AN ANTI-DOS AUTHENTICATION SYSTEM IN M-COMMERCE *

Liang Wang and Runtong Zhang
School of Publishing Communication and Management, Beijing Institute of Graphic Communication
Institute of Information System, Beijing Jiaotong University, Beijing, China

Keywords: M-Commerce, Identity Authorization, Anti-DoS, S/Key OTP.

Abstract: This paper analyzed the shortages under DoS attack of S/KEY OTP system in m-commerce identity authentication and suggested an improved one-time password system based on bidirectional virtual authorization in m-commerce systems. On one hand, this suggestion can reduce the calculation stress of both client and server, accordingly increases the efficiency of authorization and withstands the DoS attack. On the other hand, the suggestion can implement the bidirectional authorization and reduce the possibility of fishing attack.

1 BACKGROUND

1.1 One-Time Password

The idea of OTP (One-Time Password) was first suggested by American scientist Leslie Lamport (Lamport, 1981) in early 1980s of the 20th century. The principle of OTP is adding some uncertain factors in the procedure of authorization. Every time user logins, the information transmitted on network is different, thus the security is improved (Wang, 2007).

1.2 The S/KEY OTP System (Haller, 1995)

Based on the idea of OTP system, Bellcore produced S/KEY OTP system in 1991. An S/KEY OTP system client passes the user's secret pass-phrase through multiple applications of a secure hash function to produce a one-time password. On each use, the number of applications is reduced by one. Thus a unique sequence of passwords is generated. The S/KEY OTP system host verifies the one-time password by making one pass though the secure hash function and comparing the result with the previous one-time password (Haller, 1995). In S/KEY OTP system, the secret pass-phase stores in neither client nor server. And only an irreversible one-time password transmitted on the network, the secret pass-phase doesn't be transmitted at any time, so this system can counter replay-attacks effectively. Figure 1 outlines the procedures of S/KEY OTP system.

The S/KEY OTP system is a simple mechanism and does not need a notarization by the third part. So it is suitable for some low performance system like mobile devices. Thus the S/KEY OTP system can be used in mobile commerce identity authentication.

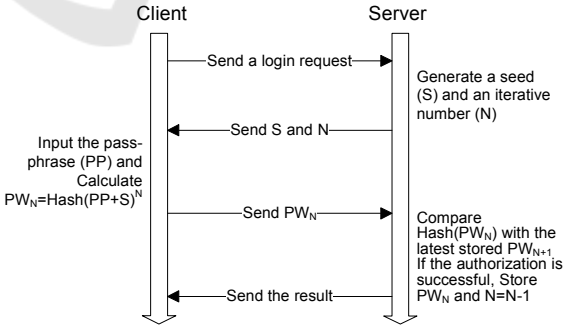

Figure 1: The authorization procedure of S/KEY OTP system.

* This work is supported by Key Research Project of Beijing Institute of Graphic Communication under contract with No.23190110015 and the Fundamental Research Funds for the Central Universities under contract with No.2009YJS034.

Zhang R. and Wang L.
AN ANTI-DOS AUTHENTICATION SYSTEM IN M-COMMERCE.
DOI: 10.5220/0003268702520256
In *Proceedings of the Twelfth International Conference on Informatics and Semiotics in Organisations (ICISO 2010)*, page
ISBN: 978-989-8425-26-3

2 SHORTAGES OF S/KEY OTP SYSTEM IN MOBILE APPLICATION

There are a lot of advantages of S/KEY OTP System, such as serviceability, flexibility and dynamism. But in the environment of mobile commerce identity authentication, some shortages appear.

1) The S/KEY OTP system will launch multiple calculation whenever it receive a legal of illegal requests., Hackers may utilize this shortage to make a mass of illegal requests to implement a DoS attack. The authorization server makes huge amount of calculation for the illegal requests until crashed.

2) The S/KEY OTP system only implement one side authentication, Hackers may utilize this shortage to make an imitated server to implement a fishing attack.

3 BIDIRECTIONAL VIRTUAL AUTHORIZATION

To solve the problems, two tasks must be achieved. One is to cut down the amount of calculation to the full. The other is to let the client verify the identity of the server.

So we suggest the model of "Bidirectional Virtual Authorization", the following content tells the procedure of this model. Figure 2 outlines the physical architecture of the improved system.

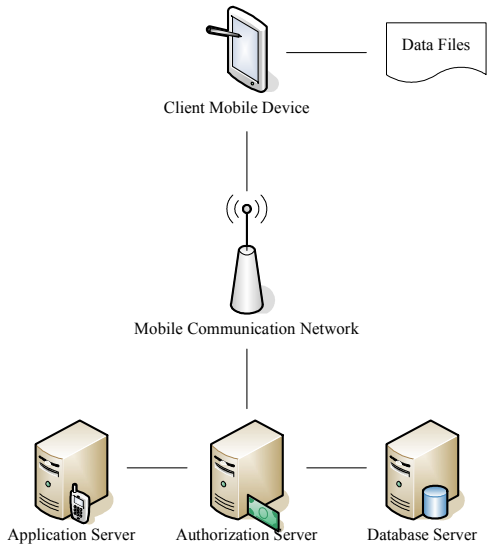

Figure 2: The physical architecture of the improved system.

3.1 The Procedure of Registration

Step 1: The client generates a request of registration;

Step 2: The server generates a response to establish a connection;

Step 3: The client inputs user's id (UID) and pass-phrase (PP);

Step 4: The server checks the existence of UID. If UID has existed, return the error message and finish the registration. Else return the success message.

Step 5: If UID does not exist, the server generates a seed (S) and an initial iterative number (N0) and sends S and N0 to the client.

Step 6: The server calculates the initial server-side password (PWS0) and saves it as current server-side password (PWS), at the same time, save the current iterative number (N) using the initial iterative number subtracts 2:

$$PW_S = PW_{S0} = \text{Hash}(PP + S)^{N0} \quad (1)$$

$$N = N_0 - 2 \quad (2)$$

Step 7: The client calculates the initial client-side password (PWC0) and saves it as current client-side password (PW_C):

$$PW_C = PW_{C0} = \text{Hash}(PP + S)^{N0-1} \quad (3)$$

The procedure of registration completes. See figure 3.

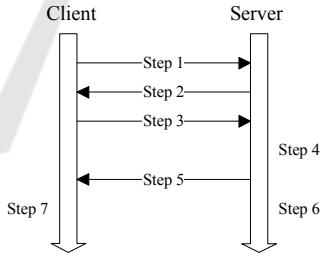

Figure 3: The registration procedure of the improved system.

3.2 The Procedure of Authorization

Step 1: The client generates a request of authorization;

Step 2: The server generates a response to establish a connection with the seed (S), current iterative number (N) and current server-side password (PWS);

Step 3: The client get S, N and PWS, then calculates Hash (PWC). If PWS = Hash (PWC), the

server's identity is authorized, Else the client will finish the authorization. In this step, we have established the server-client authorization successfully.

Step 4: After verifying the server, the client calculates Hash (PP+S) N-1 and compares it with PWC stored locally, if PWC ≠Hash (Hash (PP+S) N-1) 2, the client should ask the user to re-input the pass-phrase without notifying the server. In this step, we have established the virtual authorization on client-side successfully.

Step 5: The client sends the value of Hash (PP+S) N to the server.

Step 6: The server get the value of Hash (PP+S) N sent by client, then calculates Hash (Hash (PP+S) N) 2 and compares it with PWS stored locally, if PWS ≠Hash (Hash (PP+S) N) 2, the server should send an error message to the client.

Step 7: After complete an authorization successfully, the server should update the current server-side password (PWS) with the value of Hash (PP+S) N, at the same time, the iterative number (N) subtracts 2:

$$PW_S = \text{Hash (PP+S)}^{N0} \quad (4)$$

Step 8: After complete an authorization successfully, the client should update the current client-side password (PWC) with the value of Hash (PP+S) N-1.

The procedure of authorization completes. See figure 4.

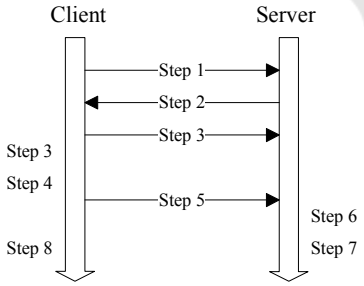

Figure 4: The authorization procedure of the improved system.

3.3 The Procedure of Synchronization

When the iterative number goes to zero or the client reinstall the system, the system must reset the iterative number (N). In these situations, the procedure of authorization occurred first. After complete the authorization successfully, the server generates a new initial iterative number (N0) and sends N0 to the client. To solve the two problems above, two tasks must be achieved. The communication should be under secure environment.

4 SYSTEMS SIMULATION

4.1 Running Environment of the Simulation

Platform: Intel(R) Core2 E7500 with 2G Memory
Operating System: Microsoft Windows Server 2003
Develop Environment: Microsoft Visual Studio 2008
Application Server: Microsoft IIS 7
Analysis Toolkits: NS2, Gnuplot and Xgraph Tools.

4.2 Simulation Approach

According to the authorization procedures analyzed above, we developed a simulation system. This system executes the authorization procedures several times and records the network traffic and delay using NS2 software and the Gnuplot and Xgraph toolkits.

The wireless model essentially consists of the mobile node at the core, with additional supporting features that allows simulations of mobile networks. The mobile node object is a split object. The C++ class mobile node is derived from parent class Node. A mobile node thus is the basic node object with added functionalities of a wireless and mobile node like ability to move within a given topology, ability to receive and transmit signals to and from a wireless channel etc. In this paper we described the internals of mobile node, its routing mechanisms, the routing protocols, creation of network stack allowing channel access in mobile node, brief description of each stack component, and trace support and movement/traffic scenario generation for wireless simulations), see figure 5.

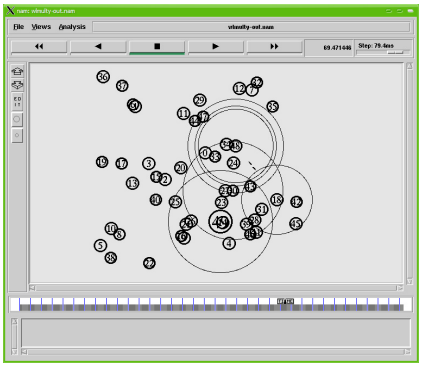

Figure 5: The simulation approach of the improved system.

4.3 Simulation Results

Table 1: Average network traffics simulation result data of the original and improved system in common situation.

Nodes	Avg. Traffics of Original Solution (Bytes/ms)	Avg. Traffics of Improved Solution (Bytes/ms)
10	2417.6	2433.8
20	3515.1	3601.2
30	8262.5	8266.1
40	13866.3	14011.2
50	17662.3	17710.1

According to the data form Table 1, we get the chart below.

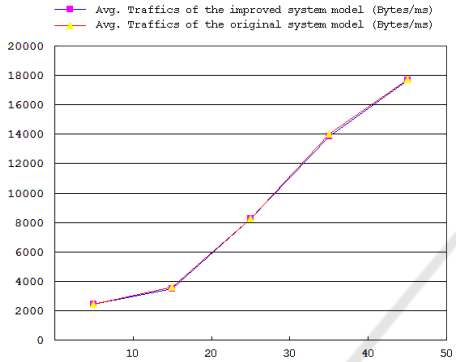

Figure 6: Average network traffics comparison between the original and improved system in common situation.

Table 2: Average network traffics simulation result data of the original and improved system in DoS attack simulation situation.

Nodes	Avg. Traffics of Original Solution (Bytes/ms)	Avg. Traffics of Improved Solution (Bytes/ms)
10	3756	2455.3
20	6899.1	3811.5
30	15176.3	8512.2
40	24701.8	15227
50	32833.3	18216.5

According to the data form Table 2, we get the chart below.

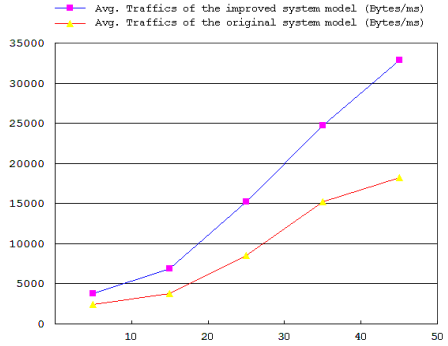

Figure 7: Average network traffics comparison between the original and improved system in DoS Attack Simulation Situation.

5 THE COMPARISON BETWEEN THE IMPROVED AND THE ORIGINAL SYSTEM

Comparing with the Original S/KEY OTP system, the improved system changes the digression factors to 2 from 1, and stores the values of N times and N-1 times iterative on server and client respectively. With this method, the bidirectional virtual authorization is established. The advantages of the improved system have shown in the following factors.

5.1 Portability

When the client of improved system meets wrong login information, it can verify the information locally without notifying the server, then the stress of the server is reduced greatly and the server can resist the DoS attack to a certain extent.

5.2 Bidirectional Authorization

When an authorization request is generated, the client asks the server to send the information that stored in server latest and verifies it. If the verification failed, the authorization procedure will be interrupted. Thus the client can resist the fishing attack to a certain extent.

6 CONCLUSIONS

In this paper, we analyzed the characteristics of mobile commerce, suggested the shortages of S/KEY OTP system in mobile commerce applications. Then we proposed an improved One-Time Password system model. According to our discussion, our One-Time Password system model inherited the advantages of S/KEY OTP system, and improved it in portability and security. The improved system model is more suitable for the authorization of mobile commerce.

REFERENCES

Lamport. L., 1981. Password Authentication with Insecure Communication. In *Communications of the ACM 24.11, pp.770-772*.

Haller. N., 1995. The S/KEY One-Time Password System. In *Bell Communications Research and Naval Research Laboratory*.

Hongying Wang, 2007. Research and Design on Identity Authentication System in Mobile-Commerce. In *Beijing Jiaotong University, pp. 18–50.*

Haller. N., and R. Atkinson, 1994. On Internet Authentication. In *Bell Communications Research and Naval Research Laboratory.*