Combined Web/Mobile Authentication for Secure Web Access Control

Ali Al-Qayedi, Wael Adi, Ahmed Zahro
Etisalat College of Engineering
United Arab Emirates
Email: {alqayedi, adi, zahro}@ece.ac.ae

Ali Mabrouk
Lufthansa Systems
Germany
Email: ali.mabrouk@lhsystems.com

Abstract— **Previous Web access authentication systems have used either the Web or the Mobile channel individually to confirm the claimed identity of the remote user. Both approaches proved to be insecure when used in isolation. An investigation is presented into the enhanced security of a new combined Web/Mobile authentication system. The hybrid system enables strong authentication by augmenting the traditional Web-based username/password approach with a Mobile-based challenge/response authentication. Experiments show that the combined system is relatively immune to eavesdropping attacks and provides a trade-off between security and usability of the remote authentication system. The system is promising for current as well as for future 3G mobile and pervasive computing environments [1].**

Keywords-component; Authentication; access control; mobile security; J2ME

I. INTRODUCTION

Recent developments in online transactions over the Internet have given rise to significant concerns regarding the confidentiality and authenticity of those transactions. In an e-commerce transaction, a consumer typically makes a payment using a debit/credit card. The communication link between the consumer PC and the merchant server is usually protected against eavesdropping using Secure Socket Layer (SSL) [2]. Even so, a number of security threats remain. One reason for these remaining vulnerabilities is that SSL does not obligate client authentication. As a result, it is not easy to verify if the person who is making a payment is the legitimate cardholder or not. A malicious user, who may have obtained card details by some means, may then be able to use them to make payments over the Internet at the expense of the legitimate cardholder. Consequently, a way to reduce the risk of such frauds is to perform user authentication. User authentication is the task of confirming or denying a person's claimed identity. On the one hand, failure to properly authenticate a transacting party may lead to situations such as illegal transfer of funds, unauthorised ordering of goods, mischievous alteration of data, and repudiation of completed transactions. On the other hand, complex authentication systems may sacrifice the convenience of online services and turn them unusable.

Most online businesses are still conducting user authentication through the traditional username/password approach even though the method proved to be insecure mainly due to its susceptibility to brute force password guessing attacks for which the HTTP protocol in known to be vulnerable. As a result, a number of alternative authentication techniques have recently been considered such as tokens, smart cards and biometrics. Those techniques are either used individually (single-factor authentication) or in combination with other techniques (two-factor authentication). In many implementations of both approaches all authentication evidences between the client and the server are exchanged via a single communication channel, usually the Web, making it prone to eavesdropping attacks. Given the large penetration of mobile phones, some recent studies considered using the wireless mobile networks in combination with the wired Web to achieve enhanced user authentication via two different communication channels. This also adds an extra degree of freedom in accessing WWW information while on the move [1]. The remainder of this paper is organized as follows: section 2 gives an overview of the related work. Section 3 describes our combined Web/Mobile authentication approach. Section 4 presents the developed system setup and implementation. Section 5 illustrates some experimental results and discussion. Section 6 gives concluding remarks and recommendations for future improvement.

II. COMBINED WEB/MOBILE AUTHENTICATION

Researchers of the Katholieke University Leuven [3] proposed one of the combined Web/Mobile payment approaches. Their approach mainly operates as follows: (1) a customer can initiate and complete an electronic payment over the GSM network, where the network operator is an active participant. (2) The pre-payment related interaction is done via the WWW. (3) The customer receives a receipt with which he/she can pick up the goods (post-payment). This approach has some security and implementation limitations. The protocol relies on SMS messages, such messages are not real-time and can only contain 160 characters that have to be taken into consideration when defining the exact content of the protocol messages. The presented electronic payment

system seems to offer more security than today's widely used mechanisms; however, it does not really offer more privacy. Merchants know at least the mobile phone number of their Customers.

Another combined Web/Mobile approach was proposed by the Department of Mathematics at the University of London [4]. This protocol design utilises the subscriber identity authentication algorithm. In every SIM, there exists a long-term secret key Ki, which is unique and known only to the Subscriber Identity Module (SIM) card and the Authentication Center (AuC) of the subscriber's home network operator. The operator is the organization with whom the subscriber has some kind of contractual arrangement for the provision, tariffs and payment for this service.

This approach also suffers some security and implementation limitations. Prior agreement is required between the merchant and the mobile service provider to support the protocol between the AuC and the merchant server. Merchants may be charged for the AuC services. This cost therefore has to be weighed against the cost of `card not present' charge backs, which may vary from merchant to merchant. This proposal required U-SIM Toolkit to be used, which requires a U-SIM compatible Mobile Equipment (ME) and SIM card.

III. System Overview

A. Requirements and Conditions

In the proposed concept, we take the following facts into consideration:

- The user has a mobile connection. This could be a permanent one, as in the case when using General Packet Radio System (GPRS) connection. In such a connection, the charging amount depends solely on the amount of exchanged data and not on the duration of the connection.
- The whole authentication should not be accumulated on the web server. This is due to the fact that a web server is generally due to several hacking attacks which means, it is more efficient to split the authentication process of the client between the web sever and an Authentication Server offered by the network service provider. This is especially significant, if we consider the privacy of the users.
- The connection between the web user and the web server is secure. This could be achieved using SSL or a virtual private network (VPN).

B. Overview

Our combined Web/Mobile authentication system attempts to resolve some of the issues associated with the two previously mentioned systems. The main steps involved in our system are: basic authentication, challenge/response and temporary password. The system generally operates as follows:

1. **Web-Based Basic Authentication:** firstly, the user has to proof his identity to the Web server using a Web-based username/password basic authentication.
2. **Mobile-Based Challenge/Response:** The challenge/Response process covers all the participating entities. After authenticating the web user using username/password, the Web server sends a challenge to the web user. The same challenge, together with an identity number of the web user (which is a priori exchanged with the Authentication Server) is sent to the Authentication Server. After receiving the challenge, the web user sends it to the mobile user, which in his turn sends the correct response to the Authentication Server through a pre-established General Packet Radio System (GPRS) connection. This demands no new connection, as the connection for GPRS is always established and the costs depend only on the amount of data exchanged.
3. **Combined Web/Mobile Temporary Password:** finally, given that the user supplied the correct response to the Web server, he/she receives a temporary one-time password on his/her Mobile. The user enters this temporary password from the Web browser, the password is checked by the server to complete the user authentication process and grant or deny access to the user.

Each of the above main steps is composed of one or more steps. Figure 1 illustrates the detailed operation of the system, which can be described as follows:

1. The user enters the Web site and submits his/her username and password via the browser. The connection to the web server is secured via a secure channel or tunnel.
2. The Web server verifies that the user has a valid username/password combination.
4. In case of valid username and password, the Web Server moves to the next step of authentication, and sends an authentication request of the web user together with a timestamp to the Authentication Server. The authentication request contains a web user reference assigned a priori between the Web Server and the Authentication Server. This could be a certificate for instance. Otherwise an error message is sent to the user rejecting his/her access and this terminates the authentication process.
5. After receiving the authentication request, the Authentication Server determines the mobile number assigned to the web user and sends a challenge (RAND) to the mobile user.

5. The client uses the random number (RAND) and the secret key (Ki) (which is known before to both parties as the Authentication Server is part of the Service Provider of the mobile user) to encrypt a shared piece of data. This shared piece of data could be a secret image ***F*** stored on the user's mobile. The image could be any image that acts as a user's signature. In our system we have used an offline-captured image as a unique biometric feature of the user. The same image is also stored on the Authentication Server.

6. The user sends the encrypted image from his Mobile to the Authentication Server.

7. The Authentication Server decrypts the image using the same RAND and Ki used for encryption. The Authentication Server compares the decrypted image ***F*** with the stored image using a normal template matching process. In case of a match, the system moves to the next step, otherwise the authentication process is terminated and the user access is denied.

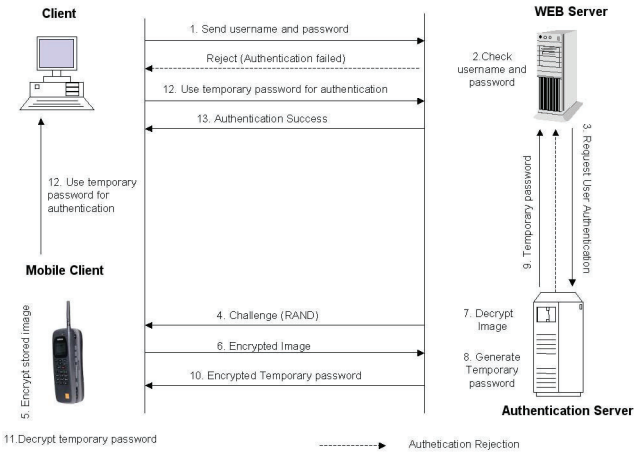

Figure 1: Detailed operation of the combined authentication system.

8. For a matching image, the Authentication Server generates a temporary one-time password.

9. The Authentication Server sends the generated one-time temporary password together with the original request timestamp via a secured channel to the Web Server.

10. The Authentication Server sends the encrypted temporary password to the mobile client

11. The mobile client decrypts the one-time password using RAND and Ki.

12. The user enters the decrypted one-time temporary password via the Web browser and sends it to the Web server.

13. The Web server checks if the temporary password matches the one it just received and decrypted from the Authentication Server then it grants access to the user, otherwise an error message is sent to the user indicated denied access.

The above described authentication steps need to be accomplished within a given timeframe. This assures that the access credentials are only to be used within this given timeframe. Empirically we have set the system to timeout after 90 seconds beyond which the user access is automatically denied. This is only an auxiliary choice which could be tuned according to the needs of the established system.

C. Security Analysis

The introduced concept extends in some way, the Kerberos authentication procedure with the assistance of mobile device. We enhanced ticket-granting mechanism by inserting a mobile device assistance to assure that the web user is the one he/she claims to be.

One of the major benefits of the proposed concept is the gain of privacy. The Web Server (this could be the server of a merchant) do not know anything more about the user other then his username/password and the identity number of the web user (which is a priori exchanged with the Authentication Server). The information about the user (mobile number, image, etc...) are only known to the Authentication Server, which is part of the mobile network service provider. Hence, there is no loss in privacy.

The image ***F*** that is captured offline is used as an add-on to the system security. It can be considered as the Credit Card holder's photo that is printed on the front side of his/her Card and can be used by the cashier to verify the cardholder's identity. Of course, the image needs to be stored in a tamperproof area on the Mobile such as a smart card, so that it cannot be replicated and used to access the Web server by illegitimate users.

A better approach would be to capture the Image **F** online, e.g. using a built-in Mobile camera, which nowadays comes bundled with many affordable price handsets. In this case, **F** would be different from the reference image stored on the Authentication Server; As a result, a careful consideration needs to be given to choosing a suitable threshold that achieves a compromise between the False Accept Rate (FAR) and False Reject Rate (FRR) biometric measures.

The use of timestamps guarantees that no cascaded authentication request could occur. With this timestamp, it could be assured that the requests will be distinguished from all the parties of the transaction. Furthermore, this could prevent replay attacks if any occur.

However, the proposed system could represent some single points of failures. In the following, such possible points are discussed:

1. The Web Server: this represents the interface between the web client and the authentication server.

This means that the web server should be secured against any manipulation from the client, especially input manipulation.

2. The authentication server should be secured against any possible abuse from the mobile client (in form of denial of service attack, when a malicious client tries send a big number of images to be decrypted by the authentication server).

In this concept, we assume that the two servers are secured against dangers that threaten their availability.

IV. Implementation And Performance Issues

The global programming environment for the system was java. Java provides five programming packages used for different sorts of applications; three of those packages were used in this project. These packages are: Java 2 Enterprise Edition (J2EE) which is used in developing applications for servers and enterprise computers, Java 2 Standard Edition (J2SE) which is used in developing applications for servers and personal computers, and Java 2 micro edition J2ME which is used in developing applications for Mobile phones and Personal Digital Assistances (PDAs).

A. Java 2 Micro Edition (J2ME)

Java 2 Micro Edition (J2ME) is a platform for developing applications for mobile devices [5]. It's designed for devices with limited memory, display and processing power including Personal Digital Assistances (PDAs) and pagers. Within J2ME, configurations define the run-time environment for a set of devices by specifying the Java features that are available, as well as which virtual machine will be used.

In J2ME, the Connection Limited Device Configuration (CLDC) defines a configuration targeted at devices that have limited processing power, display and memory. The majority of these devices are mobiles.

On top of these configurations are profiles. Profiles provide Application Programming Interfaces (APIs) for user interface design, network support, and persistent storage. The Mobile Information Device Profile (MIDP) is a set of Java APIs, which, together with the CLDC, provide a complete J2ME application run-time environment targeted at mobile devices such as mobile phones, pagers and entry level PDAs [5].

B. J2ME MIDP / J2EE Integration

Using both the J2ME MIDP and J2EE platforms, it is possible to implement mobile enterprise solutions. On the server-side, J2EE applications are developed and deployed. On the client-side, MIDP applications are developed. These applications can be run on any MIDP-compliant device, whether it's a mobile phone or PDA. This allows serving a wider range of clients.

In MIDP, the Hypertext Transport Protocol (HTTP) provides the most suitable network transport between the MIDP application and the server-side J2EE application. MIDP includes standard support for HTTP 1.1, and APIs for generating HTTP GET, POST and HEAD requests, basic header manipulation, and stream-based consumption and generation of messages.

V. Experimental Results

The system has been implemented and tested using a set of scenarios as shown in Table 1.

TABLE I. Different test scenarios and their authentication results.

Scenario	*U*	*P*	K_i	*F*	*TP*	*T*	*AuR*
1	√	√	√	√	√	***< 90***	***A***
2	***X***	√	-	-	-	***< 90***	***R***
3	√	***X***	-	-	-	***< 90***	***R***
4	√	√	***X***	-	-	***< 90***	***R***
5	√	√	√	***X***	-	***< 90***	***R***
6	√	√	√	√	***X***	***< 90***	***R***
7	√	√	√	√	√	***> 90***	***R***

U: Username, P: Password, K_i: Secret key

F: Image, TP: temporary password, T: timeout

AuR: Authorization Result

A: Accept user.

R: Reject User

The results show that the system performs as expected. The test cases of Table 1 show that scenario 1 is the only condition in which the Authorization Result ***AuR*** indicates that the user access request is accepted by the Web server, that is when all the necessary authentication information is correctly supplied by the user within the allocated time frame. All other cases (scenarios 2 to 6) show that the user failed to show at least one valid type of the required information, as a result the access request was Rejected ***R*** in all cases.

Of special interest is test scenario 7 in which the user has supplied all valid information, however, he/she failed to complete the authentication process within the 90 seconds Timeout ***T***, as a result the system timed out and the user access was Rejected ***R***. Given the complexity of the authentication algorithm, the Timeout element ***T*** plays an important role in the authentication process, especially in busy environments with considerable amounts of network delays. As a result this factor was set to be tuneable.

The performance of the proposed solution is at of the same level as the Kerberos-based authentication if we consider the fact that the only possible performance bottleneck of the system is the communication between the

authentication server and the mobile client and that the encryption of the image is not done online.

VI. CONCLUSION

A combined Web/Mobile access control scheme has been implemented whereby the security of remote Web access has been improved, while still maintaining a trade-off between system security and usability through the use of a normal Mobile handset and a tunable timeout factor. Observations have shown that the combined system offers generally better eavesdropping security compared to a standalone Web or Mobile authentication system. The security of the system can be further improved through the online capture of image from built in Mobile cameras.

REFERENCES

[1] A. Al-Qayedi, R. El-Khazali, A. Zahro, S. Al-Shamsi, "Secure Centralised Mobile and Web-based control system USING GPRS with J2ME", ICECS2003, Sharjah, U.A.E, 2003.

[2] Carlisle Adams & Steve Lloyd, "Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations", New Riders Publishing, 2001

[3] Joris Claessens, Bart Preneel and Joos Vandewalle, "Combining world wide web and wireless security", Department of Electrical Engineering, Katholieke University Leuven

[4] Vorapranee Khu-smith and Chris J. Mitchell, "Enhancing e-commerce security using GSM authentication", Information Security Group, Department of Mathematics, Royal Holloway, University of London

[5] John Muchow, "Core J2ME Technology & MIDP", The Sun Microsystems java series, 2001