Securing Graphical Password Techniques from Shoulder Surfing and Camera Based Attacks

Esha Kumar

Abstract*: Authentication is a procedure that checks for validity and may be carried out in a variety of methods, including tokens, biometrics, and passwords with text and graphics. Usability is the primary driver of graphical passwords. However, shoulder surfing and camera-based attacks are the main potential disadvantage of this strategy. Shoulder surfing is a sort of social engineering method used in computer security to peek over the victim's shoulder and steal information, including personal identification numbers (PINs), passwords, and other private information. This attack can be carried out either up close by peering straight over the victim's shoulder or from a further distance, perhaps by utilizing a pair of binoculars or other comparable equipment. Crowded areas are when an assailant is most likely to shoulder surf the victim. These days, it's fairly typical to enter passwords by looking. The fundamental process for gaze-based password entering is same as regular password entry, with the exception that the user stares at each desired character or triggered location in sequence rather of typing a key or touching the screen, much like when they are eye-typing. Therefore, in my project, I have made an effort to avoid these limitations by utilizing a powerful encryption technique like the Vernam Cipher.

***Keywords*: Vernam Cipher, Password Entry, Security, Shoulder Surfing**

I. INTRODUCTION

Shoulder surfing is the practice of gathering information by employing direct observation tactics, such as peering over someone else's shoulder[1]. Because it's quite simple to stand next to someone and see them fill out a form, input a PIN number at an ATM, or use a calling card at a public pay phone, shoulder surfing is a useful technique for gathering information in busy areas[2]. Long distance shoulder surfing is also possible with the use of binoculars or other vision-improving tools[3]. Since the introduction of the first cellphones 10 years ago, there has been a marked growth in public awareness of the harm potential posed by shoulder surfing[4]. And while there are no reliable statistics on the frequency of shoulder surfing attacks, a 2016 study by Memon and Nguyen discovered that 73% of mobile device users surveyed had seen someone else's PIN (although not always with malicious intent), and a 2017 study of shoulder surfing awareness presented at the CM Conference on Human Factors in Computing Systems revealed that 97% of those surveyed claimed awareness of a shoulder surfing attack[5]. Vernal encryption is part of a strategy that has been used to stop and prevent this shoulder surfing threat. Each character of the message's plaintext is "mixed" with one character from the key stream, according to the Vernam Cipher's underlying theory[6]. The outcome will be a really "random" ciphertext that has no connection to the original plaintext if a truly random key stream is utilized[7]. The key stream and individual bits of plaintext are combined to create the ciphertext by using the logical XOR operation (exclusive-or)[8].

II. ARCHITECTURE

A. Initial Phase

The user is prompted to give two inputs one being the registration email and the other being the password which the user may choose from the given list of suggested passwords which are tested for being difficult and highly inconvenient to crack or may define a password explicitly.

B. Authentication Phase

Initially the user is needed to enter the pre-requisite details to login to the software, once the details are entered, the software then uses a secret keyboard to generate a sequence for every user entered character the keyword is made unique for each and every session and for every unique user.

C. Proposed Algorithm

The Keyboard mechanism is basically implemented to remove Shoulder surfing attackers from gaining any insights on the personal details of the individual. It is a simple and easy solution even for camera based attacks. The newly substituted sequence is randomly generated every time such that even when the same characters are entered, they appear as a sequence of completely different characters. It is to be noted that all these character substitutions occur in the front end display fields and not in the back end. The hidden keyboard lies in the back end and we shall use a different sequence of letters each time thereby eliminating any chances of active attacks.

III. PRE-EXISTING WORKS

- In one of the papers, the use of colour pass techniques has been discussed as a defence against shoulder surfing assault. Without disclosing the real PIN, the user can access the session. It offers protection from shoulder surfing assaults and has a smart user interface. It could, however, take a considerable period of time. Its dependence on a partially observable attacker model is its biggest drawback[1].

Manuscript received on 28 June 2022 | Revised Manuscript received on 12 July 2022 | Manuscript Accepted on 15 September 2022 | Manuscript published on 30 September 2022.
***** Correspondence Author

Esha Kumar*, Senior Identity and Access Management Analyst, Schneider Electric, Bengaluru, India. Email: eshakumar.98@gmail.com

Retrieval Number: 100.1/ijrte.B71640711222
DOI: 10.35940/ijrte.B7164.0911322
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

- In one of the papers, it is suggested to use a new technique that keeps as little information about the password items on display. The suggested approach permits both password and distracter objects to be utilised as the challenge set's input in addition to hiding the password objects and the total number of password objects. The whole set of password objects must be known in order to determine the correctly typed password, which looks to be random. As a result, it would be challenging for an opponent to figure out the user's true password through shoulder surfing. According to simulation findings, each challenge set's right input object and location are chosen at random, guarding against frequency of occurrence analysis attacks. Results of the user research indicate that the suggested strategy can stop shoulder-surfing attacks. The suggested solution reportedly makes use of photos as the password since they're simple to remember[2].
- In one of the papers, they have offered a strategy to stop this SS onslaught. We do this by altering the keypad's layout and using sophisticated BW (lack White) and session key methods. The session key's simplicity would often be a significant drawback. 4 length restriction, round redundancy, and security. The main drawbacks of adopting a W technique are the inability to record with too few cameras[3].
- An innovative method is put forth in a study that employs digraph substitution rules to hide the process or action needed to generate password-images. In the suggested way, a user only has to click on one of the pass-images rather than both pass-images that are displayed for three sets of challenges in a row. The suggested method's digraph replacement rules, however, may be known to the attackers[4].
- In this paper, a novel solution to the issue of shoulder surfing attacks is PassBoard. Recently, attempts have been made to adapt these keyboards by loading the layout dynamically and rearranging it to confound the spying miscreant[5].
- In one of the works, the user suggests a better text-based, shoulder surfing-resistant graphical password scheme employing colour PIN input mechanisms. The user may log into the system quickly and effortlessly under the suggested plan. The proposed solution protects the password from accidental logins and shoulder surfing[6].
- One of the projects involves developing a technique especially intended to thwart sniffer attempts. The relevance of password concealment is first covered in the article, and then the solution to the issue is discussed. However, alphanumeric password protection must be taken into consideration, along with improved randomised password scrambling and manipulating operations[7].
- One of the articles suggests a brand-new hybrid graphical password-based solution. The system, which combines recognition and recall-based approaches, offers several advantages over current systems and may end up being more user-friendly. The technique is immune to numerous other graphical password assaults as well as the shoulder surfing attack. It is suggested for smart mobile devices, which are more portable and practical to use than conventional desktop computer systems (such as smart phones, such as the iPod, iPhone, PDAs, etc)[8].
- In one of the works, it was also suggested to utilize a novel method of user authentication called Graphical Password Authentication utilizing Images Sequence. In this way, the user uploads pictures from his or her own gallery or directory to choose a password. The photographs that one user uploads will not be viewable by another user. This approach substitutes a graphical password for the text-based, conventional alphanumeric password[9].
- One of the works introduces early and developing fundamental security components based on AI concepts, specifically, a graphical secret key with strong fundamental structures, which larger things can be built based over Captcha invention of new things, and it is known as Captcha as graphical passwords (CaGP). CaGP generally focuses on various security challenges, such as guessing attacks, relay attacks (from one location to another), and, if combined with double view innovations of new objects, bear surfing assaults. Additionally, CaGP offers a novel technique for addressing critical image hotspot graphical key difficulties[10].
- One method, called PassPoints, was designed and tested with human users in one of the publications. The evaluation's findings were encouraging in terms of the graphical password's memorability. The study broadened our understanding of human factors by examining two topics: first, the impact of tolerance, or margin of error, while selecting password points, and second, the impact of the picture used as the password system. The results of the tolerance research indicate that putting a relatively tiny tolerance (10 x 10 pixels) around the user's password points significantly reduces correct recall for the password. The results demonstrate that there was little real variation in how well the photos performed. This early finding implies that a variety of graphics may aid in graphical password system's memorability[11].
- A thorough analysis of the available graphical password schemes was carried out in another work. They then offered a potential theory of their own as well[12].
- In one of the extended abstracts, a straightforward graphical password authentication scheme was suggested. They emphasized key components of the system and provided an explanation of how it worked using certain instances[13].
- A review of graphical password schemes from 2005 to 2009 was published in one publication, and it was suggested that these schemes would be resistant against shoulder surfing assaults[14].

IV. PROCEDURE

Initially, the user is prompted to give two inputs one being the registration email and the other being the password which the user may choose from the given list of suggested passwords which are tested for being difficult and highly inconvenient to crack or may define a password explicitly. Once the other pre-requisite details are entered, a secret keyboard will pop up and the user will be using it to enter the password securely.

When user enters a character key, the software generates a unique keyboard with a new sequence by using Vernam Cipher.

Retrieval Number: 100.1/ijrte.B71640711222
DOI: 10.35940/ijrte.B7164.0911322
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The XOR function is used to create the cypher text from the plaintext and a random stream of data that has the same length. This process is extremely safe since it is different for each session and each user.

A. Cipher Used

Every character of plaintext from a message is "mixed" with one character from a key stream, according to the theory behind the Vernam Cipher. A genuinely "random" cypher text that has no reference to or similarity to the original plaintext will result from the usage of an entirely random key stream. In that instance, the encryption resembles the uncrackable One-Time Pad quite a bit (OTP). The technology is also known as One-Time Tape, or OTT, since it was typically used with teleprinters and 5-level punched tape. If the generated cypher text in the aforementioned OTT system is indeed completely random, it may be delivered securely over the air without being at risk of being interpreted by an observer. To decipher the original plaintext, all the receiver needs to do is combine the cypher text with the same OTT. Just make sure the OTT is truly random, that there are only two copies, that both copies are quickly destroyed after use, and that each copy is only ever used once. The key stream and individual bits of plaintext are subjected to the logical XOR operation (exclusive-or), which creates the encrypted text. plaintext + key = cipher text ⇒ cipher text + key = plaintext The XOR operation is also known as modulo-2 addition in mathematics. In this instance, each bit of the plaintext and each bit of the key are XORed. Only if the two input bits are distinct from one another will the output bit be "1." The result will be "0" if they are both equal (both 1 or both 0). Take the letter "," which is represented by the number 00011, then combine it with the letter "B," which is symbolised by the number 11001.

B. Advantages

The Vernam Cipher is considered to be a comparatively strong stream cipher which is practically almost impenetrable if the key used is exclusive.

- A block cipher cannot be implemented here since what we need to do here is to encrypt the password in real time which is only possible if the text size that we are sending is small to keep sustainable performance.
- The technique is relatively quick since encryption is carried out using the XOR function.
- As the cipher is symmetric, the same algorithm can be used for decrypting data.

C. Disadvantages

- This cypher requires a key that is the same length as the original data in order to encrypt it. To encrypt a hard drive, for instance, we need a second hard drive the equal size to hold the key.
- This cipher's need that the key data be selected fully at random is another drawback. The majority of the computers we use today are unable to provide such really random keys.

V. CODE

```
<!doctype html>
<html>
<head>
  <title>NIS Keyboard</title>
  <link rel="stylesheet" href="Style.css"/>
  <script>
  function validateForm() {
   var x = document.forms["vform"]["passw"].value;
   if (x == "") {
    alert("Field must not be left blank");
    return false;
   }
   else{
   document.write("The value Entered is : "+ x);
   }
  }
    function myFunction(event) {
    var x = event;
    var treshold = 20000000000;
    var c = {
      0: [], // input encoded
      1: [], // key encoded
      2: [], // cipher encoded
      3: []  // decoding performed
    };
    for (i=0;i<=x.length;++i)
      c[0].push((x[i]+"").charCodeAt(0));
    // c[0] is the plain text
    // generate random key
    for (i=0;i<=c[0].length;++i)
      c[1].push(Math.round(Math.random()*treshold));
    alert("Generated Initial Pad: \n" + c[1].join(", "));
    // generating cipher text
    for (i=0;i<=c[0].length;++i)
      c[2].push(c[0][i] ^ c[1][i]);
    alert("Resulting Cipher : \n" + c[2].join(", "));
    // Recalculating Pad
    for (i=0;i<=c[0].length - 1;++i)
      c[3].push(c[2][i] ^ c[1][i]);
    alert("Has decoding been successful? \n" + ( c[0].join()
== c[3].join() ? "Yes" : "No" ));
  }
  </script>
</head>
<body>
    <div class="cable">
    </div>
    <div class="keyboard">
        <div class="logo">
        NIS REVIEW
        </div>
        <form method="post" name="vform"
onsubmit="return validateForm()">
          <div class="section-a">
             <div class="pass">
           <input type="password" name="passw"
id="ps1" onkeydown="myFunction(event)">
               </div>
           <div class="key backspace">
           <input type="submit"
value="SUBMIT" />
           </div>
```

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

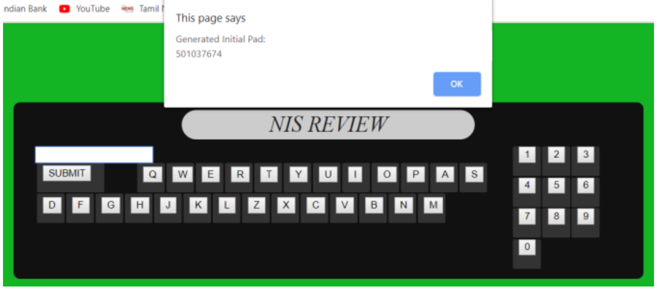
```
  <div class="key letter">
<input type="button" name="q" value="Q">
</div>
    <div class="key letter">
<input type="button" name="w" value="W">
</div>
  <div class="key letter">
 <input type="button" name="e" value="E">
</div>
  <div class="key letter">
 <input type="button" name="r" value="R">
</div>
<div class="key letter">
<input type="button" name="t" value="T">
</div>
<div class="key letter">
<input type="button" name="y" value="Y">
</div>
<div class="key letter">
<input type="button" name="u" value="U">
</div>
<div class="key letter">
 <input type="button" name="i" value="I">
</div>
<div class="key letter">
<input type="button" name="o" value="O">
</div>
<div class="key letter">
<input type="button" name="p" value="P">
</div>
<div class="key letter">
<input type="button" name="a" value="A">
</div>
<div class="key letter">
<input type="button" name="s" value="S">
    </div>
    <div class="key letter">
<input type="button" name="d" value="D">
</div>
    <div class="key letter">
<input type="button" name="f" value="F">
  </div>
    <div class="key letter">
<input type="button" name="g" value="G">
</div>
    <div class="key letter">
<input type="button" name="h" value="H">
    </div>
    <div class="key letter">
<input type="button" name="j" value="J">
    </div>
    <div class="key letter">
<input type="button" name="k" value="K">
  </div>
      <div class="key letter">
<input type="button" name="l" value="L">
  </div>
<div class="key letter">
<input type="button" name="z" value="Z">
</div>
```

```
  <div class="key letter">
  <input type="button" name="x" value="X">
  </div>
  <div class="key letter">
  <input type="button" name="c" value="C">
  </div>
  <div class="key letter">
  <input type="button" name="v" value="V">
  </div>
  <div class="key letter">
  <input type="button" name="b" value="B">
  </div>
  <div class="key letter">
  <input type="button" name="n" value="N">
  </div>
  <div class="key letter">
  <input type="button" name="m" value="M">
  </div>
 </div><!-- end section-a-->
 <div class="section-b">
  <div class="key num dual">
  <input type="button" name="one" value="1">
  </div>
  <div class="key num dual">
  <input type="button" name="two" value="2">

  </div>
  <div class="key num dual">
  <input        type="button"        name="three"
value="3">
      </div>
        <div class="key num dual">
  <input type="button" name="four" value="4">
    </div>
      <div class="key num dual">
  <input type="button" name="five" value="5">
    </div>
  <div class="key num dual">
  <input type="button" name="six" value="6">
  </div>
  <div class="key num dual">
  <input        type="button"        name="seven"
value="7">
  </div>
  <div class="key num dual">
  <input        type="button"        name="eight"
value="8">
  </div>
  <div class="key num dual">
  <input type="button" name="nine" value="9">
  </div>
  <div class="key num dual">
  <input type="button" name="zero" value="0">
  </div>
 <!--END NUMBER KEYS -->
 </div><!--           end
section-b-->
</form>
</div>
```

```
</body>
</html>
```

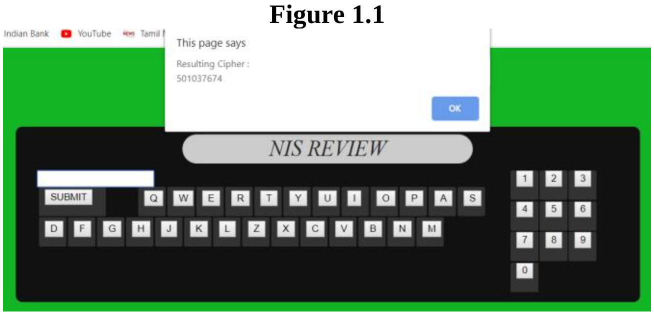
VI. SCREENSHOTS



This page says

Generated Initial Pad:
501037674

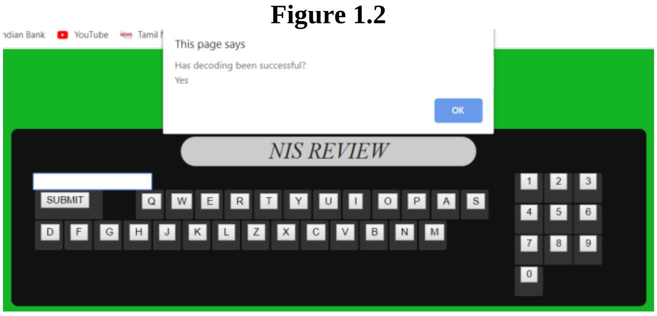
Figure 1.1



This page says

Resulting Cipher :
501037674

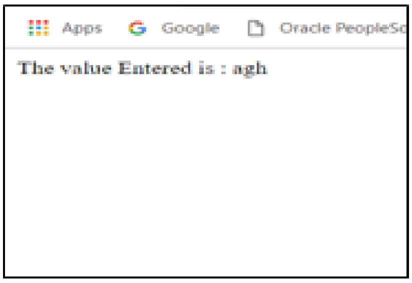
Figure 1.2



This page says

Has decoding been successful?
Yes

Figure 1.3



The value Entered is : agh

Figure 1.4

VII. CONCLUSION

With the intention of preventing Shoulder Surfing assaults, I had suggested a solution in this article that makes use of a distinct hidden keyboard mechanism. Users may quickly enter into their systems using this kind of authentication without worrying about Shoulder Surfers since the character presented on the screen differs from the character recorded in the back end. Even for assaults based on cameras, it is a straightforward and efficient approach. Since the other standard password methods are susceptible to shoulder surfing, this technique can be utilised in the future for applications that require moderate to high security. In general, I want to find a way to tackle contemporary issues using cyphers that already exist.

REFERENCES

1. Om, B., Anuja, S., Akash, P., Yogita, P., & Jagruti, M. (2017). Shoulder Surfing Attack Prevention Using Color Pass Method. *International Research Journal of Engineering and Technology (IRJET), 4(04), 2395-0056.*
2. Ho, P. F., Kam, Y. H. S., Wee, M. C., Chong, Y. N., & Yee, L. (2014). Preventing shoulder-surfing attack with the concept of concealing the password objects' information. *The Scientific World Journal, 2014. [CrossRef]*
3. Hindusree, M., & Sasikumar, R. (2015, February). Preventing shoulder surfing in secure transactions. In 2015 *International Conference on Computing and Communications Technologies (ICCCT)* (pp. 160-163). *IEEE.* [CrossRef]
4. Por, L. Y., Ku, C. S., Islam, A., & Ang, T. F. (2017). Graphical password: prevent shoulder-surfing attack using digraph substitution rules. *Frontiers of Computer Science, 11(6), 1098-1108. [CrossRef]*
5. Nand, P., Singh, P. K., Aneja, J., & Dhingra, Y. (2015, March). Prevention of shoulder surfing attack using randomized square matrix virtual keyboard. In 2015 *International Conference on Advances in C computer Engineering and Applications* (pp. 916-920). *IEEE. [CrossRef]*
6. Prabhu, K. D. D. P. (2018). Image Based Authentication Using Illusion Pin for Shoulder Surfing Attack. *International Journal of Pure and Applied Mathematics, 119(7), 835-840.*
7. Mishra, V., & Verma, N. (2014). Security againstPassword Sniffing using Database Triggers. *International General of Research in Advent Technologies, 2.*
8. Khan, W. Z., Aalsalem, M. Y., & Xiang, Y. (2011). A graphical password based system for small mobile devices. *arXiv preprint arXiv:1110.3844.*
9. Ahsan, M., & Li, Y. (2017). Graphical Password Authentication using Images Sequence.
10. Prabhakaran, S., & Ranjithkumar, M. V. (2018). ADVANCED GRAPHICAL PASSWORDS USING CAPTCHA. *International Journal of Pure and Applied Mathematics, 118(22), 351-357.*
11. Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on *Usable privacy and security* (pp. 1-12). *ACM. [CrossRef]*
12. Chavan, S., Gaikwad, S., Parab, P., & Wakure, G. (2015). Graphical password authentication system. *Department of information Technology, MCT's Rajiv Gandhi Institute of technology, University of Mumbai, Mumbai, Maharashtra, india*, 4(4).
13. Almulhem, A. (2011, February). A graphical password authentication system. In 2011 *World Congress on Internet Security (WorldCIS-2011)* (pp. 223-225). *IEEE. [CrossRef]*
14. Lashkari, A. H., Farmand, S., Zakaria, D., Bin, O., & Saleh, D. (2009). Shoulder surfing attack in graphical password authentication. *arXiv preprint arXiv:0912.0951.*

AUTHORS PROFILE

Esha Kumar, is a Senior Identity and Access Management Analyst, Technologist and Researcher at Schneider Electric, Bengaluru, India. She holds a Bachelor of Technology (B.Tech) degree in Information Technology from Vellore Institute of Technology, Tamil Nadu, India (2020 graduated). Over her tenure of 2+ years working at Schneider Electric Digital, she has gained expertise in various tools in the IAM domain. She has experience configuring applications in PingFederate using OAuth, OIDC, WS-Fed, SAML connectors. She holds technical expertise in managing AWS infrastructure, user MFA and SSO management using PingOne. She also has deep knowledge of network security mechanisms. She has also spearheaded POCs for various Passwordless solutions, including FIDO security keys, PKI smart cards, etc. Over the time, she gained experience in Project management, leading several projects as well. She is a reknowned artist, a trained singer and also an active toastmaster. Her research on secure end-to-end communication using ciphers, led her to develop an award winning prototype for which she received a funding of Rs. 1 lakh. She aspires to be a successful product manager, leading strategy driven teams working in agile methodologies.