allows implementing a Captive Portal with traffic-shaping capabilities on wireless network.

In [5] Laura Falk examined the prevalence of user-visible security design flaws by looking at sites from 214 U.S. financial institutions, and found that 76% of the sites in our survey suffered from at least one design flaw. This indicates that these flaws are not widely understood, even by experts who are responsible for web security.

In [8] Schechter et al. shows that most users are unlikely to correctly interpret SSL security context presented by a browser as part of a decision whether to authenticate to a website. In [9] Cranor et al. shows that it can be a significant challenge to design interfaces that present P3P website privacy policies to users in a straightforward manner.

In [10] Fu et al. pointed out several common mistakes in providing client authentication services on the web. They particularly examine the design of authenticators in the web cookies that are provided to clients and find that poor design of authenticators could permit an adversary to forge authenticators for an unknown user or a selected user.

In this paper we focused on the following aspects: study the current status of internet security, and study the current status of using SSL in solving website security problems specially for web browser and server, after that we installed Windows server 2008, IIS 6.0 on one laptop and consider it as a server, and used Router for making Wireless network with another laptop, after that we designed new Website using HTML, this website can be used for library, company, bank,…etc. Then we hosted this website at remote server, this server stores the data and information important to protect from piracy. In the same time we activated the SSL protocol for establishing an encrypted link between the web server and the browser.

III. Secure Sockets Layer (SSL)

SSL can best be described as a handshake protocol and is designed to negotiate encryption keys and to authenticate the server before data is exchanged. The integrity of the transmission channel is maintained using encryption,

DOI: 10.7763/IJIEE.2013.V3.263

authentication and MACs [11]. The SSL protocol supports the use of standard key cryptographic techniques to authenticate the communicating parties to each other [3]. SSL is a set of protocols that can be divided in two layers [6]:

1) The protocol to ensure data security and integrity: this layer is composed of the SSL Record Protocol.
2) The protocols that are designed to establish an SSL connection: three protocols are used in this layer: the SSL Handshake Protocol, the SSL Change Cipher Protocol and the SSL Alert Protocol.

SSL certificates become the "passport" or the digital document which verify the security and authenticity of the interaction. The SSL certificate is installed on a web server to identify the business using it to encrypt sensitive data such as credit card information. SSL Certificates give a website the capability to communicate securely with its web customers [7]. Figure (1) illustrates SSL session (SSL Certificate interaction with the Browser and the Server).

Fig. 1. SSL session and connection.

IV. Design and Implementation of Trusted Website by SSL

Secure websites have become an integral part of our day-to-day life. People conduct both their personal and job-related business using these sites. SSL certificates keep online interactions private even though they travel across the public Internet, and they help customers gain the confidence to transact with your web site. Doing business online without SSL is like leaving customer credit card numbers on the counter or offering a dressing room without a door.

An SSL certificate is a bit of code on your web server that provides security for online communications. When a web browser contacts your secured web site, the SSL certificate enables an encrypted connection. It's kind of like sealing a letter in an envelope before sending it through the mail. SSL certificates also inspire trust because each SSL certificate contains identification information. When you request an SSL certificate, a third party verifies your organization's information and issues a unique certificate to you with that information. This is known as the authentication process. When an Internet user visits a secure web site, an SSL certificate provides identification information about the web server and establishes an encrypted connection. This process happens in a fraction of a second.

V. The Proposed System Architecture

The proposed system is designed to achieve the main aim of this project which is to establish the authenticity of website by SSL in wireless network.

1) Design New Website, the designed website in this paper is Bank website.
2) Assign IP address by DNS.
3) Authentication of Website by IIS 6.0.
4) Website Certificates by SSL.
5) Hosting Website on Server.
6) Broadcasting Website through Wireless.

All these steps are in Windows Server 2008 Environment.

A. Window Server2008

Since Windows Server 2008 support number of new security-related features such as (Wireless Security with 802.1x which provides wireless networking using Windows username/password credentials without having to use certificates and Internet Connection Firewall (ICF), used to provide a basic firewall for PCs connected to the Internet). Therefore in this system, we select Windows Server 2008 as operating system for management of computer machine.

The task of implementing server security configurations in a Windows server is threefold. First, we must understand what constitutes good security. Second, we must be able to implement security for the organization's information systems for the equipment management. Finally, we must make sure the tools and methodologies are available for quickly applying a security configuration and must understand how to use and maintain them.

B. Domain Name System

DNS is very useful and necessary in all functional active directory networks for this reason it is recommended that the server computer where DNS is installed is secured and isolated from radical change. DNS uses TCP port 53 for lookups and transfers. In this system, we must have a DNS server installed and configured for designed website for install Microsoft DNS Server use the following steps:

1) Click Start, point to Settings, and then click Control Panel.
2) Double-click Add/Remove Programs.
3) Click Add and Remove Windows Components.
4) The Windows Components Wizard starts. Click Next.
5) Click Networking Services, and then click Details.
6) Click to select the Domain Name System (DNS) check box, and then click OK.
7) Click OK to start server Setup. The DNS server and tool files are copied to your computer.
8) Continue to the next step to configure the DNS server.

C. Authentication in IIS 6.0

In this system, we can require users to provide a valid bank user account name and password before they access any information on server. This identification process is called authentication. Authentication can be set at the Web or FTP site, directory, or file level. IIS provides authentication methods to control access to Web sites and FTP sites.

We perform the following steps to install IIS 6.0 on the Windows Server 2008 computer. The machine can be a standalone server, a member server in an Active Directory domain, or even a domain controller:

1) Click Start, point to Control Panel and click Add or Remove Programs.
2) Click the Add/Remove Windows Components button in the Add or Remove Programs window.
3) On the Windows Components window, click on the Application Server entry and click the Details button.
4) On the Application Server page, click on the Internet Information Services (IIS) entry and click the Details button.
5) In the Internet Information Service (IIS) dialog box, put a checkmark in the World Wide Web Service checkbox and click OK.
6) Click OK on the Application Server dialog box.
7) Click next on the Windows Components dialog box.
8) Click Finish on the Completing the Windows Components Wizard page.

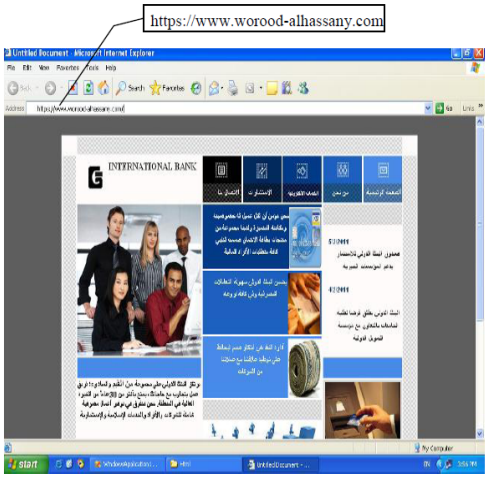

Fig. 2. Secured website by SSL.

D. Authentication and Security of Website by SSL

In this system, we use Secure Socket Layer (SSL) protocol to ensure secure transactions between web servers and browsers. The protocol uses a third party, a Certificate Authority (CA), to identify one end or both end of the transactions. This is process called *Authentication* and can implemented by the following handshake steps.

1) A browser requests a secure page (usually **https**://).
2) The web server sends its public key with its certificate.
3) The browser checks that the certificate was issued by a trusted party (usually a trusted root CA), that the certificate is still valid and that the certificate is related to the site contacted.
4) The browser then uses the public key, to encrypt a random symmetric encryption key and sends it to the server with the encrypted URL required as well as other encrypted http data.
5) The web server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt the URL and http data.
6) The web server sends back the requested html document and http data encrypted with the symmetric key.
7) The browser decrypts the http data and html document using the symmetric key and displays the information.
8) To test new settings connect, we open a browser and type website name in the address bar for example: http://www.worood-alhassany.com (See Fig. 2).

VI. Conclusion

The growth in the use of the Internet and the ongoing need for organizations to move data from point to point has created significant demand for the need to transfer data in the shortest possible time and in the most secure manner possible. The main conclusions from designing and implementation of the proposed system are:

1) The SSL is an ideal solution to the problem of authentication websites through wireless network.
2) The automatic proposed architecture can deals with people who have not skill in computer sciences.
3) The proposed system can achieve high level of information security such as credit numbers and account numbers for customers of bank.
4) Our work also shows that the current set of web security analysis and design techniques still leave significant security gaps.

References

[1] S. Garfinkel, *Web Security, Privacy and Commerce*, 2nd Edition, Publisher: O'Reilly, Pub Date: November 2001, ISBN: 0-596-00045-6.
[2] D. Akhawe and A. Barth, "Towards a Formal Foundation of Web Security," *University of California*, *2010.*
[3] M. Zawelski. (2009). Browser security handbook. [Online]. Available: http://code.google.com/p/browsersec/wiki/Main.
[4] S. Verma. (2002). Implementing Secure Services over a Wireless Network over a Wireless Network**.** [Online]. Available: http://www.opencontent.org/openpub/.
[5] L. Fal, A. Prakash, and K. Borders, "Analyzing Websites for User-Visible Security Design Flaws," *Symposium on Usable Privacy and Security (SOUPS) 2008*, July 23–25, 2008, Pittsburgh, PA USA.
[6] L. Fal, A. Prakash, and K. Borders, "Analyzing Websites for User-Visible Security Design Flaws," *Symposium on Usable Privacy and Security (SOUPS) 2008*, July 23–25, 2008, Pittsburgh, PA USA.
[7] SSL Digital Certificates. (2011). [Online]. Available: http://www.ssl.com/.
[8] S. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies," In *IEEE Symposium on Security and Privacy*, 2007.
[9] L. Cranor, P. Guduru, and M. Arjula, "User interfaces for privacy agents," *ACM Transactions on Computer Human Interaction*, vol. 12, no. 2, pp. 135–178, 2006.
[10] K. Fu, E. Sit, K. Smith, and N. Feamster, "Dos and don'ts of client authentication on the web," In *Proceedings of the 10th USENIX Security Symposium, Washington, D.C., August 2001*, An extended version is available as MIT-LCS-TR-818.
[11] Mactaggar, Murdoch. "Introduction to cryptography, Part 4: Cryptography on the Internet" March 1, 2001. URL. [Online]. Available:http://www-106.ibm.com/developerworks/library/scrypt04. Html.