AN EFFICIENT IDENTITY BASED AUTHENTICATION PROTOCOL BY USING PASSWORD

Sanjeev Kumar Mandal[1] and A R Deepti[2]

[1]Research Scholar, Department of Master of Computer Applications, Acharya Institute of Technology Bangalore, India,
[2]Associate Professor (fka), Master of Computer Applications, Acharya Institute of Technology Bangalore, India.

ABSTRACT

In a distributed system, authentication protocols are the basis of security to ensure that these protocols function properly. Passwords are one of the most common authentication protocol used nowadays. Because of low entropy of passwords make the systems vulnerable to password guessing attacks. This paper presents a simple scheme that strengthens password-based authentication protocols and helps prevent dictionary attacks, replay attacks and man in the middle attacks etc. The proposed scheme presents a new password authentication protocol by using the user and server system identification/serial number. Here there is no possibility to store the user passwords so an attacker who gets the password cannot use it directly to gain immediate access and compromise security.

KEYWORDS

Authentication, Authorization and Password.

1. INTRODUCTION

In distributed systems, authentication protocols play an important role in security aspects to ensure that these protocols are working properly. Most of these protocols found in the literature [1] contain redundancies or flaws or their designs might be error prone. Authentication, sometimes called integrity refers to protect the information from being modified by any unauthorized parties [2]. Two concepts are implicit in integrity namely 1) Identity integrity where the source of the data is indeed who it claims to be (like people or computers or services) and not with intruders, and 2) data integrity where it assures that information is unchanged or destroyed from its source.

The paper deals mainly with the identity integrity. From past to present days, humans have authenticated to each other while transferring the data. This transmission of data [3] can be done based on two people present physically near to each other or present in different far away places. In such circumstances, authentication has been done by alternate means, like secret handshakes [4] or passwords [5]. The reality of these authentication techniques often failed to validate the identity when there are times of a distance is required. Because most of the techniques currently used for authentication over a distance do not measurably provide a meaningful degree of trust. Thus, the focus of the paper deals with the methods for using data input factors that provide

DOI: 10.5121/ijnsa.2017.9605

meaningful and measurable confidence about whether or not someone is who they say they are, and that they are not.

This paper focuses a new password based method to solve the authentication problem between client and server by using system serial number of both. Then by performing mathematical calculation to this system serial number the server generate a unique id or password and send to the user. Here the user remembers a small password and carries no other information. So without the user and server system serial number and the newly generated unique id the attacker cannot impersonate the user. In addition, this method exchange strong secret key which enables the two parties to communicate securely. Also it is secure against attacks like dictionary attacks, passive attacks [6] or active attacks [7] network intruders and masquerade attacks [8]. Finally, this paper is comprised into three sections namely, Section 2 discusses the background of authentication and authorization aspects and its vulnerabilities. With the help of both user and server system serial number, a new approach of password based method has been developed. It is used to overcome the password insecurities and the rationale behind its design with an illustration. Section 3 analyzes the security concerns of the new password based approach and concludes in Section 4.

2. BACKGROUND:

With the current trend of network and computers a large amount of valuable information are stored. To secure this valuable information, security is needed in the internet world. Therefore, the first step towards network security is by keeping unauthorized persons from gaining access to resources by ensuring that only authorized persons can access it. Therefore, authentication and authorization play an important role in security part. Authentication [9] is the process of identifying a user or a machine that is trying to log on or to access the resources. Whereas authorization [10] is to verify the user is having permissions and rights to access the requested resources. To make it work, a user provides some sort of credentials- a password, smart card, fingerprint, digital certificate to identify the authorized user to access the system. Several attacks and risk are possible if the authentication is poor like [11],

1. Loss of Privacy: In day to day life, confidential information has been transmitted in business-to-business communications. So, without proper encryption, every message sent may be read by an unauthorized party.
2. Loss of Data Integrity: Even for data that is not confidential, one must still take measures to ensure data without modifying it.
3. Identity Spoofing: Apart from protecting the data, one must be careful to protect their identity on the Internet. Otherwise any intruder may be able to impersonate and gain access to the confidential information.
4. Password Authentication: In most enterprises, the use of passwords is the primary means of authenticating a user. Unfortunately, it is also the weakest form of authentication. In today's digital world, the ways to bypass this form of security are trivial. While many enterprises focus on strengthening passwords, these efforts are by and large meaningless in the face of the tools that attackers can use. The tools provide criminals with easy ability to hack, trap, or crack most passwords easily.

So, this paper discusses a new strong password based authentication method by using unique-id.

2.1 Statement Of Research Problem:

Passwords are the method often used for authenticating computer where the users can use/remember the password easily. But this approach has several vulnerabilities [12] like password may be easy to guess, writing the password down and placing it in a highly visible area, and discovering passwords by eavesdropping. Though there are different authentication protocols available widely in the world, most of them are error prone [1]. Testing tools have been used in real time applications to check whether the authentication protocols are secure by different servers is shown below,

2.1.1 Gmail Authentication:

The JSKY testing tools has been used to test the Gmail Authentication service where the authentication involves SRP authentication protocol with SSL. From figure.1, it has been proved that the Gmail is insecure against SQL Injection attack and brute force attack.

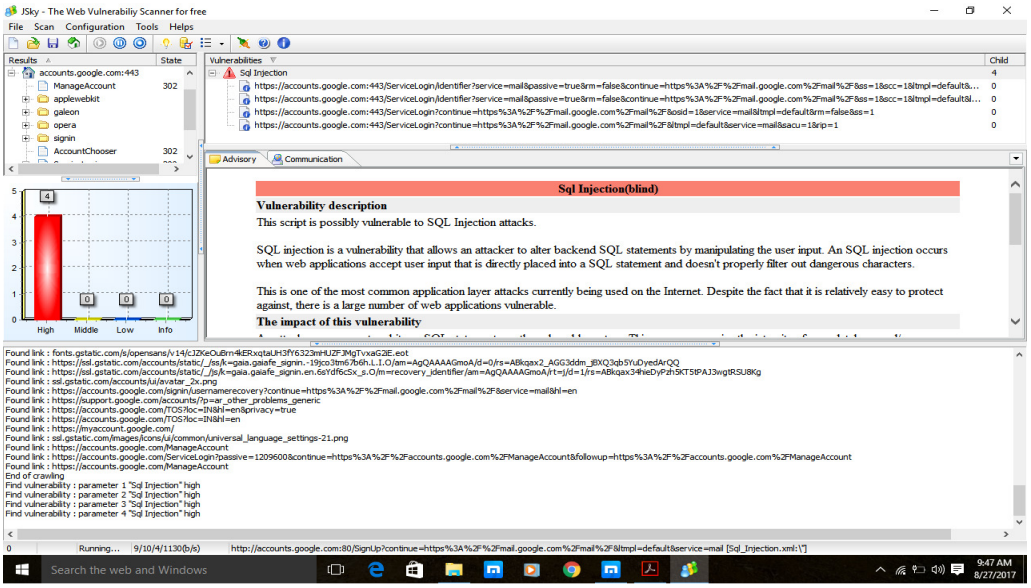

Figure 1. Testing Gmail in JSKY tool

2.1.2 Yahoo Authentication:

The yahoo Authentication service tested by using JSKY tool has shown in figure 2, that yahoo is insecure against Brute Force attack, ProRat attack, Directory attack and File backup attack.

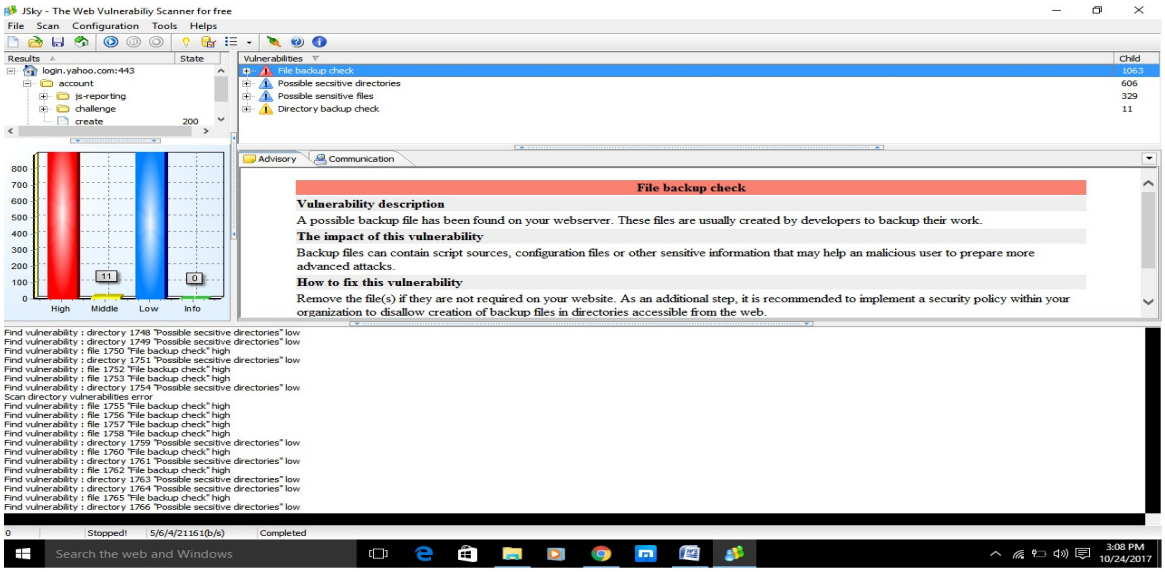

Figure 2. Testing Yahoo in JSKY tool

2.2 Proposed Method:

To overcome the above insecure features, a new approach has been developed by using the system serial number. This method comprises into two phases: registration/login, verification/ new device registration as follows,

2.2.1. Registration/login Phase:

During this phase the user must fill the application form like name, address, contact number, social security number or any government identification number and submit to the server. Upon receiving the details, the server first verify the user with the help of social security number. Then the server takes the user accessing computer system serial number which is unique (computer or laptop or mobile). With this user system serial number and the server system serial number, the server performs mathematical calculation and generates a unique id/key and transmits to the user. Now with the newly generated key i.e unique id the user can login and perform further work. Here, the user must use the same system for login and the server confirms every time with the help of user system serial number for authentication.

2.2.2. New Device Registration Phase:

If the user lost/damage/failure happens to his existing system, then with the help of old unique id and social security number he/she can send a request to the server, where the server verifies and generate a new unique id/key for the new system and transmit to the user to logon.

2.2.3. Design Phase:

Notation used:
User = U_i, Server = S_i, Registration Request = RQ, Device id = DID, Social Security number = SSN, Login Services Request = SRQ, Phone Number = PH, Address = ADD, Server Database SSN = SDB-SSN_i, Unique id/key = UI, Server Device ID = SDI, User Device ID = UDI.

Registration Phase:

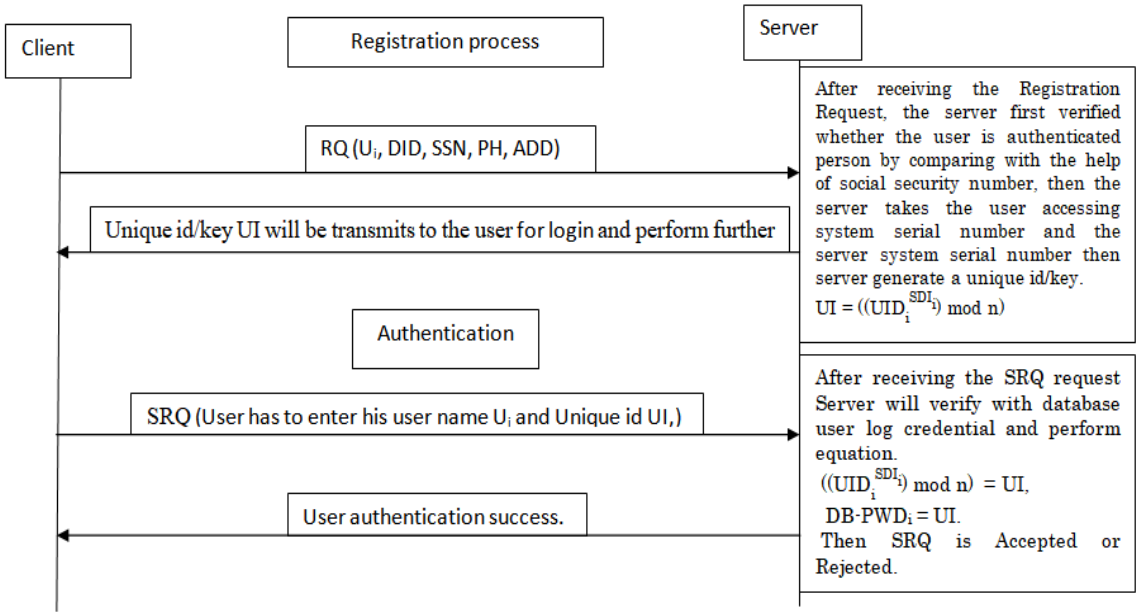

Figure 3. Registration process

U_i = RQ { U_i, DID, SSN, PH, ADD }
S_i = RQ
UI = $((UDI_i^{SDI_i}) \bmod n)$
$S_i = U_i$ (UI)

Login Phase:

1. U_i = SRQ (U_i, UI_i)
2. S_i = SRQ,
3. S_i = (U_i =, SDB-SSN_i) is true, server perform final device check
4. SRQ (Device id = $((UDI_i^{SDI_i}) \bmod n)$ if is true then he/she can access the Services from the Server.
5. If (Device id ≠ $((UDI_i^{SDI_i}) \bmod n)$, then Server will block the access of unauthorized person.

```
String sql="select * from user where NAME='"+uname+"'  and  DOB='"+dob+"' and SSN='"+SSN+"'and EMAIL_ID='"+emailid+"'";
                        rs=st.executeQuery(sql);


                        while(rs.next())
                        {


                                String uuname=rs.getString("NAME").trim();
                                String ddob=rs.getString("DOB").trim();
                                String SSN=rs.getString("SSN").trim();
                                String emid=rs.getString("EMAIL_ID").trim();

                                if(uname.equals(uuname) &&dob.equals(ddob) &&SSn.equals(SSN) &&emailid.equals(emid))

                                {

                                        found=1;
                                        break;
                                        int usersystemid = st.executeQuery(wmic bios get serialnumber);
                                }

                                }
                                }
```

Figure 4. A sample SQL code to generate User System Serial Number by the Server

Verification & New Device Registration phase:

When Service request is sent by the User Login Services Request SRQ = (U_i, UI) to Server S_i, then server performs the following operation in order to verify the User U_i.

Verification

1. S_i = (U_i =, SDB-SSN_i) is true then server perform final device check
2. SRQ (Device id = (($UDI_i^{SDI_i}$) mod n) if is true then he/she can access the Services from the Server.
3. If (Device id ≠ (($UDI_i^{SDI_i}$) mod n), then Server will block the access of unauthorized person.

New Device Registration phase

1. For new device registration user send a request to server where the server perform the following steps:

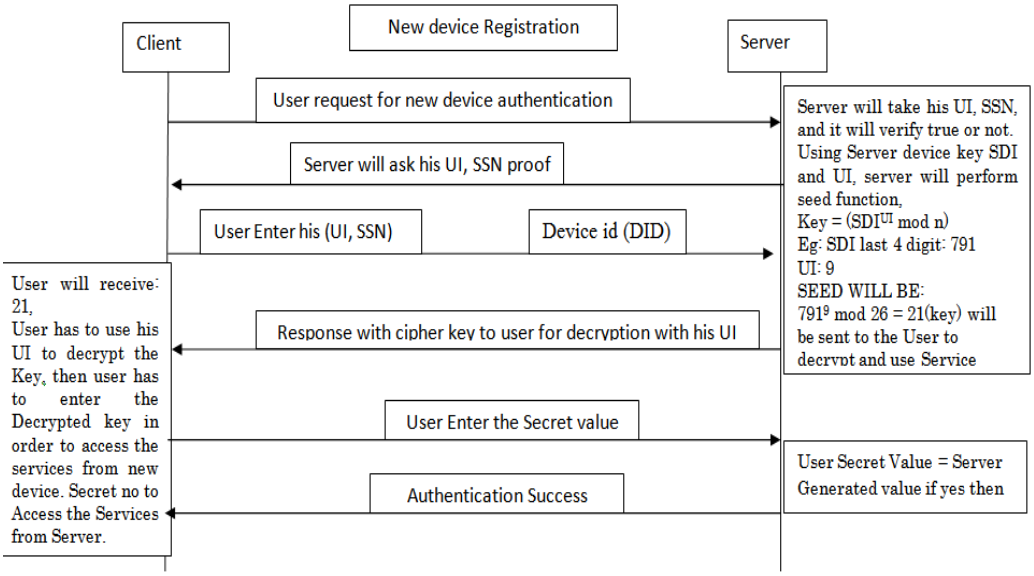

Figure 5. New device Registration

2. User send a request for new device registration with his old SRQ (U_i, UI, SSN) number then he/she has sent SRQ to the server, server will check his SSN from the database. If SSN = SDB-SSN_i, UI = server database UI, then server will generate new device id.
   Key = (SDI^{UI} mod n)
   Key will be sent to the user U_i he/or she can decrypt the id with help of his UI_i,

3. Server will verify by Key = Server Key,
   SSN = SDB-SSN_i.
   Finally, server will grant access to the new device.

The time complexity of the proposed method is $14T_h+12T_x$

2.3. Illustration:

2.3.1 Registration phase:

The registration of the client to the server is done with his/her personal information in figure 6.

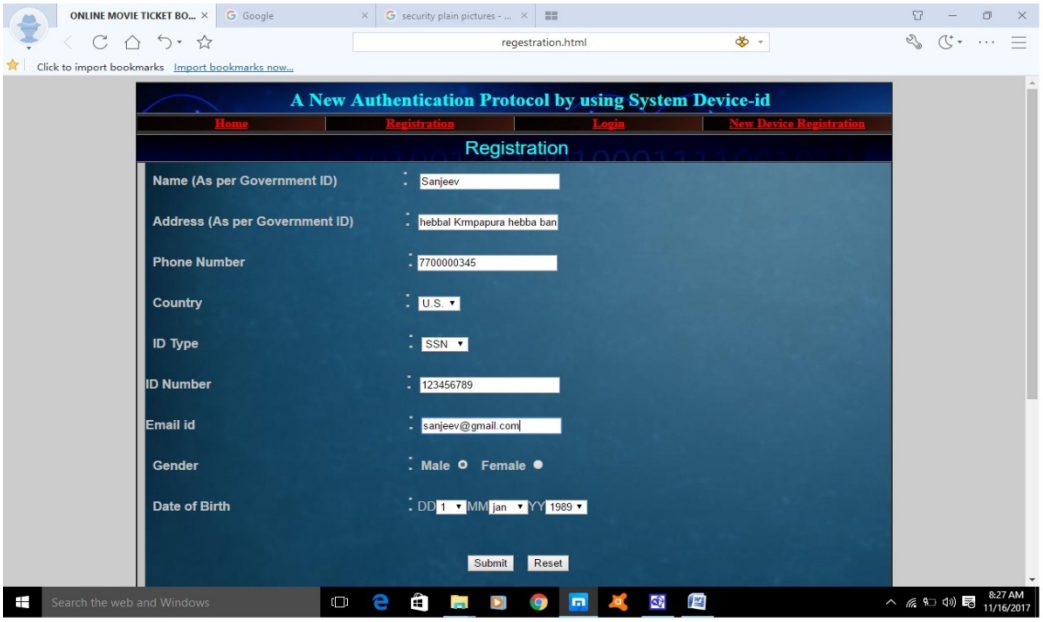

Figure 6. Registration Phase

User Data verification from Server database:

Government ID	ID NO	NAME
Adhar (India)	123456789	Sanjeev
The national ID(Thailand)	987654321	Tomsan
Social Security number (SSN) U.S.	123456789	Sanjeev

The servers verify with the help of social security number and generate unique id.

Creating Unique Id UI for User:

Name U_i	Sanjeev
Uniq id reorganized by government	123456789
ID Type	Social Security number (SSN) U.S.
Email-ID	sanjeev@gmail.com
Phone no	7700000345
User Device ID	123456789
Server device ID	791
UI	9

$UI = ((UDI_i^{SDI_i}) \bmod n))$

Eg: $123456789^{791} \bmod 12 = 9$

UI = 9 this number is used for log in from new device or password change.

2.3.2 Login Phase:

Now with the help of unique id the user can login and proceed further work.

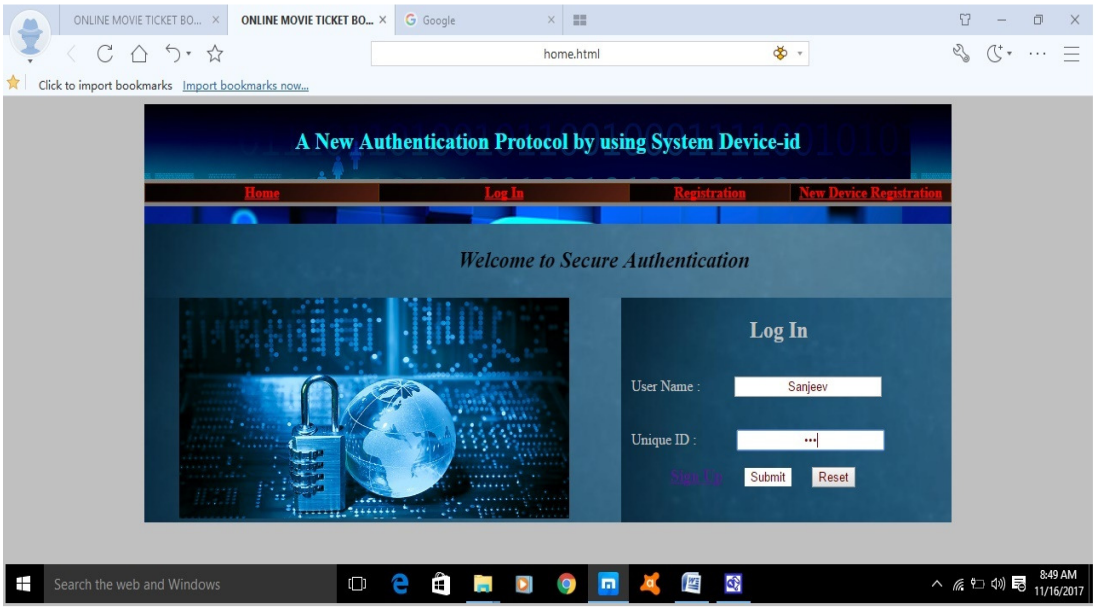

Figure 7. Login Phase

New device Registration:

If the same user wants to use different device or loss of an old device, he/she has to re-register with the help of his existing uuid and govt. id.

Table 1. New Device Registration Phase

U_i	Sanjeev
UI	9
ID Type	Social Security Number
ID Number	123456789

Then Server request the user UI and SSN for verification through secure channel,
Ex: UI = 9,
SSN = 123456789
Then SSN and UI are verified by the server and then the server does the following steps:
Server device Id $S_i = 791$,
UI = 9,
Ex: $791^9 \bmod 26 = 21$ (this will be sent to the user via a secure channel).
Users have to use his UI for performing inverse modular function and give the key to the server.
Now the server authenticates the user and the user uses the new key for further access.

3. SECURITY ANALYZING:

The proposed password method helps to secure against the attacks are given below,

3.1 Man in the Middle attack:

A man-in-the-middle attacks like eavesdropping. In the proposed method, even if intruder captures the user information he/she cannot able to access it without proper user and server system device-id is shown in figure 8.

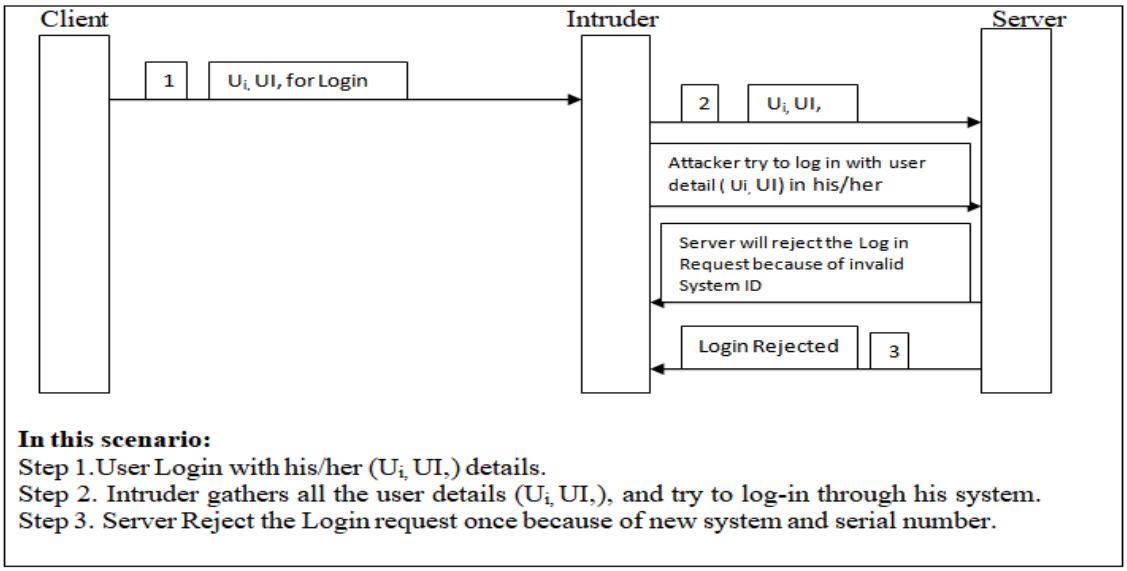

Figure 8. Man-in-middle attack for the proposed password method

3.2 Denial of service attack:

A denial-of-service attack occurs when an attacker takes action that prevents legitimate users from accessing computer systems, devices or other network resources. In the proposed method, even if the intruder knows the user system serial number and other details, it is difficult to authenticate without the user system. So it is secure against denial of service attack.

3.3 Password guessing Attack:

Password guessing attacks can be classified into two namely, Brute Force Attack and Dictionary attack.

3.3.1 Brute Force attack:

It is a password guessing attack and it consists of trying every possible code, combination, or password until the correct password is found. In the proposed method, suppose an intruder collects the user information and try to authenticate with the server is difficult, because of using different computer system and system id. So, the proposed method can withstand brute force attack which is shown in figure.9 by using OWASP testing tool.

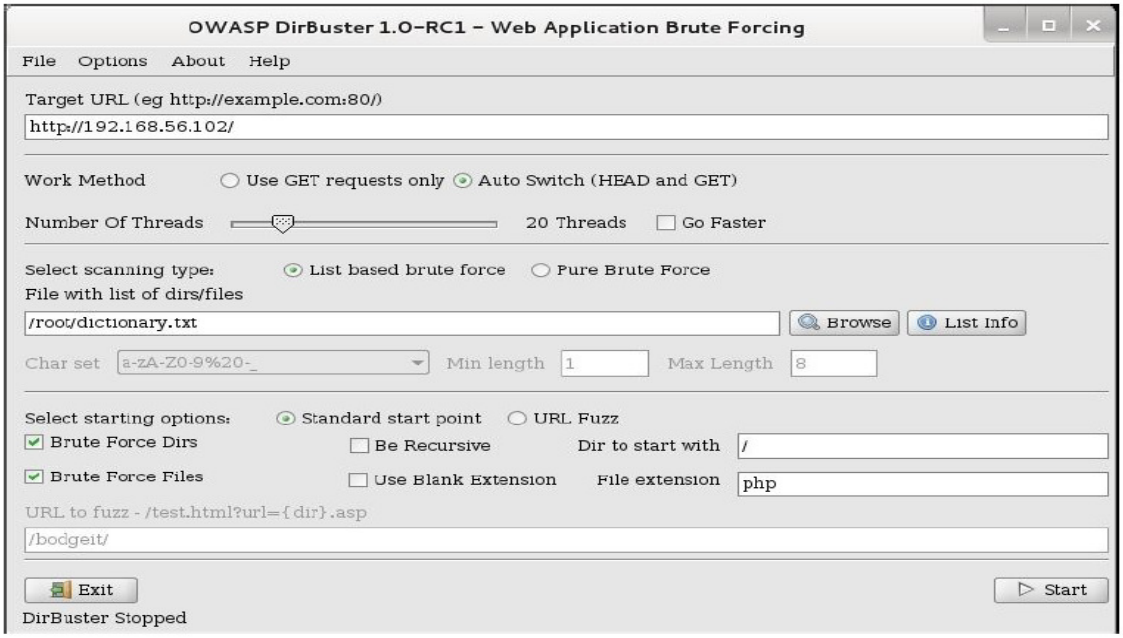

Figure 9. Brute Force Attack for the proposed method by using OWASP

3.3.2. Dictionary Attack:

A dictionary attack is another type of password guessing attack which uses a dictionary of common words to identify the user's password. To secure the dictionary attack, Brutus testing tool has been used in the proposed method, shown in figure 10.

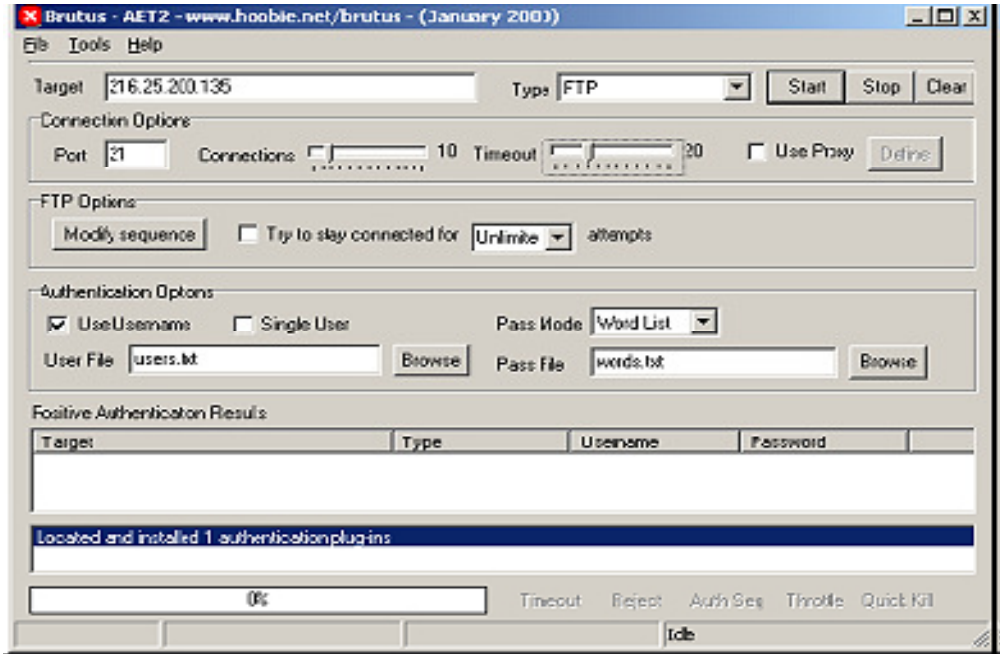

Figure 10. Dictionary Attack by using brutus tools for the proposed method

3.5 Replay Attack:

Replay attacks are the network attacks in which an attacker spies the conversation between the sender and receiver to collect the authenticated information. In the proposed method, the intruder tries to gain the information and without proper credentials like user/server system serial number, is difficult to authenticate.

4. CONCLUSION

In recent years security plays a major part in the internet world and it is a challenging one to design strong security protocols. To achieve authentication and confidentiality, several authentication protocols have been proposed and analyzed. Most authentication mechanisms focus only on security, while others offer proper scalability, minimized communication, and computation overhead. In this regard different authentication techniques arise but the Password-based authentication is the most widely used method for verifying the identity of persons who are requesting access to computer resources. However, authentication based only on passwords often does not provide adequate protection. So, this paper uses system serial number as a password to verify the identity of system users and can substantially increase the security of an authentication system.

REFERENCES:

[1] Sanjeev Kumar Mandal and A. R Deepti (2017), "A General Approach of Authentication Scheme and its Comparative Study", International Journal of Computer, Vol. 26 No. 1, pp. 15-22.

[2] Abdulrahman Hamed Almutairi and Abdulrahman Helal Alruwaili (2012), " Security in Database Systems", Global Journal of Computer Science and Technology Network, Web & Security, Vol. 12 Issue. 17, pp. 9-14.

[3] Prateek Kumar Singh, Pratikshit Tripathi, Rohit Kumar, Deepak Kumar (2017), "Secure Data Transmission", International Research Journal of Engineering and Technology, Vol. 04 Issue. 04, pp. 217-222.

[4] Gene Tsudik and Shouhuai Xu (2006), "A Flexible Framework for Secret Handshakes", in Multi-party Anonymous and Un-observable Authentication 2006 proceedings of the international conference in Berlin, Heidelberg, 2006, Springer-Verlag, Vienna, pp. 295–315.

[5] Zhu Zhaoa, Zhongqi Dongb, Yongge Wang (2005), "Security analysis of a password-based authentication protocol", Theoretical Computer Science Elsevier, No. 352, pp. 280-287.

[6] Shafiullah Khan, Noor Mast, Kok-Keong Loo, Ayesha Salahuddin (2008), "Passive Security Threats and Consequences in IEEE 802.11 Wireless Mesh Networks", International Journal of Digital Content Technology and its Application, Vol. 2 No. 3, pp. 4-8.

[7] Sobia Aslam, Saleem ullah, M. Abubakar Siddique, Abdul Sattar (2017), "Active Attacks Detection Mechanism using 3-Phase Strategy", International Journal of Computer Science and Network Security, Vol. 17 No.1, pp. 130-136.

[8] Malek Ben Salem and Salvatore J. Stolfo (2011), Data Collection and Analysis for Masquerade Attack Detection: Challenges and Lessons Learned, Columbia University, available at: https://pdfs.semanticscholar.org/b181/ee00299b9553eb5f4c995e277adea6dcd519.pdf

[9] Michael Burrows and Martin Abadi (1990), "A Logic of Authentication", ACM Transactions on Computer Systems, Vol. 8 No. 1, pp. 18-36.

[10] Na Wang, Jens Grossklags, Heng Xu (2013), "An Online Experiment of Privacy Authorization Dialogues for Social Applications", in San Antonio, Texas, 2013, Proceedings of the conference on Computer supported cooperative work, San Antonio, Acm, New York, NY, USA, pp. 23-27.

[11] Dicky Hau (2003), "Global Information Assurance Certification Paper", available at: https://www.giac.org/paper/gsec/3161/unauthorized-access-threats-risk-control/105264 (accessed 11 July 2003).

[12] David Silver, Suman Jana, Eric Chen, Collin Jackson, and Dan Boneh (2014), "Password Managers: Attacks and Defenses", in USENIX the Advanced Computing System Association 2014 Proceedings of the 23rd USENIX Security Symposium, San Diego, 2014, USENIX, pp. 449-464.

[13] A. Langley (2011), "Forward secrecy for Google HTTPS," available at: https://www.imperialviolet.org/2011/11/22/forwardsecret.html

[14] Ms. Ankita R Karia, Dr.Archana B. Patankar, Ms. Purnima Tawde (2014), "SMS-Based One Time Password Vulnerabilities and Safeguarding OTP Over Network", International Journal of Engineering Research & Technology, Vol. 3 Issue. 5, pp.1339-1343.

[15] Ms. Vidya Vijayan, Ms. Josna P Joy, Mrs. Suchithra M S (2014), "A Review on Password Cracking Strategies", International Journal of Research in Computer and Communication Technology, Vol. 3 No. 3, pp. 8-15.

AUTHORS

Dr.A.R.Deepti, is an active researcher in the area of network security and image processing. She received her PhD in computer science from the University of Madras.

Sanjeev Kumar Mandal doing his PhD research in Computer Science from Visweswaraya Technological University, Belgavi. He got Certification in Appin Lab for Information Security. His current research interests include network security and cyber security.