Lighting Two Candles With One Flame: An Unaided Human Identification Protocol With Security Beyond Conventional Limit

Asst. Prof. Nida Parkar[1], Asst. Prof. Bhavna Arora[2], Asst. Prof. Priti Rumao[3], Asst. Prof. Chandana Nighut[4]

[1]*(Department of computer Engineering, Atharva College Of Engineering,India)*
[2]*(Department of computer Engineering, Atharva College Of Engineering,India)*
[3]*(Department of computer Engineering, Atharva College Of Engineering,India)*
[4]*(Department of computer Engineering, Atharva College Of Engineering,India)*

Abstract: *Structuring an effective convention for staying away from the danger of account based assault in nearness of an amazing meddler remains a test for over two decades. Amid confirmation, the nonappearance of any safe connection between the prover and verifier makes things much increasingly powerless as, subsequent to watching an edge test reaction pair, clients' mystery may effortlessly get determined because of data spillage. Existing literary works just present new systems with guaranteeing better angles over past ones, while disregarding the perspectives on which their proposed plans adapt ineffectively. Obviously, the greater part of them are a long way from acceptable either are found a long way from usable or absence of security highlights.*
To conquer this issue, we initially present the idea of "spillage control" which puts a bar on the common data spillage rate and significantly helps in expanding both the ease of use and security measures. Prevention, yet additionally, by presenting the risk discovery procedure (in light of the idea of honeyword), our plan "lights two candles". It not just takes out the long terms security and convenience strife under the handy situation, yet alongside risk identification from customer side, it is equipped for ensuring the mystery at the server side under the appropriated structure, and therefore, ensuring security past as far as possible.
Keywords: Authentication, Password, Information spillage, Recording assault, Threat recognition, Threat aversion, Usability.

I. Introduction

Secret phrase base confirmation is one of the most straightforward type of validation as it lessens the human exertion, as it were, amid the character check (Bonneau et al., 2012). Being usable, this factor of verification has been tested under various sort of dangers over the occasions (Marechal, 2008) (Pinkas and Sander, 2002) (Kim et al., 2016) (Pan et al., 2016) (Halevi and Saxena, 2015) (Wang et al., 2016). Despite the fact that the majority of these dangers have been effectively dealt with (Wang and Wang, 2016) (Manulis et al., 2016) (Kontaxis et al., 2013), there are a couple, especially those which include human insight factor, are continuously difficult scientists in building up some productive calculation to handle the ruptures. Recording assault is one such security risk (on customer side) which has serious effect on the secret key based authenti-cation (Yan et al., 2015).

Threat model: Let a veritable client and foe be signified by H and A, separately. Amid enrollment, it is constantly expected that H effectively presents her login qualifications to a remote machine
(recognized as) in a private situation. At the season of validation, sends her login data to by utilizing a login terminal. All through a validation session, with the assistance of some chronicle gadgets (e.g., cover camera), may record the total login data put together by . Afterward, she may utilize that caught data to mimic . This sort of danger is known as perception assault, all the more vitally recording assault, on the secret phrase based verification. In this specific situation, one essential viewpoint is number of perceptions that can make, and dependent on this, the accompanying two classes are proposed in (Sun et al., 2016).

- Type 1: Video catches the whole confirmation process just once.
- Type 2: Video catches the whole validation process more than once (signified as rmax times).

It is trusted that while nature of the danger including Type 1 enemy is shrewd, Type 2 adver-sary draws in herself in an arranged assault (Wiese and Roth, 2015). In spite of the fact that nature of A can truly be both of these practically speaking, yet some striking looks into toward this path select estimation of rmax no more noteworthy than 3 (Kim et al., 2010) (Schaub et al., 2013) (Tari et al., 2006) (Schaub et al., 2012) (Zakaria et al., 2011). These references will be especially useful amid security investigation of our proposition.

Protection methodology: Defense to this danger show basically depends on an essential standard of test ( ) re-sponse ( ) convention. Amid login, sends (or a riddle) to . In light of her unique secret word (distinguished as),then derives with regard to . Consequently, we may generally present in the type of f (,). It is vital to note here that generated by varies in every validation session, in light of which likewise changes. In this manner aloof key passage (i.e., submitting instead of) by refrains to get the unique secret key.

In this paper, we return to the working rule of chronicle assault flexible aloof key section techniques that don't require any protected assistant channel, and concentrate their security perspectives. There is no disavowal of the way that no use of assistant connection mitigates the danger of various side channel assaults, all things considered, (Cˇagalj et al., 2015). Likewise, it serves to login without being reliant on any extra equipment. Be that as it may, as is plainly imparted, thusly, because of data spillage (Yan et al., 2012), these techniques can't withstand the introduction of such a large number of verification sessions.

Inspirations and Contributions: After playing out a comprehensive writing study, we have discovered that plots that don't depend on a safe channel to address the considered risk demonstrate, end up being unusable for the greater part of the clients (Hopper and Blum, 2001) (Bai et al., 2008) (Zhao and Li, 2007) (Weinshall, 2006). This thusly legitimizes the proposed claim1 by Yan et al. in (Yan et al., 2012).

Additionally, we have discovered that to address the secret word spillage from a bargained server (showing to server side risk), as of late proposed edge secret word just validation plans (Camenisch et al., 2015) (store secret key data over numerous servers, and in this way no partnership of servers upto a specific edge can master anything about the mystery) are naturally powerless to adapt to the chronicle based assault at the customer side. In this way, so as to address all the previously mentioned security angles, we have made the accompanying real commitments in this paper.

Commitment 1: We propose a "two passwords based convention", in particular TPP in which a second secret phrase is presented as the "second line of safeguard", that gives security against chronicle based assault. The use of two passwords here not just expands the general security at the customer side, yet in addition gives a circulated security structure to address the risk of secret phrase spillage from a bargained server.

Contribution 2: We present an original thought of controlling the data spillage rate expressly. Express control of data spillage helps in vanquishing A for increasingly number of verification sessions.

Commitment 3: We demonstrate that "second line of resistance" counteracts, yet additionally identifies the assailants' action partly to "light two candles with one fire".

Commitment 4: Along with the exploratory review, we additionally give a hypothetical investigation to mea-beyond any doubt the ease of use standard of the proposed methodology. The ease of use ponder deduces that proposed plan altogether decreases the outstanding burden and guarantees practically same convenience standard as of the heritage pass-word verification.

Guide: whatever is left of the paper is sorted out as pursues. Area 2 gives some fundamental data that will be useful to comprehend the proposed thought. Alongside the idea of spillage control and risk recognition, Section 3 presents the proposed strategy. Area 4 at that point manages the capacity instrument of clients' secret phrase to fit into our proposition. A point by point security and ease of use investigation of the technique is preformed then in Section 5 and Section 6, individually. Pursued by this, Section 7 shows a point by point relative investigation of our plan with the current usable conventions toward this path. At long last, Section 8 finishes up on result of our commitment.

II. Preliminaries

This area manages some applicable data and thoughts that will be useful to comprehend the establishment of the proposed convention. The exchange here will be coordinated through the accompanying points.

1. Target client.
2. Interaction among H and M.
3. Attack examination and data spillage.
4. Basics behind the proposed idea.

II.I. Target client

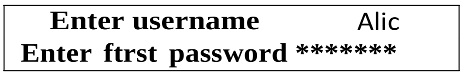
In like manner existing condition of expressions in (Kwon et al., 2014) (Chakraborty and Mondal, 2014), the plan of the proposed TPP convention here depends on the hues. We for the most part utilize 4 hues to emerge the proposed idea. Be that as it may, as appeared (Kwon et al., 2014), for the visually challenged individuals (4.5% of the absolute populace), every one of the 4 used hues in our convention can be supplanted by 4 images (like dark, white, strips and specks). Subsequently, similar to heritage secret word, anyone can utilize our plan, with the exception of the visually impaired individuals.

II.II. Interaction among H and M

Amid enrollment, alongside a username, H chooses two passwords. From a secret key space of every single printable character, the main secret phrase (P1) can be of any length (longer than a limit esteem) chosen by

. As indicated by our plan, being of the length 4, the second secret phrase (2) has a place with a secret word space of 64 characters containing A, B, ..., Z, a, b, ..., z, 0,1, ..., 9, *, # . Both these passwords permit numerous events of any character.

In TPP, amid login, alongside the username, translates 1 through the inheritance (UI) as appeared in Figure 1



Enter username Alic
Enter ftrst password *******

After providing the aforementioned information, indirectly inputs a secret bit from 2 by using the proposed login interface detailed in Section 3.3. In a nutshell, TPP integrates the legacy UI with the proposed idea in Section 3.3 for accepting HJs password information in two phases.

II.III. Attack analysis and information leakage

As discussed earlier, the core of any user authentication system that does not involve any auxiliary hidden link can be explained by a function of the form

$f : P \times C \longrightarrow R$ (1)

The absence of the hidden link together with considered threat model implies that the value of in any phase of authentication will not just be shared between and , but be fully accessed by . Like any other authentication system, we assume that no physical occlusion of user input is involved so that is fully disclosed to everyone. Thus, having full access to both and , a powerful eavesdropper can derive a set of possible secrets containing the original . The attack principle can be realized in the form of the following function

$g : R \times C \longrightarrow S$ (2)

where the set S contains all possible HJs secrets including the actual P.

Shrinking factor is the rate of secret space shrinking after records each authentication session. A derives Si after recording ith (≥ 2) authentication session then shrinking factor (sf) can be expressed as:

$sf = \text{T}_{i-1}\ \text{S}_k$

$\text{T}_{i-1}\ \text{S}_k$

where | denotes S| cardinality of the set S. $^{k=1}$

Let Si be the derived S by A after recording the ith authentication session. As values of R and C vary in each session, consequently, S also differs. Thus, for two different authentication sessions, i and j, derived Si and Sj become different. Therefore from the recorded footages of these two authentication sessions, A can perform an intersection between i and j to reduce the probable candidate elements.

Hence, the leaked information or information leakage after recording kth (> 0) authentication session can be presented in the form of the following equation.

Leaked Information = Sk if k= 1
k=1 Sk if k= 1, 2, ..., i (3)

Above equation suggests that leaked information after each authentication session shrinks the search space in favour of A. Let the entropy (Ma et al., 2010) of P be E. We denote the entropy of information leakage, resulting in secret space shrinking in each session, as OE (inevitably OE > 0). Therefore, after being used for |E/OE| authentication sessions, P gets exposed to A. Under this situation, after utilizing it for |E/OE| authentication sessions, H needs to change her P.

Note 1: Premature attack It is important to note here that after recording multiple sessions, may derive a small list of probable secrets. In future, ifdoes not get a chance to record any further authentication session, then also she may try to login by using those secrets one by one, and eventually discovers the actual P. Though this is a serious concern, but remains unaddressed in the existing literatures.

II.IV. Basics behind the proposed thought

Discussion from the previous section reveals few important facts which may help in increasing the session resiliency of a defense mechanism against the recording attack. To defeat A for more number of sessions, M may

- expand of the secret space to increase E.
- minimize the leakage rate.
- make use of both.

To fulfil the first option, requires to remember more information. But due to limited capacity of human mind this is difficult to achieve. Therefore very little work follow this direction (Weinshall, 2006) (Weinshall and Kirkpatrick, 2004). Methods that satisfy second criterion, often make login process complex for H (Hopper and Blum, 2001) (Asghar et al., 2010). Complex login procedure threats practicality of an approach to be used by the common people. It is quite intuitive that third alternative, combining the first two options, will not be able to maintain any kind of balance between the usability and security aspects.

Our study reveals the fact that easy to use methodologies suffer from high information leakage rate (Kwon et al., 2014) (Roth et al., 2004). As a consequence, sometimes becomes able to recover the secret from a single session recording only. Thus, if leakage rate can be controlled then with the same usability standard, session resiliency of a scheme can be hiked. In this paper, we have tried to achieve this. Due to leakage control, let entropy of the saved information in each session be (inevitably > and> 0). Therefore, explicit control of information leakage improves the session resiliency as the following equation stands.

Control over OT helps in managing the shrinking rate of the secret space. Next, we define the shrinking factor which relates the number of recorded sessions to the likelihood of A successfully authenticating herself. **Deftnition 1.**

The main stage presents Basic Color Identification Protocol (or BCIP) that (like some other technique) releases the data in an unhindered way and gives no security to recognizing the danger.

The second stage presents couple of essential standards for controlling the spillage rate and provides a guidance towards the danger identification.

In conclusion, based on proposed standards, we have changed BCIP and appeared by confining the spillage rate, the modified plan is equipped for identifying the security rupture with improved session flexibility. The changed plan has been named as Improved Color Identification Protocol or ICIP.

BCIP: Proposed system with tradition. Preparing the components of visual interface: As referenced prior, notwithstanding two uncommon images and #, secret word space of 2 is including every one of the letter sets (in both the cases) and the non-negative single digits from 0 to 9. To structure the visual interface, assigns every one of these characters to a 88 lattice by following a particular request (e.g., letters in order first in the in order request, the digits from that point and the images finally). An advantageous request helps in finding her secret key character from the network amid login.

As expressed in Section 2.1, we have utilized 4 hues for shading the lattice in BCIP. The shading task in BCIP is finished by complying with the accompanying guidelines

- Allotment of the hues pursues no particular request.
- Each shading shows up on 16 distinct cells.
- Position of the hues changes in each round of a verification session.

Vehicles for imparting : During confirmation, first sends to . Human just have five conventional faculties to get an upgrade: locate, hearing, contact, smell and taste. Up to an application can't encode a data by creating last two boosts, along these lines can't make utilization of taste or smell to exchange any data. Accordingly, sight, hearing and contact stay as conceivable hopefuls. Here, we investigate the visual channel to exchange C obviously from M to H.

Cooperation among H and M: After entering the principal secret phrase (P1) data, M sends a number esteem (t) somewhere in the range of 1 and 4 (length of P2) to H, by methods for a visual flag. Beginning from the primary file, H at that point recovers the character set at tth record position of P2. Give the got character a chance to be meant by η (2). A reference to η is then used to create in each round of that confirmation session.

At each round, M arbitrarily rearranges the assignments of the hues on the matrix. To pass a verification round, H needs to recognize the shading showed up at the matrix's cell containing η. Give the distinguished shading a chance to be ηC. Login interface of BCIP contains 4 diverse shading catches which are utilized as the method of HJs connection with the framework. Each shading catch holds one of those 4 hues that has been utilized to shading the network. H at that point presses ηC catch to influence M to comprehend the distinguished shading by her.

Login model: Let the picked 2 by be S7Ay. We additionally accept that like the 6 digit PIN passage technique in (Florˆencio et al., 2007), every confirmation session in BCIP is including 6 login rounds. Without loss of sweeping statement, on the off chance that gets 3 as „ at that point the chose secret key character by her future A. From there on in each ensuing round of that session, will present that shading which will show up on the letters in order An on the network. Figure 2 demonstrates an example of the login technique in a session for the secret key character A. We have utilized green, orange, red and yellow as 4 distinct hues to plan BCIP.

Assault strategy and data Leakage in BCIP: From the recorded video, A first takes a gander at the shading catch squeezed by H in every confirmation round. From there on, A discovers each one of those characters from the lattice which are of indistinguishable shading from of that shading catch. Subsequently, the reaction of H from the first round confounds An among 16 conceivable outcomes. For the login model appeared in Figure 2, spilled data after the first round produces r1 containing A, F, M, N, O, T, U, W, b, d, e, g, l, r, s, y . Underneath we have demonstrated the spilled data toward the finish of each round for the particular confirmation session, showed in Figure 2.

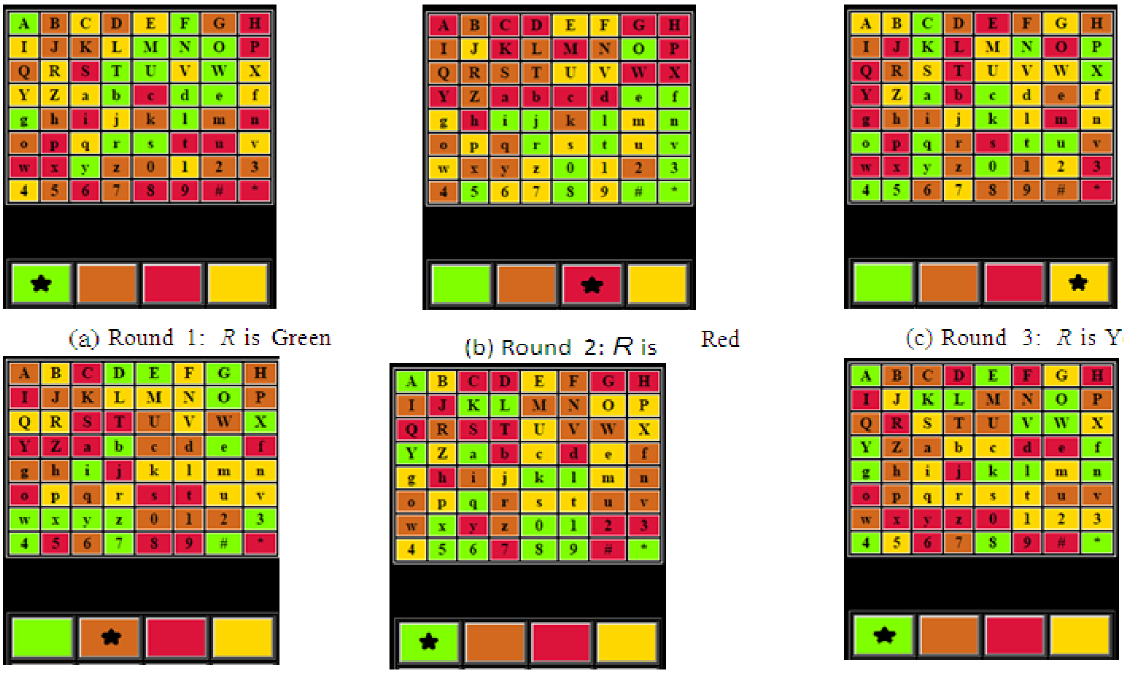
- First round: Leaked data Sr1 = {A, F, M, N, O, T, U, W, b, d, e, g, l, r, s, y}.
- Second round: Sr2 = {A, C, D, G, H, K, M, P, W, X, Y, a, b, c, d, h}. Spilled data Sr1 ∩ Sr2 = {A, M, W, b, d}.
- Third round: Sr3 = {A, B, G, M, S, U, V, W, Z, d, f, l, j, n, 2,7}. Spilled data Sr1 ∩ Sr2 ∩ Sr3 = {A, M, W, d}.
- Fourth round: Sr4 = {A, H, J, K, P, U, W, c, d, g, h, q, 0, 1, 2, 6}. Spilled data Sr1∩Sr2∩Sr3∩Sr4 = {A, W, d}.
- Fifth round: Sr5 = {A, K, L, Y, a, k, l, q, x, 0, 1, 5, 6, 8, 9, *}. Spilled data Sr1 ∩ Sr2 ∩ Sr3 ∩ Sr4 ∩ Sr5 = {A}.

In spite of the fact that exceptionally easy to utilize, yet above model demonstrates that BCIP can't withstand the introduction of a solitary verification session.

All the secret phrase characters in 2 are autonomous of one another and just uses a solitary piece from 2 to go through the BCIP. Subsequently, alongside evaluating the spillage rate in BCIP, next we will examine the security given by a solitary secret word character against the chronicle assault.

Evaluating the spillage rate: We express that in the wake of breaking down a confirmation round, in the event that An is befuddled among m (> 1) potential outcomes then the following round has likelihood 1-PDisclosure of containing enough infor-mation to protect the mystery of being spilled. Here PDisclosure is the likelihood related with: in a round, none (unavoidably aside from the first secret key character) of the m-1 plausible components from the past round gets indistinguishable shading from of the first secret phrase character. PDisclosure can be formalized by utilizing the accompanying condition.

PDisclosure
m−1
=
k=1
(64 − k) − (m − 1) 64 − k
(6)



(a) Round 1: *R* is Green

(b) Round 2: *R* is Red

(c) Round 3: *R* is Yellow

(d) Round 4: *R* is Orange

(e) Round 5: *R* is Green

(f) Round 6: *R* is Green

Figure 2: Login example in BCIP: Above figure shows color responses by H for the password character "A" in each round of the authentication session. The color button hit by H in each round is marked by a "$*$" symbol.

It is very evident that in the wake of chronicle the first round, determines m (here 16) plausible components. This infers in the following round, the shade of the first secret key character must show up on somewhere around one of the rest of the 15 characters from the first round to muddle . This yields the estimation of PDisclosure as 0.007. Along these lines, toward the finish of second round, with no spillage control component, BCIP can monitor the secret key character of with the likelihood 0.993. Yet, as the estimation of m goes down and out the proliferation of each login round, subsequently, in the wake of chronicle a total session, odds of uncovering the real secret word character turns out to be fundamentally high.

Mimicking the quality of BCIP against account assault: Figure 3 demonstrates the impact of infor-mation spillage on BCIP while tested for a hundred confirmation sessions. We found that in 92% of situations, BCIP can't ensure the mystery for a solitary validation session. For rest of the cases, the mystery has been secured for two validation sessions as it were.

Addressing the premature attack: For addressing the issue mentioned in the Note 1, the following strategy to distinguish between H and A has been adopted.

stores the leaked information in the database after successful login attempt by in an authenti- cation session. In the immediate next session, will construct few groups by using those obtained leaked information from the previous session. The formed groups will be mutually exclusive while one of them will definitely contain the original P.

If submitted in this session corresponds to any other group except one, holding the original, then will detect that is trying to login by using the recording footage (leaked information) of the previous authentication session.

- On detecting this attack, M acts according to the security policy set by the system administrator.

Detection strategy here is influenced by the concept of another threat detection mechanism, namely honeyword (false password) based authentication technique (Cohen, 2006) (ref. to appendix A), currently is being used in many domains (Catuogno et al., 2015).

III. Proposed Methodology

As P1 is transcribed through a legacy UI, thus it does not require any further introduction. In this section, we mainly focus on how makes use of the second password (2) to defeat from performing the recording attack. Contribution in this section unfolds in the following three phases.

IV. Usability examination

In TPP, the accommodation of P1 requires no control from HJs end and accordingly, it gives indistinguishable ease of use standard from of the heritage secret phrase convention. Yet, so as to create R with reference to C, H needs to process 2 in like manner and this assumes a noteworthy job in deciding the general convenience standard of the TPP. Along these lines, (until determined expressly) this area fundamentally centers around the ease of use standard given by the ICIP.

We decide the ease of use standard of the ICIP both from the hypothetical and test purpose of perspectives. As talked about in (Yan et al., 2012), the hypothetical examination here is free of a specific client set and henceforth the result stays static under any circumstance. The ease of use standard likewise incorporates the HBAT ease of use parameters which are (a) framework obstruction, (b) weight on-memorability and (c) grammatical error security.

IV.I. Theoretical investigation:

This system is primarily determined by two parts Cognitive Workload (CW) and Memory Demand (MD). CW impacts the login time and is estimated against all out response time (in a flash) required by the nuclear psychological tasks. There are four very much characterized nuclear psychological activities related with a human recognizable proof convention, and these are

- (Single/Parallel) Recognition (Sternberg, 1969)
- (Free/Cued) Recall (Nobel and Shiffrin, 2001)
- (Single-target/Multi-target) Visual Search (Woodman and Chun, 2006)
- Simple Cognitive Arithmetic (Campbell and Xue, 2001)

Subjective over-burden: From the visual test, sending the file esteem, first plays out a signaled review to see her secret phrase character. The response time for prompted review (CR) can be gotten through (0.3694+0.0383 g ψ), where g (default esteem is 1 here) indicates number of components requires to recollect for playing out the login in a round (Nobel and Shiffrin, 2001) (Corbin and Marquer, 2008). ψ is the proportion between the signaled review and single thing acknowledgment, and the default estimation of this is 1.969 (Nobel and Shiffrin, 2001). For 2 of length 4, needs to perform signaled review once toward the start of a validation session comprising of 6 rounds. In this way, normal signaled review time for each round can be determined as (CR/6) 4 which yields $\alpha 1 = 0.448$ 2 or 0.299.

So as to determine a reaction, requires to look through the right intimation from a lot of w (likewise alludes as window estimate) fluctuating items, showing on the screen. Amid distinguishing proof of a solitary focus on, the response time of H can be planned as $\alpha 2 = 0.583 + 0.0529 \times w$ (Woodman and Luck, 2004). By utilizing ICIP, H needs to recognize a shading from a solitary static cell on the matrix all through a session. In this way, w can be accepted as 1 here which restores the estimation of α2 as 0.6359.
Above dialog surmises that ICIP infers CW as $\alpha 1 + \alpha 2 = 0.9349$ for each round.

Memory request: For MD activity, the expense of each plan can be determined as the proportion between length of P2 and λop: where λop is the exactness rate of comparing memory recovery task inside a fixed remembrance time. Since acknowledgment is a lot simpler than review thusly, λop ends up 29.6% and 84.8% for review and acknowledgment, individually (Hogan and Kintsch, 1971). Along these lines MD in ICIP can be calcu-lated as 13.51, for the length of P2 as 4 and λop as 29.6%.

At long last, a general score of human power, HP, can be determined as the result of CW for a session and MD. Consequently, HP for ICIP can be gotten as 0.9349 6 13.51 = 75.78, which is altogether less contrasted with the current conventions toward this path (see subtleties Section 7).

IV.II. Experimental examination

To lead exploratory examination, we took assistance from 93 members (all having right to-typical visual perception) and recognized this arrangement of members as P∗. The members were equipped for working PCs and their age shifted between 19 to 37. Among them, 18 members were distinguished as gifted as they appreciate playing quick computer games (Kwon et al., 2014). It is vital to note here that as per the report in (Teh et al., 2016), the vast majority of the examinations around there utilized a test bunch somewhere in the range of 11 and 25, while not many utilized a test gathering of at least 50 members (Kambourakis et al., 2016). Subsequently, we trust that a lot of 93 members will give increasingly base to our trial consider.

The examination was led into two stages preparing stage and test stage. In preparing stage, we initially gave the members a fast inspiration driving our work and exhibited the working guideline of the proposed TPP. For delineating the model, we utilized the 10 Desktops of our foundation lab. From that point, we approached every one of them for login by utilizing the predefined login accreditations set by us. After every member played out the login, we gave them a whole day to utilize the proposed model (in the research facility) for getting habituated with it. In the test stage, we gathered the test information for 5 days and every member was permitted to login for multiple times. Acquired login time from talented helped us to decide the precision of inferred CW for the ICIP in the past area.
From 93 3 = 279 login endeavors, underneath we present some eminent data/results of our experi-ment.

- The proportion between the gifted and non-talented members was 1 : 4 (around).
- 16 times members neglected to enter P1 accurately.
- 23 times members flopped in creating the substantial reactions by utilizing P2.
- Overall multiple times they neglected to login utilizing TPP.

Especially for ICIP, the normal login time of the talented members was recorded as 1.31 (7.96/6) seconds per round, close enough to the deliberate CW parameter with a permissible little distinction (Yan et al., 2012).
The normal info accommodation time amid entering 1 (set as "anhour") was gotten as 3.2 seconds considering the effective login endeavors as it were.

- The normal effective mystery accommodation time for every one of the members was caught as 15.49 seconds (for entering both the mystery data P1 and P2).

Subsequent to conducing the test we requested that the members fill a criticism structure to rate our proposed model. The got criticism result was discovered promising and is introduced in Table 2.
Table 2: Recorded criticisms from the 93 members

Choices	Agreed participants	Percentage (%)
Love to use	19	20.43
Simple to use	26	27.95
Find usable	35	37.64
Bit difficult	8	8.6
Amazingly difficult	2	2.15
Not sure	3	3.23

IV.III. Evaluating ICIP under the HBAT ease of use highlights

Framework impedance: If a honeyword based methodology impacts the secret key decision of (e.g., powers to recall some additional data) at that point it fundamentally impacts on clients' comfort. As the proposed model does not impact the secret phrase decision of , along these lines framework obstruction can be considered as unimportant.

Weight on memorability: If a honeyword based methodology impacts the secret phrase decision then that May put some weight on Js mind as she may need to recall some extra data. This component likewise has extreme effect on ease of use standard and proposed ICIP does exclude this as well.

Grammatical mistake wellbeing: A honeyword age calculation is called error safe if composing botch of rarely coordinates with any honeyword. Give us a chance to expect that reaction groupings created by two subgroups in ICIP

are < Cg1 − Cg1...Cg1 − Cg1 > and < Cg2 − Cg2...Cg2 − Cg2 >; where Cgi symbolizes shading reaction comparing to amass I in the kth round. Without loss of sweeping statement, in the event that we accept that the mystery bit of

g1 g1 g1 g1

P2 is having a place with gathering 1 then H pursues the reaction arrangement < C1 − C2 ...C5 − C6 >. For any verification round I (1 ≤ I ≤ 6), as Cg1 and Cg2 dependably contrast, in this manner a couple of composing oversights will never yield

to < Cg2 − Cg2...Cg2 − Cg2 >. In this way proposed ICIP is exceptionally grammatical error safe.

V. Comparative Analysis

For contrasting proposed TPP and the current conventions, we just consider those techniques which are usable by atleast 80% of the clients (as revealed in the individual writings). Interestingly, difficult to utilize techniques, similar to low intricacy CAS (Weinshall, 2006) which requests 30 articles to be recollected by or, HB convention (Hopper and Blum, 2001), requires cryptographic calculation from , have been kept outside of this near examination.

Table 3: Comparative examination of techniques as far as security highlights. Session strength against chronicle assault for S3PAS and CHC convention are acquired from the investigation announced in (Yan et al., 2012). While security of PAS against account assault is taken from the investigation, made by Li et. al (Li et al., 2009). Variable s (0) in the above table indicates a whole number esteem. LR means number of login adjusts in a session. ~ shows with the exception of the principal verification session.

Method Secret
length (A) Total
components (n) Window Password
measure (w) space Pr[RKS]
/round LR Session
resiliency Pr[Threat
detection]
CHC 5 8
112 83 1.341 × 10 0.22 5 3 0
PAS 4+2s 5 N/A 13 4.225 × 10 0.25 4 9+s 0
S3PAS 4 7
94 94 7.9 × 10 0.076 4 8 0
TPP 6+4 95 64 1.2 × 10 1.3 × 10 ×0.25 1+6 12 0.75 ~
19 −12

Table 4: Comparative examination of strategies as far as ease of use highlights. CW per round, for every one of the strategies (with the exception of S3PAS) is gotten from (Yan et al., 2012). For S3PAS, CW/round is determined by following indistinguishable heading from referenced in Section

VI. LR demonstrates number of login adjusts in a session.

Method LR Avg. login time
talented client (sec) Avg. login time
(sec) all user Error rate (%)
all user CW/round
(sec) MD HP = CW × LR
×MD (×102)
CHC 5 56 65.5 17.1 9.326 16.89 7.87
PAS 4 33.44 41.52 15.2 6.837 13.51 3.69

S3PAS	4	36.56	50.8	15.7	10.597	13.51	5.55		
TPP	1+6	1.3 + 7.86		3.2 + 12.29		10.04	0.9349	20.27 + 13.51	1.45 + 0.7578

Because of involvement of human intelligence factor, providing good usability standard is a must criterion of an adoptable human identification protocol. We compare TPP with three existing usable protocols (also certified by the authors in (Yan et al., 2012)), Convex-Hull-Click (CHC) (Asghar et al., 2013), PAS (Bai et al., 2008) and S3PAS (Zhao and Li, 2007). The experimental data (for usability analysis) were obtained from participants belonging to P+ set: where P+ P∗ and as of P∗, P+ maintains a steady ratio between the skilled and non-skilled around 1 : 4 for obtaining the unbiased results. Table 3 and Table 4 show comparative study of the methods from the security and usability perspectives, respectively.

It is important to note here that submission of 1 does not demand any significant CW, but requires some MD. Therefore, for the default length of 1 as 6, MD can be calculated as 20.27.

Along with Discussion 5 and Discussion 6 in the previous section, the comparative analysis shows that proposed scheme stands strong in terms of fulfilling all the security aspects. Also, with a remarkable property of threat detection, TPP attains the highest usability standard among all.

VII. Conclusion

In this paper we have tried to break the chain of “Drawback-SmallImprovement-Drawback-SmallImprovement” in the research domain of human identification protocol for addressing the threat of recording attack. Pro-pose mechanism here not only reduces the human effort at a large scale, but also offers few security features that are missing in the existing state of arts. The usage of two passwords contributes in enhancing the security standard from many aspects like managing both the server and client side threats. To the best of our believe, we, for the first time introduce the idea of honeyword into recording attack resilient unaided human identification protocol design. Exploring the concept of honeyword for threat detection, ensuring the security at both the (client and server) ends and extremely simple login procedure make the proposed idea deployable in practice.

References

[1]. Asghar, H.J., Li, S., Pieprzyk, J., Wang, H., 2013. Cryptanalysis of the convex hull click human identification protocol. International Journal of Information Security 12, 83–96.

[2]. Asghar, H.J., Pieprzyk, J., Wang, H., 2010. A new human identification protocol and coppersmiths baby-step giant-step algorithm, in: International Conference on Applied Cryptography and Network Security, Springer. pp. 349–366.

[3]. Bai, X., Gu, W., Chellappan, S., Wang, X., Xuan, D., Ma, B., 2008. PAS: predicate-based authentication services against powerful passive adversaries, in: Computer Security Applications Conference, 2008. ACSAC 2008. Annual, IEEE. pp. 433– 442.

[4]. Bonneau, J., Herley, C., Van Oorschot, P.C., Stajano, F., 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes, in: Security and Privacy (SP), 2012 IEEE Symposium on, IEEE. pp. 553–567.

[5]. Broder, A., Mitzenmacher, M., 2004. Network applications of bloom filters: A survey. Internet mathematics 1, 485–509.

[6]. C̀agalj, M., Perkoviĉ, T., Bugariĉ, M., 2015. Timing attacks on cognitive authentication schemes. IEEE Transactions on Information Forensics and Security 10, 584–596.

[7]. Camenisch, J., Lehmann, A., Neven, G., 2015. Optimal distributed password verification, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, ACM. pp. 182–194.

[8]. Campbell, J.I., Xue, Q., 2001. Cognitive arithmetic across cultures. Journal of Experimental Psychology: General 130, 299.

[9]. Catuogno, L., Castiglione, A., Palmieri, F., 2015. A honeypot system with honeyword-driven fake interactive sessions, in: High Performance Computing & Simulation (HPCS), 2015 International Conference on, IEEE. pp. 187–194.

[10]. Chakraborty, N., Mondal, S., 2014. Color pass: An intelligent user interface to resist shoulder surfing attack, in: Students’ Technology Symposium (TechSym), 2014 IEEE, IEEE. pp. 13–18.

[11]. Cohen, F., 2006. The use of deception techniques: Honeypots and decoys. Handbook of Information Security 3, 646–655.

[12]. Corbin, L., Marquer, J., 2008. Effect of a simple experimental control: The recall constraint in sternberg’s memory scanning task. European Journal of Cognitive Psychology 20, 913–935.

[13]. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X., 2014. The tangled web of password reuse., in: NDSS, pp. 23–26. Defense Information Systems Agency (DISA) for the Department of Defense (DoD), 2011. Application security and develop-

[14]. ment: Security technical implementation guide (STIG), version 3.

[15]. Erguler, I., 2016. Achieving flatness: Selecting the honeywords from existing user passwords. IEEE Trans. Dependable Sec. Comput. 13, 284–295.

[16]. Florêncio, D., Herley, C., Coskun, B., 2007. Do strong web passwords accomplish anything? HotSec 7.

[17]. Halevi, T., Saxena, N., 2015. Keyboard acoustic side channel attacks: exploring realistic and security-sensitive scenarios. International Journal of Information Security 14, 443–456.

[18]. Hogan, R.M., Kintsch, W., 1971. Differential effects of study and test trials on long-term recognition and recall. Journal of Verbal Learning and Verbal Behavior 10, 562–567.

[19]. Hopper, N.J., Blum, M., 2001. Secure human identification protocols, in: Advances in cryptology-ASIACRYPT 2001. Springer, pp. 52–66.

[20]. Juels, A., Rivest, R.L., 2013. Honeywords: Making password-cracking detectable, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, ACM. pp. 145–160.

[21]. Kambourakis, G., Damopoulos, D., Papamartzivanos, D., Pavlidakis, E., 2016. Introducing touchstroke: keystroke-based authentication system for smartphones. Security and Communication Networks 9, 542–554.

[22]. Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J.W., Nicholson, J., Olivier, P., 2010. Multi-touch authentication on tabletops, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM. pp. 1093–1102.

[23]. Kim, M., Jung, Y., Song, J., 2016. A modified exhaustive search on a password system using sha-1. International Journal of Information Security , 1–7.

[24]. Kontaxis, G., Athanasopoulos, E., Portokalidis, G., Keromytis, A.D., 2013. Sauth: Protecting user accounts from password database leaks, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, ACM. pp. 187–198.

[25]. Kwon, T., Shin, S., Na, S., 2014. Covert attentional shoulder surfing: Human adversaries are more powerful than expected. Systems, Man, and Cybernetics: Systems, IEEE Transactions on 44, 716–727.

[26]. Li, S., Asghar, H.J., Pieprzyk, J., Sadeghi, A.R., Schmitz, R., Wang, H., 2009. On the security of PAS (Predicate-based authentication service), in: Computer Security Applications Conference, 2009. ACSAC’09. Annual, IEEE. pp. 209–218.

[27]. Ma, J., Yang, W., Luo, M., Li, N., 2014. A study of probabilistic password models, in: Security and Privacy (SP), 2014 IEEE Symposium on, IEEE. pp. 689–704.

[28]. Ma, W., Campbell, J., Tran, D., Kleeman, D., 2010. Password entropy and password quality, in: Network and System Security (NSS), 2010 4th International Conference on, IEEE. pp. 583–587.

[29]. Manulis, M., Stebila, D., Kiefer, F., Denham, N., 2016. Secure modular password authentication for the web using channel bindings. International Journal of Information Security 15, 597–620.

[30]. Marechal, S., 2008. Advances in password cracking. Journal in computer virology 4, 73–81.

[31]. Nobel, P.A., Shiffrin, R.M., 2001. Retrieval processes in recognition and cued recall. Journal of Experimental Psychology: Learning, Memory, and Cognition 27, 384.

[32]. Pan, X., Ling, Z., Pingley, A., Yu, W., Zhang, N., Ren, K., Fu, X., 2016. Password extraction via reconstructed wireless mouse trajectory. IEEE Transactions on Dependable and Secure Computing 13, 461–473.

[33]. Pinkas, B., Sander, T., 2002. Securing passwords against dictionary attacks, in: Proceedings of the 9th ACM conference on Computer and communications security, ACM. pp. 161–170.

[34]. Provos, N., Mazieres, D., 1999. A future-adaptable password scheme., in: USENIX Annual Technical Conference, FREENIX Track, pp. 81–91.

[35]. Roth, V., Richter, K., Freidinger, R., 2004. A pin-entry method resilient against shoulder surfing, in: Proceedings of the 11th ACM conference on Computer and communications security, ACM. pp. 236–245.

[36]. Schaub, F., Deyhle, R., Weber, M., 2012. Password entry usability and shoulder surfing susceptibility on different smartphone platforms, in: Proceedings of the 11th international conference on mobile and ubiquitous multimedia, ACM. p. 13.

[37]. Schaub, F., Walch, M., Könings, B., Weber, M., 2013. Exploring the design space of graphical passwords on smartphones, in: Proceedings of the Ninth Symposium on Usable Privacy and Security, ACM. p. 11.

[38]. Sternberg, S., 1969. Memory-scanning: Mental processes revealed by reaction-time experiments. American scientist 57, 421–457. Sun, H.M., Chen, S.T., Yeh, J.H., Cheng, C.Y., 2016. A shoulder surfing resistant graphical authentication system. IEEE

[39]. Transactions on Dependable and Secure Computing .

[40]. Tari, F., Ozok, A., Holden, S.H., 2006. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords, in: Proceedings of the second symposium on Usable privacy and security, ACM. pp. 56–66.

[41]. Teh, P.S., Zhang, N., Teoh, A.B.J., Chen, K., 2016. A survey on touch dynamics authentication in mobile devices. Computers & Security 59, 210–235.

[42]. Wang, D., Wang, P., 2016. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Transactions on Dependable and Secure Computing .

[43]. Wang, D., Zhang, Z., Wang, P., Yan, J., Huang, X., 2016. Targeted online password guessing: An underestimated threat, in:

[44]. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM. pp. 1242–1254.

[45]. Weinshall, D., 2006. Cognitive authentication schemes safe against spyware, in: Security and Privacy, 2006 IEEE Symposium on, IEEE. pp. 6–11.

[46]. Weinshall, D., Kirkpatrick, S., 2004. Passwords you'll never forget, but can't recall, in: Extended abstracts of the 2004 Conference on Human Factors in Computing Systems, CHI 2004, Vienna, Austria, April 24 - 29, 2004, pp. 1399–1402.

[47]. Wiese, O., Roth, V., 2015. Pitfalls of shoulder surfing studies, in: NDSS Workshop on Usable Security, pp. 1–6.

[48]. Woodman, G.F., Chun, M.M., 2006. The role of working memory and long-term memory in visual search. Visual Cognition 14, 808–830.

[49]. Woodman, G.F., Luck, S.J., 2004. Visual search is slowed when visuospatial working memory is occupied. Psychonomic Bulletin & Review 11, 269–274.

[50]. Yan, Q., Han, J., Li, Y., Deng, R.H., 2012. On limitations of designing leakage-resilient password systems: Attacks, principals and usability, in: 19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012, pp. 1–16.

[51]. Yan, Q., Han, J., Li, Y., Zhou, J., Deng, R.H., 2015. Leakage-resilient password entry: challenges, design, and evaluation. Computers & Security 48, 196–211.

[52]. Zakaria, N.H., Griffiths, D., Brostoff, S., Yan, J., 2011. Shoulder surfing defence for recall-based graphical passwords, in: Proceedings of the Seventh Symposium on Usable Privacy and Security, ACM. p. 6.

[53]. Zhao, H., Li, X., 2007. S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme, in: Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, IEEE. pp. 467–472.