Theme Interception Sequence Learning: Deflecting Rubber-Hose Attacks Using Implicit Learning

Shyam Diwakar[1], Priya Chellaiah[2], Bipin Nair[1], and Krishnashree Achuthan[2]

[1] Amrita School of Biotechnology, Amrita Vishwa Vidyapeetham (Amrita University),
Amritapuri, Clappana P.O., Kollam, 690 525, Kerala, India
[2] Amrita Center for Cybersecurity, Amrita Vishwa Vidyapeetham (Amrita University),
Amritapuri, Clappana P.O., Kollam, 690 525, Kerala, India
shyam@amrita.edu

Abstract. Existing cryptographic systems use strong passwords but several techniques are vulnerable to rubber-hose attacks, wherein the user is forced to reveal the secret key. This paper specifies a defense technique against rubber-hose attacks by taking advantage of image sequence-based theme selection, dependent on a user's personal construct and active implicit learning. In this paper, an attempt to allow the human brain to generate the password via a computer task of arranging themed images through which the user learns a password without any conscious knowledge of the learned pattern. Although used in authentication, users cannot be coerced into revealing the secret key since the user has no direct knowledge on the choice of the learned secret. We also show that theme interception sequence learning tool works significantly well with mixed user age groups and can be used as a secondary layer of security where human user authentication remains a priority.

Keywords: Rubber-Hose Attack, Implicit learning, TISL, Authentication.

1 Introduction

Secret key that involves a user to securely work with a system plays a major role in most cryptographic models. Even though these passwords can be stored securely, they remain vulnerable to eavesdropping, dictionary attacks, social engineering and shoulder surfing. Studies have shown that selecting the password is also related to human cognition and psychology [1]. Knowledge-based passwords may be vulnerable to coercion attacks. Rubber-hose cryptanalysis [2] is an easy way to defeat cryptography in some scenarios.

Securing passwords is one of the most significant problems today. Long and difficult-to-guess passwords usually add to user-related memory and storage issues. Although biometric authentication could be used [3,4,5] to overcome this, post-attacks, re-validation is not easy in biometric techniques as data is physiology-dependent. Images allow the human ability to understand and remember pictorial representations better than the alpha-numeric complexes of meaningless strings. Although image-based authentication schemes allow users to learn strong secret passwords that are easily memorable [6,7,8,9], these systems are not resistant to

S.C. Satapathy et al. (eds.), *Proc. of the 3rd Int. Conf. on Front. of Intell. Comput. (FICTA) 2014 – Vol. 1*, Advances in Intelligent Systems and Computing 327, DOI: 10.1007/978-3-319-11933-5_55

rubber-hose attacks due to recall awareness. Previous studies have discussed about incoercible multiparty computation and schemes of deniable encryption [10,11].

1.1 Rubber-Hose Attacks and Existing Techniques

Rubber-Hose attacks are a type of coercion attacks in which a user is physically forced by the attacker until the secret password is retrieved. Reports on the Syrian war shows that people were systematically tortured and killed using rubber belts [12] while extracting critical information.

This paper showcases the design of an anti-rubber hose attack scheme and the implementation of the tool using implicit learning, centered on cognitive psychology [13,14,15]. The technique was based on sequential arrangement of image strips [6,7] and the characteristics of associative memory recall. Representing an information using images, specifically with comic strips, increases the attention, comprehension, recall and adherence ability in human subjects. This correlation between the images and the memory construct was used in the implementation of our technique [16,17,18]. Knowledge learned implicitly are not consciously accessible to or may not be described explicitly by the person being trained [13,14,15,19,20]. Everyday examples of this phenomenon include swimming, riding bicycle, playing golf, playing musical instruments etc. These tasks are implicitly understood although explicit declaration may not be straight forward.

To overcome the problem with recall-based authentication, some recognition-based authentication schemes used images instead of textual passwords. Human ubiquity to graphical information has been better with graphical sequences than with texts and numbers [6, 7, 8,9]. Pictures or comic strips are also used in several fields such as health organizations [21], educational institutions [22], and in others [23] to enhance communication or to motivate learning. We used image sequences in order to take advantage of human ability to elicit planned emotions as a way of authenticating human user and user's emotional individuality. Implicit learning plays a major role in designing coercion-resistant security systems [2]. In techniques like ours, a user learns the secret key through implicit learning that may be detected during authentication but may not be described explicitly by an observer or the user. As part of this anti-coercion tool, users were initially trained to do a special task called Theme Interception Sequence Learning (TISL).

1.2 TISL Threat Model and Design

The tool was designed to be used as an alternate or secondary authentication system which identifies a human user, based on a pre-validated sequence of image patterns. The technique also allows physical presence of user to be validated at the time of authentication. Our tool was implemented in two phases: Training and Authentication. Training was done using a computer task that results in implicit learning of specific sequence of images which became the secret key for authentication. The server stores the trained pattern and used it to authenticate the user successfully. The attacker may not identify the same pattern unlike the user since the attacker is unaware of the training sequence.

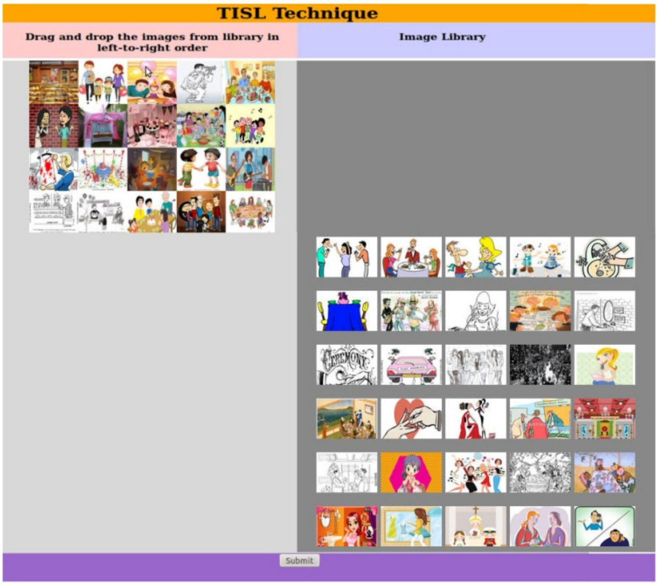
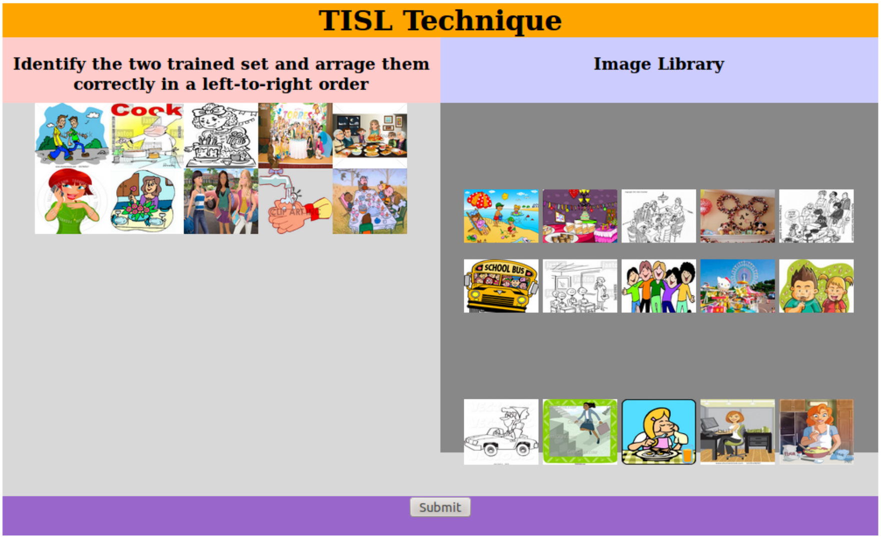

TISL Technique
Drag and drop the images from library in left-to-right order
Image Library
Submit

Fig. 1. TISL training. Screenshot of training task in progress

2 Theme Interception Based Task

The technique proposed in this paper is referred to as Theme Interception Sequence Learning (TISL) task. TISL task was based on the idea of sequence learning [24]. In this implementation, we have used various sets of comic strip series with different themed sequences. Theme interception sequence learning was based on Serial Interception Sequence Learning (SISL) [2]. In SISL task, the users developed sensitivity to patterned symbol information without any conscious knowledge of the learned information. In TISL unlike SISL, symbol sequences were not used. In a TISL task, users were sensitized implicitly to the structured information by intercepting image sequences. An image library containing different themes was presented on the right side and an empty grid was presented on the left side of the computer screen (see Fig. 1).The task-level objective for the user was to intercept the object. Interception was performed by selecting images from same theme and re-arranging onto the grid provided on the left side as per user choice. During the 20 to 25 minute training process, a user performed several TISL tasks and the sets of the image library followed covertly embedded repeated themes in 75% of the trials. Each image in the image library represented an individual event within a set in a specific theme. The image library for the authentication task (see Fig. 2) contained different sets including both trained as well as untrained sets of comic strip images. The sequences for authentication from within the trained sets were chosen randomly so that the user would get different sets during each authentication task. Participants implicitly identified the themes by repeatedly performing the TISL task.



TISL Technique

Identify the two trained set and arrage them correctly in a left-to-right order

Image Library

Fig. 2. TISL authentication. Screenshot of authentication task in progress

3 Implementation of an Anti-Rubber-Hose Attack Tool

The concept behind TISL task was to store a secret key ‘sequence’ in the human brain that could be retrieved during authentication, but may not be described verbally. It was possible to train users to remember a sequence that could be used as an alternative to password-based authentication. The image sequence themes included real life scenes like, going on a trip, daily routine of an office staff, preparing food, having dinner, playing with friends, caring pets, celebrating birthdays, festivals, marriage function etc. Each image inside a set represents an event that occurred in that theme. These events could be arranged in any order. A fixed order for these events was avoided. User choice was defined by the perceived personal or impersonal constructs as identified by the observer. Such sequence orders may be different for different users for the same theme and thereby allowing uniqueness in the pass sequence.

The user identification system was designed in two phases: training and authentication. For training task, each user was presented with an image library consisting of several themes (see Table 1). User learned five themes from the set $T = \{T_1, T_2, T_3, T_4, T_{5\ldots}\ T_n\}$. Each theme contained several sets such as $T_i = \{S_{jk}\}$ where $i = j = 1$ to n and k = 1 to m. There were five images within each set representing five events for every theme as $S_{jm} = \{x_{ef}\}$ where e = 1 to n and f = 1 to 5 . Two sets from each theme were selected to form the image library. The image library for each user contained 10 sets. These sets were selected randomly in order to avoid multiple serial sequences from same theme while a user performs a training task. This helped to avoid repeated sequence similarities and unique passwords per user. User’s task was to arrange the five events within a set as apt order based on user's thought construct and perception. This order, $O(S_{jk}) = \{x_{ef}\}$was saved and was different for various user in our tests.

Table 1. TISL sample themes and some events within each theme

Theme	Example events
Going for a trip	Planning, packing the luggage, getting into the bus, enjoying the trip, bbq camp-fire
Having Dinner	A boy playing with friends, return home, finish homework, have dinner, go to sleep
Preparing food	Planning the food item, getting the required ingredients, cleaning the ingredients, cook food, serve food
Caring pets	Giving water, clean the shed, giving food , playing with the pet, going for a walk
Playing with friends	Forming teams, game planning, getting the required things to play, playing, return home

Training. User learns 10 secret keys by performing the TISL task repeatedly in a trusted environment. The following procedure was used to train the user:

1. $\forall$ U_l where U denotes the user and l = 1 to n; Choose five different themes from the set T.
2. Randomly select two sets from the selected themes T_i and form the image library.
3. Display an empty grid on the left side of the screen to arrange the images.
4. Choose any set S_{jk} from the library and arrange the images x_{ef} with their own choice within the set in the grid provided on left side of the screen.
5. The arrangement of these events could be performed using any permutations. For ex. one of the possible orders of these events could be $O(S_{jk}) = \{ x_{e3}, x_{e5,} x_{e1}, x_{e4}, x_{e2}\}$. The participant should match with this order while performing authentication at a later time.
6. Repeat step 4 for the remaining sets in the library then submit the training. Record the sequence and store as trained order.

During training, a total of 10x5=50 images were presented to the user which took 20-25 minutes to arrange. The system recorded the final order of the images.

Authentication. For authentication, the trained user was presented with the TISL task where the image library contains sets from trained as well as untrained themes for comparison. Untrained sets were chosen from the set $M = \{M_1, M_2, M_3 \ldots M_n\}$. The untrained sets comprised of the themes similar as those selected for training. This reduces possibility of guess-based predictions for a hacker although a trained user would identify the sets because of having seen the images earlier during training. The user validates identity by also exhibiting better performance on the trained sets than untrained sets. The procedure used for authentication was as follows:

1. ∀ U_l where U denotes the user and l = 1 to n; Choose two sets from $\{S_{jk}\}$ where j = 1 to n and k = 1 to m for the trained themes $T_{i.}$
2. Randomly choose three untrained sets from the set M and form the image library by combining the sets selected in step1.
3. Choose five random numbers and randomize the sets in the image library and present it to the user.
4. User is required to identify the two trained sets and perform the TISL task for the two identified sets.
5. The TISL task is performed by arranging the images from the selected sets in the order $O(S_{op})$.
6. If the user identifies the two trained sets correctly and also if $O(S_{op})$ = = $O(S_{jk})$, then the system declares that the authentication succeeded otherwise it shows authentication failure.

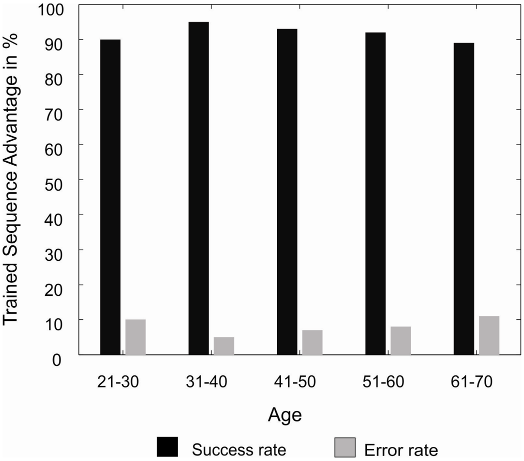


Fig. 3. Authentication success rates among varied age-groups. Percentage of successful authentication was higher than that of failure percentage. X-axis represents age of the participant's and y-axis represents the averaged percentage of authentication success.

Age-Based User Analysis. An assessment test was conducted immediately after authentication task to evaluate the role of implicit learning based success among users and to test that authentication's dependence on user age. The technique was performed by a subject group of 25 participants of age between 21 and 70 (see Fig. 3). The training procedure described in the previous section was used and included a total of 50 trials that took 20-25 minutes to complete. Participants completed the TISL authentication test immediately after training phase while estimating the amount of learning-based recall in each participant. In this immediate test, most of the participants successfully identified two trained sets and performed TISL task. Our tests suggest training and authentication was not dependent on age group of users since that percentage of successful authentications was higher than that of percentage of failed cases.

4 Conclusion and Future Work

Implicit learning and user behavior were crucial to train and authenticate in this image theme based technique. Although extensive tests need to be done, we have shown that success rate for training and authentication remained similar for age ranges 21-70. Since the tool uses a set of cartoon images as different themes to generate the secret key, it may take a significant amount of time for training as well as authentication task. The objective of such schemes was to deter common rubber hose attacks that relies on explicit authentication and to serve as a secondary layer of protection in secure systems where human user authentication remains a priority. This scheme requires the physical presence of the user so remote authentication is not possible. Adversary may guess the sequence order since the sequence length used for authentication is of short strips (images per sequence =5). This may be prevented by increasing the sequence length and by selecting the themes that are more related to the user's social cyber life. This scheme may be used by participants of any age group as it was implemented based on human implicit learning of events and themes in order to generate the secret key. The problem of forgetting the password may be overcome by performing the training task when required.

This implemented technique used a special 'task' to learn the sequence and hence was titled, Theme Interception Sequence Learning (TISL). The tool needs to be improved via other cognitive tests such as recall assessment to study the dependency of implicit learning on age of the participants, the rate at which the learned secrets are forgotten, the frequency required to refresh the training session etc. The training task will be modeled by adding different levels such as high, intermediate and sparse to study the effectiveness of sequence length in implicit learning.

Acknowledgments. This project derives direction and ideas from the Chancellor of Amrita University, Sri Mata Amritanandamayi Devi. Authors would like to acknowledge all participants who have contributed to this use-case study.

References

1. Anderson, R.: Usability and Psychology. Security Engineering, 17–62 (2008)
2. Bojinov, H., Sanchez, D., Reber, P., Boneh, D., Lincoln, P.: Neuroscience Meets Cryptography: Designing Crypto Primitives Secure Against Rubber Hose Attacks. USENIX Security (2012)
3. Kale, A., Rajagopalan, A.N., Cuntoor, N., Krueger, V., Chellappa, R.: Identification of humans using gait. IEEE Transactions on Image Processing 13, 1163–1173 (2002)
4. Bhattacharyya, D., Ranjan, R., Alisherov, F.A., Choi, M.: Biometric Authentication: A Review. International Journal of u- and e- Service, Science and Technology 2(3) (September 2009)
5. Monrose, F., Reiter, M., Wetzel, S.: Password hardening based on keystroke dynamics. Int. J. of Inf. Sec. 1(2), 69–83 (2002)

6. Sonkar, S.K., Paikrao, R.L., Kumar, A.: Graphical Password Authentication Scheme Based On Color Image Gallery. International Journal of Engineering and Innovative Technology (IJEIT) 2(4) (October 2012)
7. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., Memon, N.: Authentication Using Graphical Passwords: Basic Results. In: HumanCompute Interaction International, Las Vegas, NV (2005)
8. Almuairfi, S., Veeraraghavan, P., Chilamkurti, N.: A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. Mathematical and Computer Modelling 58, 8–116 (2013)
9. Dunphy, P., Yan, J.: Do Background Images Improve Draw a Secret" Graphical Passwords? In: Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 36–47 (2007)
10. Canetti, R., Gennaro, R.: Incoercible multiparty computation. In: Proceedings of the 37th Annual Symposium on Foundations of Computer Science, pp. 504–513 (1996)
11. Canetti, R., Dwork, C., Naor, M., Ostrovsky, R.: Deniable encryption. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 90–104. Springer, Heidelberg (1997)
12. Krever, M., Elwazer, S.: Gruesome Syria photos may prove torture by Assad regime. CNN.com. Cable News Network (January 22, 2014)
13. Destrebecqz, A., Cleeremans, A.: Can sequence learning be implicit? new evidence with the process dissociation procedure. Psychonomic Bulletin & Review 8, 343–350 (2001)
14. Cleeremans, A., Jiménez, L.: Implicit learning and consciousness: A graded, dynamic perspective. Implicit learning and consciousness, 1–40 (2002)
15. Sanchez, D., Gobel, E., Reber, P.: Performing the unexplainable: Implicit task performance reveals individually reliable sequence learning without explicit knowledge. Psychonomic Bulletin & Review 17, 790–796 (2010)
16. McVicker, C.: Comic Strips as a Text Structure for Learning to Read. International Reading Association The Reading Teacher 61(1), 85–88 (2007)
17. Megawati, F., Anugerahwati, M.: Comic strips:A Study on the Teaching of Writing Narrative Texts to Idonesian EFL Students. TEFLIN Journal: A Publication on the Teaching and Learning of English 23(2) (2012)
18. Pierson, M.R., Glaeser, B.C.: Using Comic Strip Conversations to Increase Social Satisfaction and Decrease Loneliness in Students with Autism Spectrum Disorder. Education and Training in Developmental Disabilities 42(4), 460–466 (2007)
19. Denning, T., Bowers, K., van Dijk, M., Juels, A.: Exploring implicit memory for painless password recovery. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2615–2618. ACM (2011)
20. Weinshall, D., Kirkpatrick, S.: Passwords you'll never forget, but can't recall. CHI Extended Abstracts, 1399–1402 (2004)
21. Houts, P., Doak, C., Doak, L., Loscalzo, M.: The role of pictures in improving health communication: a review of research on attention, comprehension, recall, and adherence. Patient education and counseling, 61(2), 173 -190 (2006)
22. Bolton-Gary, C.: Connecting through Comics: Expanding Opportunities for Teaching and Learning. Online Submission (2012)
23. Ginman, M., von Ungern-Sternberg, S.: Cartoons as information. Journal of Information Science, 29(1) 69-77 (2003)
24. Sun, R., Giles, L.: Sequence Learning: From Recognition and Prediction to Sequential Decision Making. Intelligent Systems, IEEE 16(4), 67–70 (2001)