SECURED AUTHENTICATION PROTOCOL SYSTEM USING IMAGES

G. Arumugam
Prof. & Head, Department of Computer Science
Madurai Kamaraj University
Madurai, India.
gurusamyarumugam@gmail.com

R. Sujatha
Research Associate, SSE Project, Department of
Computer Science
Madurai Kamaraj University
Madurai, India.
sujamurali72@gmail.com

Abstract—In order to protect secret information from sensitive and various applications, secured authentication system should be incorporated; it should contain security and confidentiality. Even if it is assumed that the cryptographic primitives are perfect, the security goals may not be achieved: the system itself may have weaknesses that can be exploited by an attacker in network attacks. In this paper a Secured Authentication Protocol System using Images (SAPSI) is presented. It ensures confidentiality, and authentication using server and Image based authentication mechanism.

Keywords- Confidentiality, Security, Server, Image-Based Authentication System, Authentication.

I. INTRODUCTION

A significant challenge in providing an effective network system defence mechanism is to detect the intrusions and implement counter-measures. Organizations who use Secured Authentication system tolerate no leakage at all. Cryptographic primitives are useful tools but security of the primitives does not guarantee security of the system. Usage of different level of security provides a security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories.[1, 5, 6].

Cryptographic mechanisms are communication systems that rely upon cryptography to provide security services across distributed systems. Applications increasingly rely on encryption services provided by cryptographic systems to ensure confidentiality and authentication during secure transactions over the network. However the security provided by these encryption services might be undermined if the underlying security system has any flaws in the design or implementation. Weaknesses in security systems such as misuse of encryption, compromising the private encryption key etc., are yet to be addressed. [8].

Secured Authentication System is an application of a computer system to process information with different sensitivities (i.e. classification of information at different levels) to permit simultaneous access by users with different security clearance and to prevent users from obtaining access to information for which they lack authorization. Secured Authentication has two goals: first goal is to prevent unauthorized personnel from accessing information. Second goal is to prevent unauthorized personnel from declassifying information. The traditional view of secured authentication is one of ensuring that information at a high security classification cannot flow down to a lower security classification.[1, 3, 12].

In this paper, Secured Authentication Protocol System using Images is proposed. It overcomes the identified drawbacks of existing systems. The attacks on existing model embedded in encrypted sessions are detected as monitoring the processes taking part in the systems is integrated. The new system uses encryption mechanisms. Hence the inside information is protected and also the outside attacks are prevented. To establish this, a server with authentication mechanism is used. Types of attacks were proscribed in the proposed system are Brute force attack, Dictionary attack, Keyloggers, Shoulder Surfing, Man-In-The-Middle attack and Database Server Compromise attack.

Brute force attack. The hacker can try two kinds of Brute force attacks on this system. One is re-using of images and another is without re-use of images. For a user, there will be a unique password of length 8 or above selected in SAPSI for the given session. Possible image patterns were dynamically changed on every session along with random numbers. By performing this attack in SAPSI hacker unable to break the password because it needs two processes.

Dictionary attack. Dictionary attack is one of the most commonly used techniques to break a Password-based system. If same kind of sequences appeared in the network for a long time it can be guessed by the hacker.

Keyloggers. Keylogger is a program, which captures the user’s keystrokes and sends this information to the hacker. The natural protection for an authentication system from the keylogger is to have a one-time password (or Dynamic password).

Shoulder Surfing. Shoulder surfing is looking over someone’s shoulder when they enter a password or a PIN code. It is an effective way to get information in crowded places because it is relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done at a distance with the aid of...
binoculars or other vision-enhancing devices to know the password.

**Man-In-The-Middle Attack.** A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other.

This strategy is implemented to protect information from unauthorized disclosure or modification and to provide mechanisms to authenticate users participating in the exchange of information.[7].

In section 2 related works are discussed with their drawbacks.

Section 3 discusses the overview of Proposed Secured Authentication System with server and Authentication mechanism using images methodology.

In section 4 implementation details related to the system are presented. Conclusion is given in section 5.

## II. RELATED WORK

Enhanced authentication mechanism using multilevel security model (EAMMSM) is the system that belongs to and applies multilevel security. Any sensitive application it includes confidential and secret information which must be used effectively in complicated and authenticated procedures. Using five levels of authentication methods with a set of privileges assigned, each user has to surpass 50% of every level to get the privileges rights.[1].

During authentication the information was hacked from the network plane using network analyser tool. Leakage of information occurred in three levels while transmitting answers with username and multiple questions methods.

In Improving text password through persuasion (ITPTP), users entered their passwords with visibility.[2].

Users tend to choose their passwords in a simple manner by entering visibility method, which makes the hacker to know with shoulder-surfing process.

An authentication method combining text and graphical passwords (AMCTGP), and users selecting their passwords using random numbers assigned to images, is given in [11].

Users selecting their passwords by clicking random numbers listed in the selection panel can be identified by a hacker using movie-clip camera phones.

In Multiple password interference in text and click-based graphical passwords (MPITCGP), users select their passwords from the given image as pass points.[10].

Users selecting their passwords from the given image is a hectic process. If any mismatch of pass points occurred the original user itself would be unable to get authentication even by knowing pass point selections.

In Pass Pattern System (PPS): A Pattern-Based User Authentication Scheme, data hacked from database through database compromise server attack is represented. [7].

There are several attempts reported in literature about authentication schemes in lieu of the traditional Password-based system. Each attempt is successful in increasing the strength of the system against some of the known attacks. They are either computationally intensive or they require additional hardware/software in the infrastructure. In this section we review the current attempts, identify the gaps and emphasize the motivation for developing Secured Authentication Protocol System using Images.

---

**Figure 1: Secured Authentication Protocol System using Images Flow Diagram**

*SSE Project funded through NTRO, New Delhi*
Motivation for Secured Authentication Protocol System using Images: We proposed secured authentication system is robust against attacks such as the brute force, shoulder surfing, social engineering, database server compromise attack and Man-In-The-Middle attacks. It incorporates the essence of Image-based authentication system.

III. SECURED AUTHENTICATION PROTOCOL SYSTEM USING IMAGES

This system involves the use of authentication mechanism and a server that minimizes the hacking by the attackers. It monitors the clock cycle process effectively. Two processes are involved in this system. They are a) Authentication using Images and b) Security Questions Authentication using server represented as flow diagram in Figure 1.

A. Authentication using Images

This is a Image-based authentication system based on the premise that ‘humans are good at identifying, remembering and recollecting graphical image patterns than text patterns’.[9].

In SAPSI the client gets authenticated in two levels. In the first level the client gets authenticated using username and password method with graphical image patterns. It is illustrated in Figure 2.

For providing the password the client has to enter the index number provided at the images. While entering index numbers in the password area it will be hidden and bullet marks will be displayed. For example, if the client chooses images rose, white lion and lord shiva then the index numbers 27, 44 and 17 should be entered in a selected order. While confirming password images index numbers were shuffled, so user has to re-enter the password by giving different index numbers according to the images chosen. Here both image patterns and index numbers are represented as dynamic arrangements in every login attempt. Due to this setup no one would be able to read or guess the mechanism involved.

For every authentication the images were shuffled and index numbers were varied and shuffled. It is represented in Figure 3.

The client has to enter the index numbers according to the selected images in an order given during registration. As per the selection made during registration, the client has to enter index numbers now as 29, 34 and 61.

Each image will be mapped with a corresponding number which is stored in the Image-Map table. Instead of comparing the images, the mapped numbers are compared. It serves as user friendly for the end-user and machine friendly for the system by reducing the comparison time by using numbers rather than images. A mapping mechanism which validates the index numbers with hidden letters is represented in Table I.

Figure 3: A sample shuffling mechanism of Secured Authentication Protocol System using Image Patterns.

The client can select the images on some sequences familiar to him/her. Due to shuffling mechanism, this method reduces the guess ability of the persons who are related to the clients. During entry of password, only bullets appear in the password area which avoids the shoulder surfing attacks.

When sending random numbers in the network plane, it will be converted into a computed ascii value, so that Man-In-The-Middle attack is prohibited.

<table>
<thead>
<tr>
<th>Image Numbers</th>
<th>Const Hid Characters</th>
<th>Random Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1 Iteration</td>
</tr>
<tr>
<td>I1</td>
<td>AO</td>
<td>23</td>
</tr>
<tr>
<td>I2</td>
<td>IP</td>
<td>70</td>
</tr>
<tr>
<td>I3</td>
<td>LJ</td>
<td>31</td>
</tr>
<tr>
<td>I4</td>
<td>XI</td>
<td>41</td>
</tr>
<tr>
<td>I5</td>
<td>YU</td>
<td>12</td>
</tr>
<tr>
<td>I6</td>
<td>MK</td>
<td>17</td>
</tr>
<tr>
<td>I7</td>
<td>HR</td>
<td>27</td>
</tr>
<tr>
<td>I8</td>
<td>EW</td>
<td>44</td>
</tr>
<tr>
<td>I9</td>
<td>SA</td>
<td>55</td>
</tr>
</tbody>
</table>

Figure 2: A sample Secured Authentication Protocol System using Image Patterns

TABLE I
A SAMPLE IMAGE-MAP MECHANISM FOR SAPSI

ISSN 1947-5500
http://sites.google.com/site/ijcsis/
Using this mapping mechanism the shuffling process of images and index numbers are generated. The images are validated only by using the hidden characters and index numbers which reduce the time complexity of comparing the images.

The image positions are generated using permutation sequences. Let \( A = \{I_1, I_2, I_3\} \), this set can be arranged in 3! ways as,

\[
\begin{align*}
\end{align*}
\]

For \( n \) images \( n! \) Sequences were generated and it will be used randomly for every attempt of registration or login.

### Security Potency of Secured Authentication Protocol System using Images:

In general, several attacks are possible on an authentication system. For any authentication system, the hacker can attack at least at three places: they are server, client and the communication link. The attack on server includes Brute force attack, Dictionary attack and compromising the server as a whole. At the client, the possible attacks are key logging and shoulder surfing. Finally on the communication link, the possible attack is Man-In-The-Middle attack, which can be done using packet sniffers.[7]

In terms of the data being passed from the user to the server the data stored in the secured server is comparable with the classical Password-based authentication system. In both cases, user sends the username and a password. This will be compared with the registry in the database. But because of the dynamic nature of password selection system, SAPII is more secure than ordinary password-based scheme to attacks such as Brute force, Dictionary attack, Keylogger, Shoulder surfing and Server database compromise attack. The best known solution for such attacks is to use cryptography protocols at the server or on the communication link. In this we analyse the impact of the four attacks mentioned here on SAPII.

On analysing Brute force attack - I in SAPII, if the hacker wants to guess the password, the probability of success will be \( 1/(64^n) = 5.96046E-08 \) (Since there are unlimited images, 64 images are taken as sample). If the guess is wrong, probability of success will remain the same for the next guess. It is because the password will change with every attempt.

Hence,

The probability of success for every attempt = \( 1/64^n \)

The other way of doing Brute force attack - II is to try all combinations of positions. For example, if we consider a 8x8 Image Pattern setup there will be \( 64^n \) (if selection of images includes reuse of images) or \( 64^n \)P\( _n \) (without reuse of images) different images of length \( n \).

Number of possible Image Patterns = \[
\frac{(N^2)^n}{(N^2-n)!}
\]

Number of possible Image Patterns for the size of N x N matrix with re-use of images as passwords \( (N^2)^n \) is illustrated in Table II and without re-use of images as passwords \( (N^2)!/(N^2-n)! \) is represented in Table III.

### Table II

<table>
<thead>
<tr>
<th>Size of Matrix - N</th>
<th>Length of the Image Password - n</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>65536</td>
</tr>
<tr>
<td>6</td>
<td>65536</td>
</tr>
<tr>
<td>8</td>
<td>16777216</td>
</tr>
<tr>
<td>9</td>
<td>43046721</td>
</tr>
<tr>
<td>10</td>
<td>100000000</td>
</tr>
<tr>
<td>12</td>
<td>429981696</td>
</tr>
<tr>
<td>13</td>
<td>815730721</td>
</tr>
</tbody>
</table>

### Table III

<table>
<thead>
<tr>
<th>Size of Matrix - N</th>
<th>Length of the Image Password - n</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>43680</td>
</tr>
<tr>
<td>6</td>
<td>1413720</td>
</tr>
<tr>
<td>8</td>
<td>15249024</td>
</tr>
<tr>
<td>9</td>
<td>39929760</td>
</tr>
<tr>
<td>10</td>
<td>94109400</td>
</tr>
<tr>
<td>11</td>
<td>203889840</td>
</tr>
<tr>
<td>12</td>
<td>412293024</td>
</tr>
<tr>
<td>13</td>
<td>787083024</td>
</tr>
</tbody>
</table>

To break the system, the hacker on an average has to break \( (nx64^n)/2 \) images (with reuse) or \( (nx64^n)/2 \) (without reuse).

Number of images that are to be broken = \[
\frac{n (N^2)^n}{2N^2} \]

\[
\frac{n (N^2)^n}{2(N^2-n)!}
\]
Number of images that are to be broken by evaluating the length of the password in Brute force attack – I method is depicted in Graph 1 and Brute force attack – II is represented in Graph 2.

![Graph 1: Number of Images that are to be broken with reuse of Images.](image)

Shoulder surfing can be done easily on the password system, just by seeing the keys that the user is typing. But to decode the password in SAPSI, the hacker has to see both the key sequence and Image patterns and do a mapping before user submits the page. So shoulder surfing is of little or no use in SAPSI as compared to a password-based system.

In the case of SAPSI, using Man-in-the-middle attack the attacker is not able to get original messages because the images and random numbers changed dynamically on every presentation or session.

Comparing these attacks and it is represented in Graph 3.

The images used for password selection can be of any kind. Depending on the application it can be varied. For sample discussion nature images were used. For implementation characters, numbers and special characters were used as images. Two digit and three digit random numbers were used in implementation. In compact display applications two digit random numbers preferred and in large display applications three digit random numbers preferred to mystify hackers.

![Graph 2: Number of Images that are to be broken without reuse of Images.](image)

Graph 3: Comparison of Attacks in Authentication Systems using Existing and Proposed System.

### B. Security Questions Authentication

In second level the client gets authenticated using security questions. A 10-digit number is issued to the client at the time of registration. The client has to answer three security questions and the results are encrypted with a 10-digit number.
A resultant factor is passed over the network plane for validation to the server.

Encryption Process

- Three security questions queried (s1, s2, and s3).
- Ascii value evaluated for two security questions (a1 and a2).
- Bitwise operation is performed,
  - \(\text{sum1} = (a1 \& a2) \mid s3\)
- resultant factor (sum2) = sum1 \(\oplus\) id
- Ascii value of resultant factor (sum2) send to verifier.

Verification Process

- During Client registration a shared 10-digit key (id) and resultant factor (sum2) issued to server.
- Authentication process: achieved result (sum3) of client \(\oplus\) resultant factor (sum2).
- Authentication granted – a shared 10-digit key (id) generated. If not then authentication denied.

The server decrypts the resultant factor and gets the registration number of the client.

After passing the Authentication using Images level and Security questions authentication level, the client gets authenticated.

IV. ANALYSIS AND IMPLEMENTATION

In this new system all drawbacks of existing methods are overcome with new secured authentication protocol system using images. This system is implemented both in single client and multiple clients with server.

Only two levels are used for authentication with single server to authenticate clients. No repetitive methods are used in this proposed method which does not irritate the client. No leakage of information is possible in this new method which avoids the Man-In-The-Middle attack. In [1] leakage of information which occurred during sublevel transitions is avoided in this new system. When entering password no visibility is there which protects the shoulder surfing attacks from related persons. In [2, 11] given passwords are processed using shoulder surfing and if any person tries to hack the password using capture devices, which is protected in new system by giving passwords in a hidden manner. Even if any capturing devices are used to capture images, no one will get information due to hidden bullets in the password area. It is very difficult to remember the pass points in an image [10]. This difficulty is avoided in this new system by selecting the random numbers in the images. This avoids the confused remembrance of pixel positions instead of whole images.

Both existing and proposed systems were implemented and the time difference is evaluated and it is represented in Figure 5. The total image position sequences were generated for 9 images are 362880 and the results were shown in Figure 6.
V. CONCLUSION

In order to improve the confidence in security system, detecting intrusions in those systems plays a vital role, as the security system design is not always perfect. Our system overcomes the problem encountered in existing systems and ensures the confidentiality and authentication when sending a message.

ACKNOWLEDGMENT

This paper is part of SSE Project funded through a National Technical Research Organization, New Delhi is gratefully acknowledged.

REFERENCES


[5] Hubert common and vitaly shmatikov, Is it possible to decide whether a cryptographic protocol is secure or not?


