DATABASE AND SECURITY FILES

Author Name: Altaf khan and Ahmed Mohammad Ahmed

Implementation of Yen Shen Hwang's One Time Password using c#.net

Table of Content

Yen-Sheh-Hwang's One-Time Password Authentication Scheme Implementation

1. Introduction:

In that scheme, mutual authentication of a user and server is used. We implemented One Time Password Authentication Scheme using Visual studio 2010 frame work. User and Server communicate with each other. First user will register and after this server will authenticate user. When user login server will verify and if he computes this verification then server show that this is verified user. Code and implementation is given at: https://github.com/akniazi001/Database-and-file-security.git.

2. Implementation:

There are three main part of implementation. First is registration of user. Second is login and third is authentication of user by nounce and password. There are some steps to implementation of One Time Password.

2.1 **Registration**: If user want to register to a server he connect to server and Server will send him a secrete key (seed). Show in figure below.

Figure 1.1 Registration One Time Passwords

And after this server will send him three parameters N, D(nounce) XoR with Seed and hashed value of D. N and D is randomly generated value by server. We will use 3 different type of function to perform this type of task. User gets D (nounce) value from D XoR Seed by performing again XoR function. We developed GetXOR(string input,string key) which gets two values from user one is original data and other is key value and returns the XOR value of both.

After this he will perform hash function on it if answer will match with server sending hashed function value then it is consider as correct D-nounce. The hash function is a function which return hashed value we developed this function in c#.(protected string GetHash(string password, string salt) . password is actual data which you want to hashed and salt is any value you want to use as a key to perform hash function.)

After this, user will perform login procedure. User send password XOR with D- nounce and password is hashed by above function with salt(seed). Server disclose password and store it with his database. The process is shown in figure 1.2 below

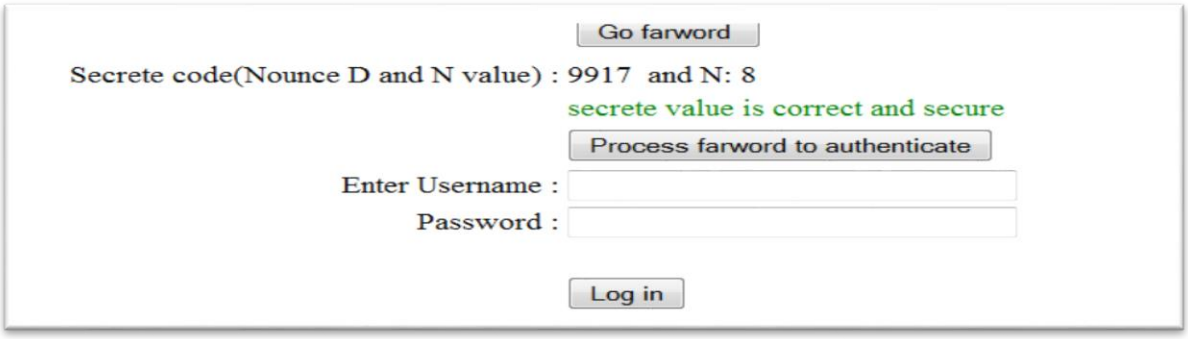

Figure 1.2 shows that user verify the nounce value and get N value from server.

Actually user enter seed value we took seed value from above label 'seed' then user is not entering first time but the next time user will enter this value otherwise user can't get nounce and N value.

3. Login stages:

When user will login again then server will compare it previous information and send it new Nounce value encrypted with Seed and user get this value and implement has function on this and compare the result with hash value sending by server. Server sends hashed nounce Xor with previous password and user enter previous password with Seed value. Server verify it and authenticate the use each time N becomes on less and so on if it becomes zero then system shows a message that user authentication has been expired please register again.

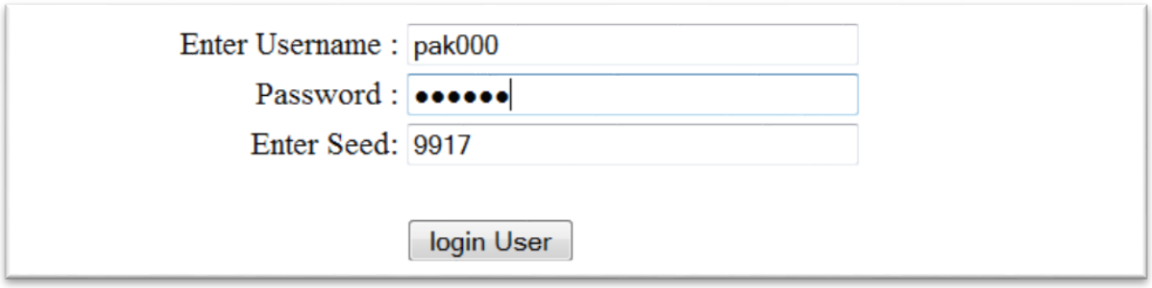

Figure 1.3 show that user enter name password and seed value for next time login.

Each time system store new password and replace old password and generate new nounce value. If user enter wrong password then system check it and when system want to get nounce it will not match with previous password value hence it show value is not correct. If password is correct system forward the user to next successful login page.

4. Reference:

Yum D.H., Lee P.J. Cryptanalysis of Yen-Shen-Hwang's One-Time Password Authentication Scheme, IEICE Trans. Communic., v. E88-B, No. 4, April 2005, 1647-1648,