IBIMA Publishing
Journal of Mobile Technologies, Knowledge and Society
http://www.ibimapublishing.com/journals/JMTKS/jmtks.html
Vol. 2009, Article ID 107112, 6 pages

A Secure Remote User Authentication System – Digital Certificates

Vimala Balakrishnan, Hossein Arabi, Siong-Hoe, Lau, and Kung Keat, Teoh

Faculty of Information Science and Technology, Multimedia University, Malaysia

Abstract

This paper presents remote user authentication mechanism by using digital certificates. Mutual authentication is used to authenticate both user and server before a secure connection is established. We present the mechanism involved in creating these certificates and how these can be used so as to be able to share and access internal resources securely from a remote location. It is believed that with the use of internally created certificates, the dependency on a third party can be eliminated, and thus costs can be saved as well. The mechanism is implemented and tested to ensure a secure connection is established between a remote user and the internal server only when both parties successfully authenticate themselves with the use of digitally signed certificates.

Keywords: remote user authentication, digital certificates, mutual authentication, secure connection

1. Introduction

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication is commonly done through the use of user logon and password in private and public computer networks. This is generally known as password-based authentication. However, the use of password logons are not considered very secure as it is much easier for a potential impostor to acquire the password by shoulder-surfing and systematic trial-and-error attacks.

It is crucial for organizations to authenticate their users in order to control and safe-guard the access to their resources. This is especially more important for a remote access, that is, when a user wishes to access his/her organization's internal server remotely. In this case, there is a need for a remote user authentication mechanism, and using a password logon is simply not going to be secure enough.

In order to verify the legitimacy of remote user login request, remote user authentication schemes are widely used. Many researchers

have proposed various authentication schemes, for example, Lamport proposed a remote user authentication scheme with password table [8]. However, it has been pointed out that once the password table was

stolen or modified, the whole authentication system will be compromised. On the contrary, another mechanism which uses smartcard without maintaining a password table has been proposed [5, 6, 14]. Many other similar schemes have been proposed to enhance the security and practicability of authentication [2, 4].

In this paper, we propose the use of internally created digital certificates to remotely authenticate the users. Digital certificates are commonly used to offer evidence in electronic form about the holder of the certificate. A digital certificate is used to associate or "bind" a person to a public key, which is contained in the certificate. Digital certificates are used in electronic commerce, where the owner of a secure site will obtain a digital certificate that's checked by a browser for a secure session. The information associated with this certificate is also used to set up an encrypted session so that others cannot see personal information like credit card numbers, PIN numbers or even passwords when they are in transit [12]. In addition, our mechanism also imposes the use of mutual authentication to further enhance the security. When a mutual authentication is used, both the

Author contact: Vimala Balakrishnan, email: vimala.balakrishnan@mmu.edu.my

user/client and the server must authenticate each other successfully before a communication or connection is allowed. Fig. 1 below depicts the mechanism for mutual authentication.

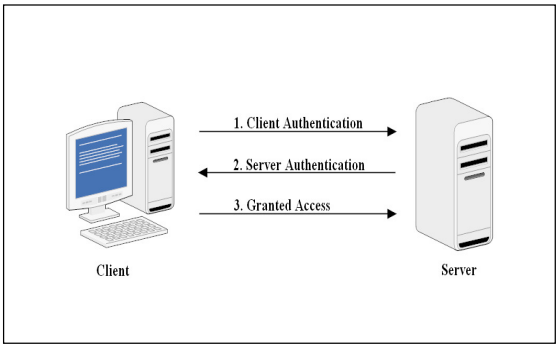

Fig.1: Mutual Authentication

The following section discusses some of the closely related work. This is then followed by a discussion on the implemented system, strength and also weakness of the system.

2. Literature Review

A remote user authentication scheme allows the authenticated user to login the remote system for accessing the services offered. As stated in the previous section, many schemes have been proposed. Password based authentication is one of the most simple and convenient authentication mechanisms over insecure networks. Unfortunately, passwords often are easily accessible to colleagues and even occasional visitors and users tend to pass their tokens to or share their passwords with their colleagues to make their work easier. Lamport proposed a remote password authentication scheme by employing a one-way hash chain; however, their scheme requires a verification table to be maintained on the remote server in order to validate the legitimacy of the requesting users. This password verification table can be easily attacked by an intruder [2].

Researchers who recognized the above-mentioned problems proposed other solutions, for example, the use of smartcards [4, 7, 10]. In a typical smartcard based authentication scheme, remote users are authenticated with their smartcards. The card receives a password as an input from the user and creates a login message from the given password. Then a message is sent to the remote server, which then checks the validity of the login message before allowing access to any services or resources. Although the use of a smartcard is more secure than password based authentication, it is to note that a card reader will be required. This would impose a problem when users are traveling away from their organization and not to mention costly as well.

Recently, some biometrics-based remote user authentication schemes have also been designed. Biometrics are automated methods of identity verification based on the principle of measurable physiological or behavioral characteristics such as a finger print, an iris pattern or a voice sample [11]. Some researchers have explored the integration of biometrics technologies with smartcards [9] and digital certificates [1]. Although the integration of biometrics and smartcards or certificates are more secure, but this combination can impose problems when users are located in a remote area. It is definitely not feasible for a user to travel while carrying a biometric sensor.

In our system, we implemented remote user authentication via digital certificates [13]. Digital certificates are commonly used on web applications, for example, online banking. However, almost all of these applications implement only one-way authentication, that is, server authentication due to issues with complexity, cost, and logistics in issuing certificates to the users, however, this creates an opening for a man-in-the-middle attack. Pursuant to this, we decided to implement mutual authentication whereby both client and server must authenticate themselves to each other. Instead of depending on a third party, we will create our own digital certificates. The users are required to bring along this certificate when they travel (saved in a disc, thumb drive etc.) or they could also access their certificates from the secure shared room (a space created to upload and download certificates). This method is not costly as no additional gadgets such as a reader is needed and it is also very convenient. The next section elaborates on our system in a more thorough manner.

3. System

We used Java Cryptography Extension (JCE) APIs to generate the digital certificates and the RSA algorithm to create public and private keys. The signature algorithm was "SHA1 with RSA Encryption" [3]. Apache Tomcat Server was used as the main server to run the JSP code and the server was configured to enable the Secure Socket Layer (SSL) and mutual authentication (kindly refer to [13] for more details on SSL Authentication).

In our system, the server plays two roles:

i. As a server to authenticate itself to user/client and also to authenticate the user/client.
ii. As a dynamic Certificate Authority (CA), that is, to issue or sign the user/client's certificate.

3.1 System Flow

In this section, we present the overall flow of the system.

Fig. 2 shows an overall view of the system, beginning with the client requesting for a digital certificate and ending at the secure site. The system flow can be categorized as follows:

Step 1: Requesting for the digital certificate

Users who wish to access the internal server would require a digital certificate that will be issued by the CA. In our system, the CA is the system administrator himself, so users will request for a certificate from the administrator. There are two possible ways for this: one is for the user to be present at the point of time when a certificate is going to be issued, and second is to make a request via a phone call. The latter takes place when a user has left the organization without getting hold of a certificate first. In this case, the administrator can ask the user some personal question (akin to credit card authentications) for authentication purpose.

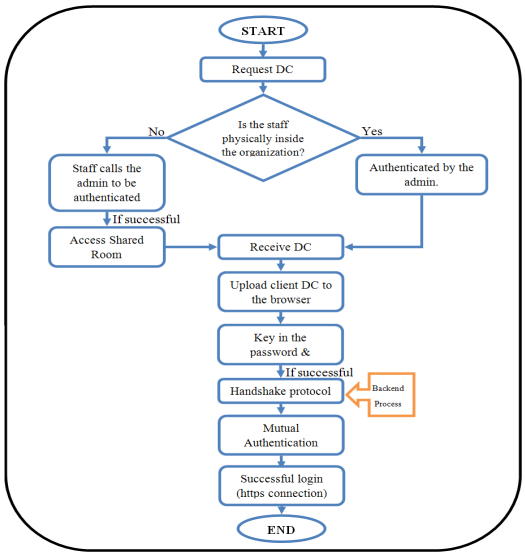

Fig. 2. System Flow

Step 2: Generating the digital certificate

When the initial authentication is successful, the administrator will proceed to generate a digital certificate for the user. This is done via our stand-alone application for certificate generation and management (see Fig. 3).

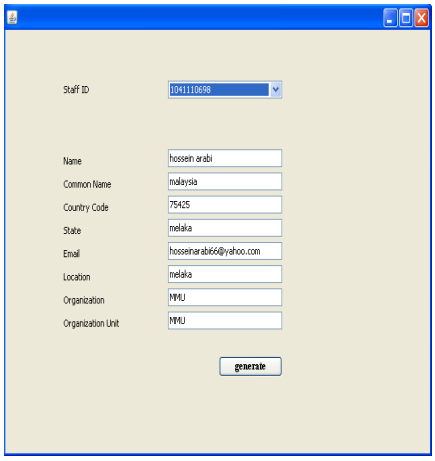

Fig. 3. Digital Certificate Generation

Upon entering all the necessary details in Fig. 3, a new certificate would be generated for the particular user (see Fig. 4).

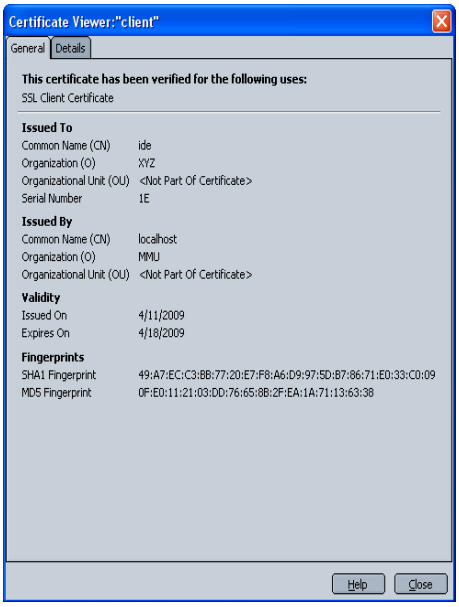

Fig. 4. A sample digital certificate

The administrator will store the digital certificate in a specific directory that it accessible by the secured shared room. The user will use his/her

password to encrypt the certificate's private key so; it is just known to the user. It is to note that in our system, the certificate actually contains a certificate chain (i.e. CA's certificate and the user's certificate) and also the user's private key.

The stand-alone application can also be used to revoke certificates, for example, when a user resigns. The following figure shows how the administrator can easily manage the certificates in the database (Fig. 5).

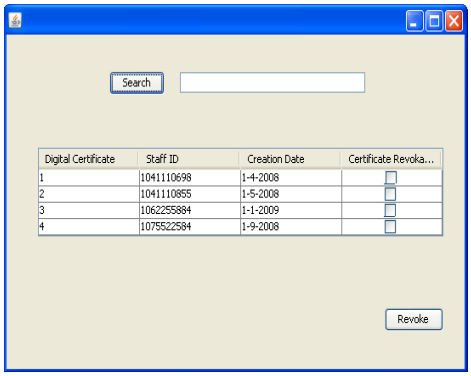

Fig. 5. Digital Certificate Revocation

Step 3: Importing/uploading the digital certificate

The digital certificate needs to be uploaded into the browser for the mutual authentication to take place. Our mechanism is tested on the Netscape browser. In order to upload the certificate, the user needs to open the certificate manager of the Netscape browser through Tools -> Options -> Advanced -> Encryption. In the "Your Certificate" section, he/she will click on the import button (see Fig. 6).

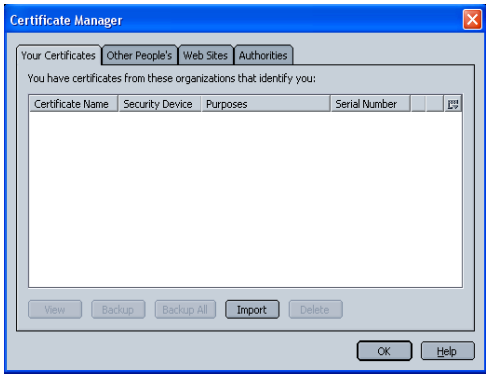

Fig. 6. Certificate Manager

When the user is prompted to select his/her certificate, another screen as in Fig. 7 below will be displayed.

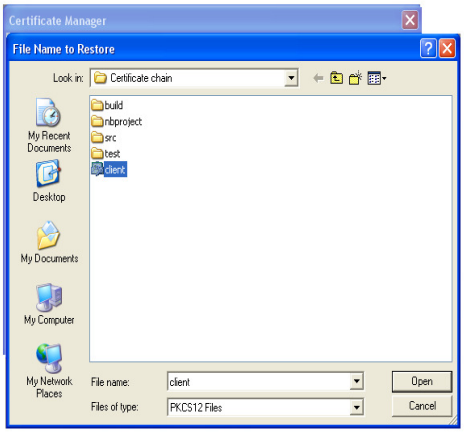

Fig. 7. Select Digital Certificate

When a certificate is selected, a password prompt will appear. This password is meant to protect the certificate that is going to be uploaded. This is necessary so that an intruder or any other third party who uses the same system will not be able to establish the secure connection even if he/she gets access to the uploaded certificate (see Fig. 8).

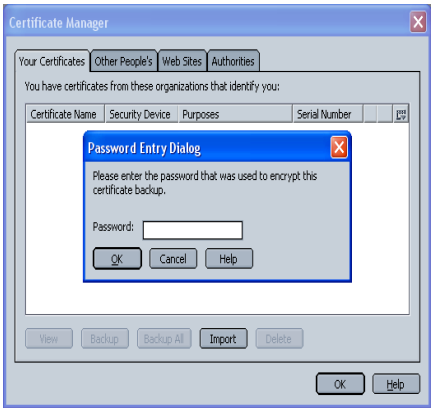

Fig. 8. First Password

Fig. 9 below shows the second password that needs to be entered, which was the initial password used to encrypt the private key of the certificate (when the certificate was generated by the CA).

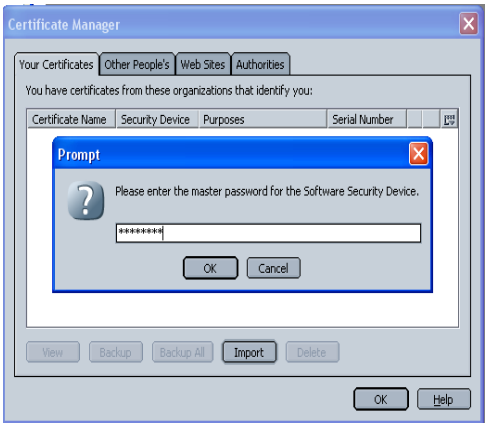

Fig. 9. Second Password

If the second password is correct and the certificate manager could decrypt the certificate successfully, the user will see the prompt that the digital certificate is successfully imported (see Fig. 10).

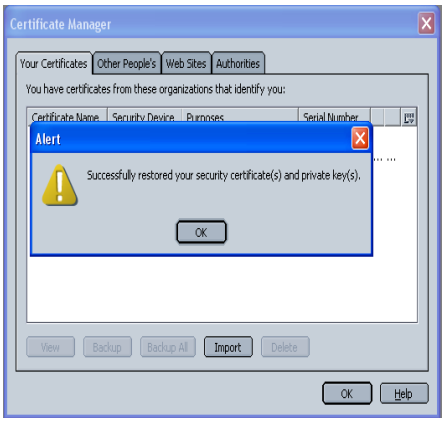

Fig. 10. Successful Importing

Step 4: Secure log in

After importing the digital certificate to the browser, the user is now able to log in to the main page. When an access to the internal server (via the website) is attempted, the system will automatically try to authenticate both the user and the server based on the certificates. If the authentication is successful, a secure connection (https) will be established as shown in Fig. 11. The information that passes between the client and server will be encrypted so, it will be immune from any third party.

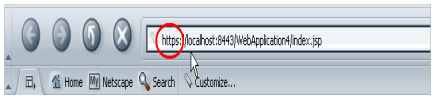

Fig. 11. Secured Website

4. Strength and Weakness

The use of self-signed digital certificates for remote user authentication is common; however, many depend on third parties, such as, Verisign. In this system, the administrator also acts as the CA, so the certificates will be self signed. This removes the dependency on a third party, and thus saves cost as well. Moreover, the number of generated certificates is not limited and it can be increased to the population of the user in an organization.

Our system is also considered safe in the sense that if an intruder gets hold of a user's certificate, he/she still will not be able to access to the internal server without knowing both the passwords as we have implemented two levels of password authentications. Moreover, in order to enhance the security, we have implemented mutual authentication and therefore both user and server must authenticate themselves to each other before a secure connection can be established.

The system is convenient as users who lose their digital certificates or forget to bring their certificates can request for a new certificate remotely and obtain it via the secured shared room. Naturally a lost certificate will be revoked by the system administrator. In addition, the system is also very easy to be used as users are only required to know how to upload their certificates into the browser for the authentication to take place.

Unlike some of the open source software, our application that generates the certificates can be implemented on any operating system, hence it is entirely portable.

It is also to emphasize that we have yet to perform a thorough security analysis on the implemented system. This, however, will be accomplished in our future work. Moreover, this implementation works only for users who belong to an organization as the aim was to provide a secure authentication mechanism for users who travel outside the organization.

5. Conclusion

We have implemented mutual authentication mechanism using digital certificates in order to remotely authenticate users. Our implementation shows that this can be done easily by generating the certificates internally without depending on a third party. Connections to the internal server can be securely established once user and server successfully authenticate themselves to each other. This enables both parties to communicate with each other securely knowing that both their identities have been verified. Our implementation is also simple, cost saving and not to mention effective as well.

6. References

[1] Bechelli, L., Bistarelli, S., Martinelli, F., Petrocchi, M., and Vaccarelli, A., Integrating Biometric Techniques with an Electronic Signature for Remote Authentication, Retrieved April 5, 2009, http://www.iat.cnr.it/attivita/progetti/progetti.html

[2] Chen, C.M., and Ku, W. C. "Stolen-verifier attack on two new strong-password authentication protocol," *IEICE Transactions on Communications*, E85-B(11), 2002, pp. 2519–2521.

[3] Hook, D., 2005, *Beginning Cryptography with Java*. John Wiley and Sons. 2005

[4] Hsu, C. L. "Security of Chien et al.'s remote user authentication scheme using smart cards, " *Computer Standards & Interfaces*, (26: 3), 2004, pp. 167–169.

[5] Hwang, M.S. and Li, L.H. "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, (46:1), 2000, pp. 28–30

[6] Ku, W.C., and Chen, S.M. "Weaknesses and improvements of an efficient password base remote user authentication scheme using smartcards," *IEEE Transactions on Consumer Electronics*, (50:1), 2004, pp. 204–206.

[7] Kumar, M. "New remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics,* (50:2), 2004, pp. 597–600.

[8] Lamport, L, Password authentication with insecure communication, Communications of the ACM 24, 1981

[9] Lee, J. K., Ryu, S. R., and Yoo, K.Y. "Fingerprint-based remote user authentication scheme using smart cards, " *Electronics Letters*, (38:2), 2002, pp. 554–555.

[10] Leung, K.C., Cheng, L.M., Fong, A.S., and Chan, C.K. "Cryptanalysis of a modified remote user authentication scheme using smart cards, " *IEEE Transactions on Consumer Electronics,* (49:4), 2003, pp. 1243–1245.

[11] Matyáš, V., and Říha, Z, "Biometric authentication – Security and Usability", Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, 2002, pp. 227 – 239, Deventer, The Netherlands.

[12] RSA Security, 2004, Digital Certificates, Retrieved April 5, 2009, from http://www.rsa.com/glossary/default.asp?id=1014

[13] SSH Communications Security, 2003, Introduction to SSH Secure Shell, Retrieved April 3, 2009, from http://www.ssh.com/support/documentation/online/ssh/adminguide/32/Introduction_to_SSH_Secure_Shell.html

[14] Sun, H.M. "An efficient remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics* (46: 4), 2000, pp. 958–961.