University of Kent

Kent Academic Repository

Yuan, Haiyue, Li, Shujun, Rusconi, Patrice and Aljaffan, Nouf (2017) *When Eye-Tracking Meets Cognitive Modeling: Applications to Cyber Security Systems.* In: Tryfonas, Theo, ed. Human Aspects of Information Security, Privacy and Trust 5th International Conference. Lecture Notes in Computer Science . Springer, Cham, Switzerland, pp. 251-264. ISBN 978-3-319-58459-1.

Downloaded from

https://kar.kent.ac.uk/69559/ The University of Kent's Academic Repository KAR

The version of record is available from

https://doi.org/10.1007/978-3-319-58460-7_17

This document version

Author's Accepted Manuscript

DOI for this version

Licence for this version

UNSPECIFIED

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in *Title of Journal* , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).

When Eye-tracking Meets Cognitive Modeling: Applications to Cyber Security Systems

Haiyue Yuan[1], Shujun Li[1], Patrice Rusconi[2] and Nouf Aljaffan[1]

[1] Department of Computer Science and Surrey Centre for Cyber Security (SCCS), University of Surrey, Guildford, United Kingdom
[2] School of Psychology, University of Surrey, Guildford, United Kingdom

Abstract. Human cognitive modeling techniques and related software tools have been widely used by researchers and practitioners to evaluate the effectiveness of user interface (UI) designs and related human performance. However, they are rarely used in the cyber security field despite the fact that human factors have been recognized as a key element for cyber security systems. For a cyber security system involving a relatively complicated UI, it could be difficult to build a cognitive model that accurately captures the different cognitive tasks involved in all user interactions. Using a moderately complicated user authentication system as an example system and CogTool as a typical cognitive modeling tool, this paper aims to provide insights into the use of eye-tracking data for facilitating human cognitive modeling of cognitive tasks more effectively and accurately. We used visual scan paths extracted from an eye-tracking user study to facilitate the design of cognitive modeling tasks. This allowed us to reproduce some insecure human behavioral patterns observed in some previous lab-based user studies on the same system, and more importantly, we also found some unexpected new results about human behavior. The comparison between human cognitive models with and without eye-tracking data suggests that eye-tracking data can provide useful information to facilitate the process of human cognitive modeling as well as to achieve a better understanding of security-related human behaviors. In addition, our results demonstrated that cyber security research can benefit from a combination of eye-tracking and cognitive modeling to study human behavior related security problems.

Keywords: Eye-tracking, cognitive modeling, CogTool, user interface, design, cyber security, human behavior, user authentication

1 Introduction

Psychologists and computer scientists have developed computational cognitive architectures and models (e.g. ACT-R [1,4], Soar [21,29] and CLARION [30]) to simulate human behaviors using computers to study human cognitive processes such as perception, memory, and attention. Due to their ability to help designers and researchers evaluate human performance and refine user interface (UI) designs more easily without prototyping and user testing [13], cognitive models

such as Keystroke-Level Model (KLM) [8] and other more complicated models following the GOMS (Goals, Operators, Methods, and Selection) rules [17] have been widely used in the Human-Computer Interaction (HCI) field. However, such models are relatively less known to and used by cyber security researchers and practitioners, except for some limited work on using human cognitive modeling tools to estimate usability of user authentication systems [19, 20, 28].

Although human cognitive modeling is less used in the cyber security field, the wider human factors have been actively studied by cyber security researchers. It is well known that many security problems are caused by insecure human behaviors such as weak passwords and poorly-designed/-implemented security policies. In addition, the UI design of a system may lead to insecure human behaviors and thereby compromise the system's security. For instance, as reported in [24,33], for many challenge-response based password systems against observer attacks, human users respond to different challenges differently in terms of the time spent. This allows an attacker to derive the password based on some observable timing differences after seeing a sufficient number of authentication sessions conducted by a target user.

The "standard" approach to identifying insecure human behaviors is to conduct user studies with real human participants. However, this approach is not only time consuming, but also has other issues such as limited/bias samples, ethical concerns, and privacy issues, which could potentially delay the detection of human behavior related security problems and leave systems vulnerable to potential attacks for a longer time. Therefore, it is important and beneficial for both security system designers and end users to discover human behavior related security problems as early as possible ideally at the design stage, which can be considered as a special case of the widely-recognized "security by design" principle [11].

Differently from the above standard approach, cognitive modeling could provide a quicker and sometimes also better solution to study human behavior related security problems. Considering the broad scope of cyber security systems as well as potential security problems related to human behavior, this paper does not aim to provide a comprehensive account of how to model human cognitive tasks for any cyber security systems, instead, we use one advanced user authentication system as a representative example to show how human cognitive modeling can help UI designers and security analysts. Furthermore, some researchers have reported that eye-trackers can provide useful information for cognitive modeling tasks, but the combined use of eye-tracking and cognitive modeling technologies for security-sensitive systems is very rare. We hope this paper will fill this gap as well.

In this paper, we report our work on combining eye-tracking data and CogTool [16], a widely-used cognitive modeling tool, to model human cognitive tasks involved in a relatively complex user authentication system called Undercover [27]. The eye-tracking data proved useful for guiding the modeling process, and helped us to reproduce some *non-uniform* and *insecure* human behavior observed in a previous lab-based user study conducted by Perković

et al. in 2011 [24]. The simulation results of the eye-tracking assisted cognitive model led to more insights into the observed non-uniform human behavior and how the UI design may be further refined to improve its security, going beyond what Perković et al. predicted in [24]. Our work suggests that cyber security researchers and practitioners could benefit from a *combined* use of cognitive modeling techniques and eye-tracking data.

The rest of this paper is organized as follows. The next section presents some related work. Then, we describe the authentication system (Undercover) we focused on as a showcase, how we used eye-tracking data to refine the cognitive model of Undercover, and what new insights we learned from the process. The final section discusses the benefits of using eye-tracking data in cognitive modeling of cyber security systems.

2 Related Work

Goals, Operators, Methods, and Selection rules (GOMS) are among the well-established cognitive modeling concepts for analyzing UIs. A number of variants of GOMS models such as KLM, CMN-GOMS [9], and CPM-GOMS [17] have been proposed. Most of these cognitive models can estimate human performance in terms of time needed by an average skilled user to complete a specific task.

Differently from GOMS models, low-level cognitive architectures and models such as ACT-R [1, 4] and Soar [21, 29] can be used to model broader human cognitive processes, e.g., modeling users' performance on multi-modal UIs such as car navigation systems, which represents a challenge for traditional GOMS analysis [6, 26]. ACT-R specifies the time parameters of processes such as the shifting of a user's visual attention, so it can be used to model visual search tasks. For example, Fleetwood and Byrne [12] compared two models representing different strategies of searching for a target icon among distractors.

Cognitive models and related software tools do not normally have built-in support on various UI elements. To fill the gap, a number of software tools (e.g. CogTool [16], SANLab-CM [23], Cogulator [31]) have been developed to make cognitive modeling tasks easier. Such tools often implement a GOMS model from a user-defined UI layout design and then convert that to a model based on one of the lower-level cognitive architectures such as ACT-R. Although these tools are very powerful to support cognitive modeling tasks, it could be difficult for a designer to decide how to model a system involving complicated cognitive tasks, e.g., if they depend on individual characteristics and/or the context. One of the widely-used human cognitive modeling tools in the HCI community is CogTool [16], which is based on KLM and ACT-R and has proven to be a useful tool for predicting and simulating human performance of skilled users to complete computer tasks [18].

Despite the fact that human cognitive modeling has been extensively studied and used in the HCI field, to the best of our knowledge only a few studies in the cyber security community used cognitive modeling to evaluate/design security systems. Kim et al. [19] used CogTool to evaluate the usability of a shoulder surf-

ing resistant mobile user authentication system, and Sasse et al. [28] combined CogTool with a user study to estimate the usability of a user authentication system. Kwon et al. [20] used CPM-GOMS to investigate human shoulder surfers attacking PIN entry methods that rely on the evidence of effective human perceptual and cognitive capabilities.

Although cognitive modeling has not been extensively used in the cyber security field, some cyber security researchers have started considering human cognitive abilities in the design of cyber security systems to achieve a better balance between usability and security. Belk et al. [5] proposed two-step personalized user authentication tasks based on individual cognitive styles of processing textual and graphical information. Al Galib et al. [2] designed a new user authentication system based on a game of cognitive tasks to capture individual users' implicit cognitive signatures. More recently, Castelluccia et al. [10] developed a new authentication scheme (MooneyAuth) based on using implicit memory to reduce the cognitive load of remembering passwords. Such work also calls for more research on modeling of human cognitive abilities to study usability and the security of such systems.

Eye trackers capture human users' eye movements (fixations and saccades), scan paths, and metrics such as pupil dilation and blinks which provide information about the user's cognitive processes while performing a task. Thus, they have been widely used in studies on cognitive modeling especially on cognitive tasks related to visual objects shown on computer displays [14]. Some researchers also used eye trackers to help validate and compare cognitive models of visual search tasks [7, 12, 15, 25]. There is also research about using eye trackers to better understand human users' cognitive processes when interacting with security-sensitive systems, e.g., recently Miyamoto et al. [22] conducted a study on using eye-tracking data to link UI elements to the detection of possible phishing websites. Alsharnouby et al. [3] used eye trackers to assess the influence of browser security indicators and the awareness of phishing on a user's ability to avoid cyber attacks. While there is quite some work on the combined use of eye tracking and cognitive modeling, to the best of our knowledge, except some general recommendations such as those reported in [15] still limited work has been done on combining the two techniques for cyber security applications. This paper aims to further advance this neglected area.

3 Eye-Tracking Assisted Cognitive Modeling Experiment

In this section, we explain our work in detail. We start with a brief description of the target system Undercover. Then we report our initial cognitive models of Undercover and the simulation results when eye-tracking data were not used. These are followed by an explanation of the eye-tracking experiment we conducted to improve the initial models which were found inaccurate. The last part of the section presents our re-modeling work and the new insights emerged from the eye-tracking assisted cognitive modeling experiment.

3.1 Target System: Undercover

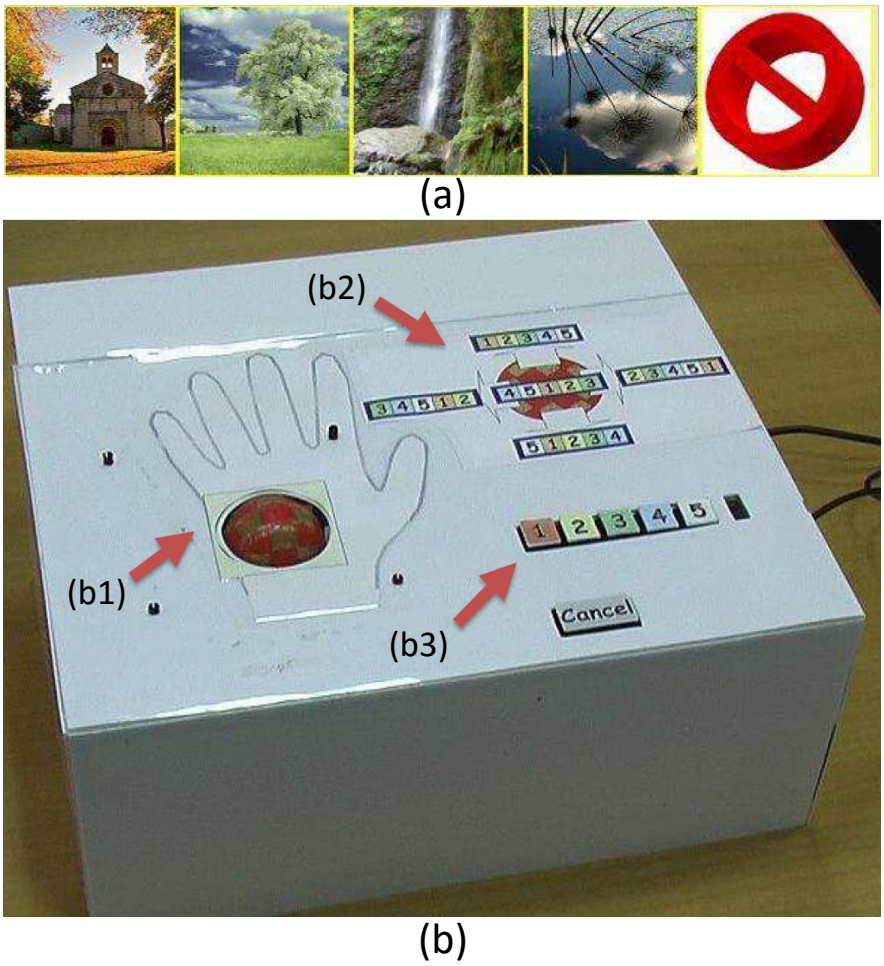

Fig. 1. The UI of Undercover [27]: (a) the public challenge panel shown on the computer display; (b) a box composed of the following UI components: (b1) a track ball for transmitting the hidden challenge, (b2) the hidden challenge button layout panel, (b3) the response button panel.

Undercover [27] is an observer-resistant password system (ORPS) developed based on the concept of partially-observable challenges. The password P a user needs to set is a set of five secret pictures called "pass-pictures", selected out of an image pool. To complete an authentication session, the user needs to correctly

respond to seven challenge screens, where each challenge screen contains a hidden challenge c_h described below and a public challenge c_p consists of four pictures and a "no pass-picture" icon as shown in Fig. 1(a). The hidden challenge c_h is transmitted via a haptic device (a track ball) covered by the user's palm, as shown in Fig. 1(b1). Five different rotation/vibration modes of the track ball correspond to five different values of c_h: "Up", "Down", "Left", "Right", "Center" (vibrating). As illustrated in Fig. 1(b2), each hidden challenge value corresponds to a specific layout of five response buttons labeled with 1-5. To respond to a challenge screen, the user should firstly obtain a hidden response r_h which is the position index of the pass-picture in the public challenge (1-4 if present and 5 if absent). Then the user looks for r_h in the correct hidden challenge button layout to get a new position index r'_h, and finally presses the button labeled with r'_h in the response button panel as shown in Fig. 1(b3). There are some more subtle security settings, for which readers are referred to [24, 27].

There are three main reasons why we chose Undercover for our work:

1. Undercover is a relatively complex security-sensitive system that involves different cognitive tasks that are not straightforward to model.
2. Perković et al. [24] conducted a lab-based user study that revealed some *non-uniform* and *insecure* behavioral patterns on how human users responded to hidden challenges (the average response time to the hidden challenge value "Up" is significantly smaller than to other values) which were believed to be caused by an improper design of the UI.
3. How human users actually interact with the Undercover UI remains largely unclear which may lead to other security problems or insights of a better UI design.

We therefore wanted to use eye-tracking data and CogTool to see if we can reproduce the non-uniform behavioral patterns observed and provide some further insights about the actual human behaviors, which will then serve as a good example showcasing the usefulness of combining eye tracking with cognitive modeling techniques.

3.2 Initial CogTool Models (without Eye-tracking Data)

To make an adequate comparison with findings reported by Perković et al. [24], we used CogTool to model their Undercover implementation (which is conceptually the same as the original Undercover system reported in [27] but with some minor changes to the UI and the use of an earphone and an audio channel to transmit the hidden challenge instead). The layout of the UI with functionality of each component (which is called the design script in CogTool), and how human interact with the UI (which is called the demonstration script in CogTool) are essential to CogTool. Undercover has a static UI layout, but the user interaction is dynamic where different hidden challenges can result in different visual scan paths, and require different buttons to be pressed.

A key problem we met in the modeling task is how to model human users' visual scan paths for the three separate parts of a challenge screen: the public

challenge picture panel, the hidden challenge button layout panel, and the response button panel. Since we did not have any clue about the actual visual scan paths, we decided to make two initial models based on two simple visual scan paths explained below and shown in Fig. 2.[3]

- **A1**: for each part of the challenge screen the user identifies the target without an obvious visual searching process, i.e., the user looks at the pass-picture in the public challenge panel, then moves to the (correct) hidden challenge button layout directly, and finally to the (correct) response button directly.
- **A2**: the same as **A1** but before the user looks at the (correct) hidden challenge button layout (s)he looks at the whole hidden challenge button layout panel first.

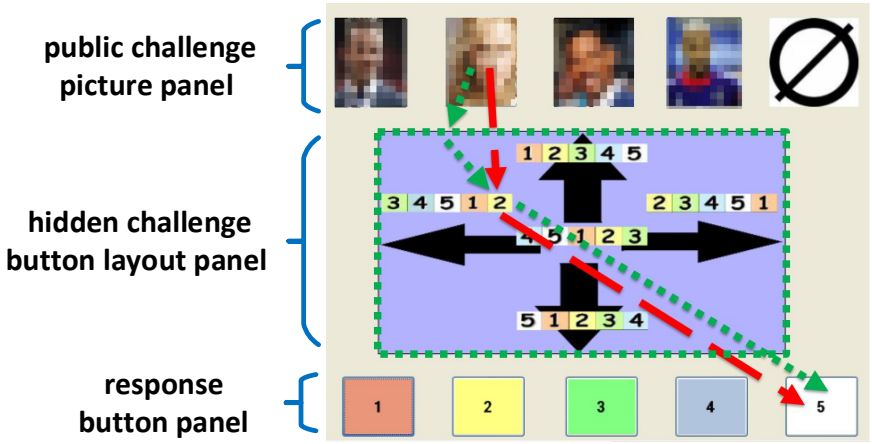

Fig. 2. An illustration of the two visual scan paths when the pass-picture is the second picture in the public challenge and the hidden challenge is "Left": the red dashed and dark green dotted lines show **A1** and **A2**, respectively.

With the two models, we generated all five possible instances according to the hidden response $r_h = 1, \cdots, 5$ and obtained the average response times as shown in Fig. 3. Comparing the results of **A1** and **A2**, we can see **A2** requires more time due to the added cognitive task, and the hidden challenge value corresponding to the fast average response time differs ("Up" for **A1** and "Center" for **A2**). While the non-uniform response time pattern of **A1** loosely matches the findings

[3] We actually built a number of models for each of the two models as CogTool supports only static cognitive tasks but Undercover involves dynamic ones related to varying challenges. We are developing an extension of CogTool to facilitate modeling of such dynamic cognitive tasks, but in this paper we will not focus on this issue.

reported in [24], the cognitive model is obviously too simplistic, e.g., a proper visual searching process is expected for finding out if a pass-picture is present and where the pass-picture is in the public challenge.

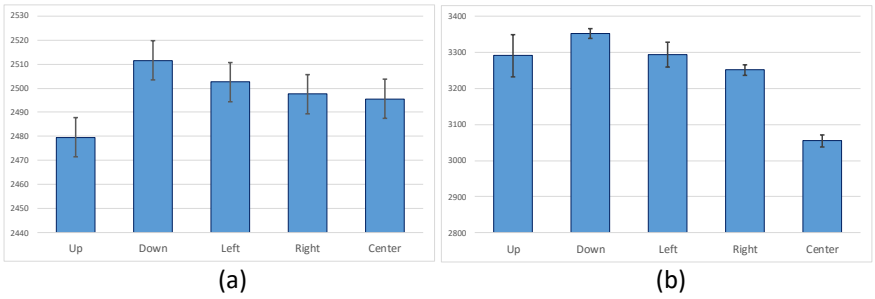

Fig. 3. Average response times for (a) A1 and (b) A2.

3.3 Eye-tracking Experiment

As shown above, the lack of knowledge on human users' actual visual scan paths prevented us from making a more informed decision on how to model Undercover. We therefore decided to conduct an eye-tracking experiment in order to gain such knowledge. We implemented a fast prototype of Undercover in MATLAB and used a Tobii EyeX eye tracker (with an upgraded license for research purposes) [32] for the experiment. Nine participants (5 female and 4 male), who did not wear glasses were recruited. Each participant was briefed about Undercover and had a training session to get familiar with the authentication process. We set the same password for all participants, and each participant was given time to memorize the pass-pictures before the actual experiment started.

During the experiment, each participant was asked to complete seven challenge screens (equivalent to one authentication session) once or twice. Among the seven challenge screens, each of the five values of the hidden challenge and the hidden response was present at least once. In total, we collected 98 sets of eye-tracking data (each set represents the process of responding to one challenge screen). We removed 12 sets of data due to inaccuracy caused by change of sitting position during the experiment and incomplete tasks. This gave us 86 valid sets of data whose eye-gaze trajectories were manually inspected to identify visual scan patterns. The results revealed four important (not all expected) visual scan patterns explained below and illustrated in Fig. 4.

1. *No obvious searching process for the correct hidden challenge button layout or the correct response button*: For these two parts of the challenge screen,

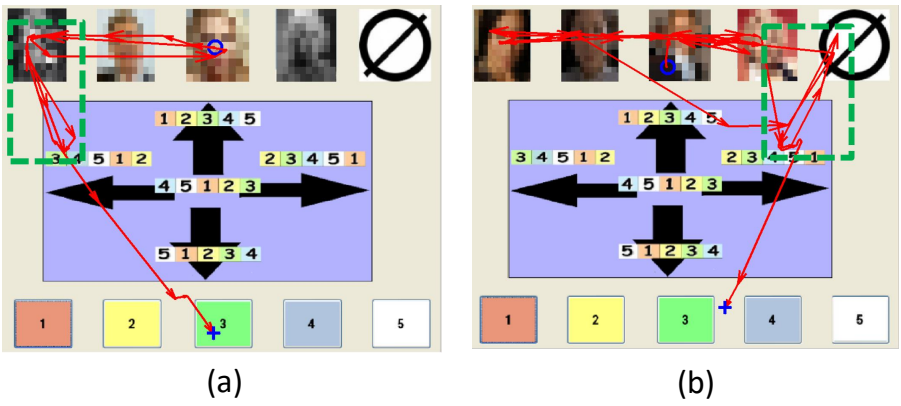

Fig. 4. An illustration of observed visual scan patterns where red lines show the eye gaze trajectories, blue circles and blue crosses indicate the starting and ending gazing positions: (a) $r_h = 1$, $c_h =$ Left; (b) $r_h = 5$, $c_h =$ Right.

participants identified the targets directly without an obvious visual searching process.

2. *Two searching patterns for the pass-picture*: For 87% cases, participants adopted a searching strategy of center-left-right as illustrated in Fig. 4(a), and for the rest 13% cases, participants searched for the pass-picture simply from left to right.
3. *Confirmation pattern for the pass-picture*: For 59% of all cases, participants showed a confirmation pattern where they went from the hidden challenge button layout panel back to the pass-picture in the public challenge panel before moving to the response button panel, which are highlighted inside the green dash-line rectangles shown in Fig. 4. This pattern is consistent with the findings reported in [25], which suggests that several saccades to the location of the memorized target are typical. We also noticed that the confirmation process rate varies depending on the value of the hidden challenge (see Fig. 5) c_h: 40.91% (Up), 92.31% (Down), 64.71% (Left), 61.9% (Right), 46.15% (Center). Interestingly, the non-uniform confirmation rates partly match the non-uniform response time reported in [24], suggesting they may be one source of the non-uniformity.
4. *Double scanning pattern for absent pass-picture*: When no pass-picture is present in the public challenge, in 66% cases participants double scanned the public challenge picture panel to make sure there was indeed no pass-picture, which is illustrated in Fig. 4(b).

3.4 Re-modeling Undercover (with Eye-tracking Data)

The four visual scan path patterns learned from our eye-tracking experiment provided additional evidence for us to remodel Undercover in a more compli-

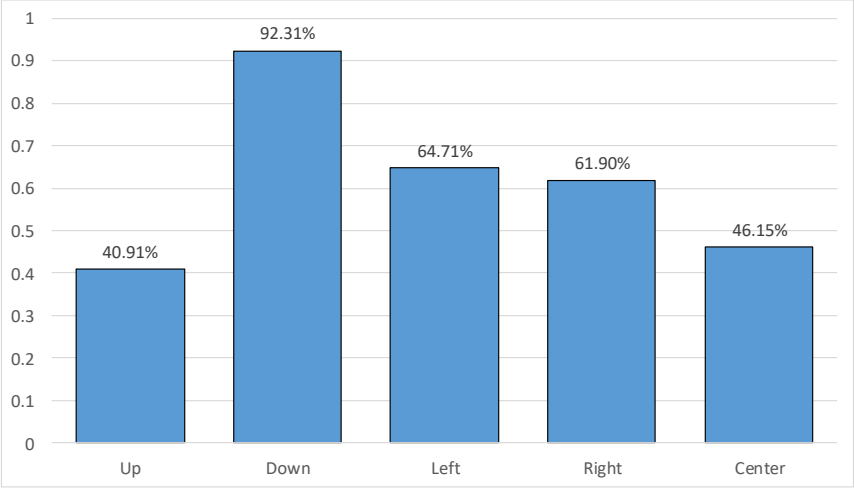

Fig. 5. Confirmation rate for hidden challenges

cated (and hopefully more accurate) manner. We firstly constructed four new models named as CLR-C, CLR-NC, LR-C and LR-NC, where CLR represents the (C)enter-(L)eft-(R)ight searching strategy for the pass-picture; LR represents the simpler (L)eft-(R)ight searching strategy for the pass-picture; C after the hyphen stands for the (C)onfirmation process and NC after the hyphen means there is (N)o (C)onfirmation process. As in the case of the two initial models, for each of the above models we also created five instances for the five values of r_h for each model to get the average response time. When $r_h = 5$ (i.e., there is no pass-picture in the public challenge), we also created two further sub-models with and without the double scanning pattern, whose simulation results (response times) are then added up using the weights 0.66 and 0.34 to get the predicted average response time for the case of $r_h = 5$.

The results of the predicted average response time for all the four models are shown in Table 1, from which we can see the hidden challenge value corresponding to the smallest average response time is "Up" (consistently across all models), matching the findings reported in [24].

Based on the four models, we constructed a mixed probabilistic model where CLR-LR and N-NC patterns are considered based on different probabilities: 87% CLR and 13% LR for all challenge values; 40.9% C and 59.1% NC for "Up", 92.3% C and 7.7% NC for "Down", 64.7% C and 35.3% NC for "Left", 61.9% C and 38.1% NC for "Right", 46.2% C and 53.8% NC for "Center". The predicted average response time for each hidden challenge value of the mixed probabilistic model is shown in Fig. 6(a), where the average response time for the hidden

Model	Hidden Challenge				
	Up	**Down**	**Left**	**Right**	**Center**
CLR-C	4148.2	4331.6	4266.2	4229.2	4243.8
CLR-NC	3385.0	3453.2	3445.4	3401.2	3424.6
LR-C	4125.3	4297.5	4232.8	4203.5	4220.3
LR-NC	3362.1	3419.1	3411.9	3375.5	3401.1

Table 1. Average response time (in milliseconds) to each hidden challenge value for different models.

challenge value "Up" is significantly smaller than for other four values, which accords with the finding in [24].

We also looked at the average response times for different values of r_h and the results are shown in Fig. 6(b). The results confirmed another observation in [24], which states that most users tended to respond more slowly when $r_h = 5$ (i.e., there is no pass-picture in the public challenge), and this could be explained by the double scanning pattern we described above. Furthermore, as identified in our eye-tracking experiment, in most cases participants adopted the CLR visual searching strategy for the pass-picture, and thus it is not surprising to observe that $r_h = 3$ (when the pass-picture is right in the middle of the public challenge panel) corresponds to the smallest average response time.

Comparing with the results reported in [24], there are still some noticeable differences. These differences could be caused by some subtle differences between our experimental setup and the one used in [24]. For instance, in the user study reported in [24], participants were allowed to use either mouse or keyboard to click the response button. However, for our models only mouse users are considered because keyboard users are more difficult to model due to various keyboard types and different individual human behaviors of using the keyboard. The smaller and different population of participants used in our experiment may be another source.

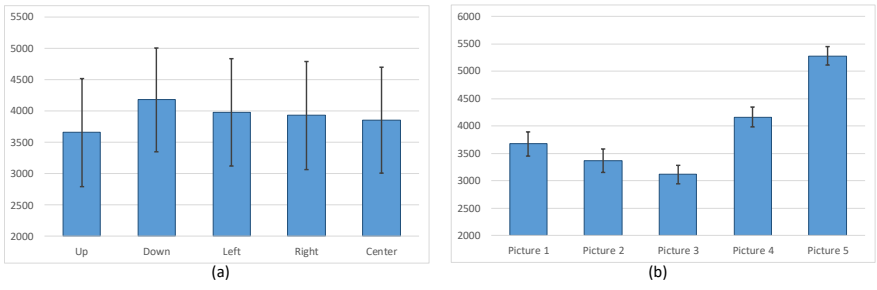

Fig. 6. Average response times (in milliseconds) for different values of (a) the hidden challenge c_h and (b) the hidden response r_h.

Our model could be further refined by considering the additional mental effort of converting r_h to r'_h. This will differ for different values of c_h because this conversion is effectively not needed for "Up" (the hidden challenge response button layout is "12345", which means $r'_h = r_h$). We thus can reasonably hypothesize that there will be less mental efforts for the "Up" case so that the response time is faster, which is also the main hypothesis Perković made in [24]. However, as demonstrated in the above results, the conversion process from r_h to r'_h is not the sole (may not be even the main) factor causing the observed non-uniform human behavior on average response time, which is a new insight obtained from our eye-tracking experiment. In our future work, we plan to investigate the conversion process from r_h to r'_h and see how that can be considered in the cognitive modeling task.

4 Conclusion

Taking Undercover [27] as a relatively complex user authentication system and CogTool as a typical cognitive modeling tool, we demonstrated that the use of an eye tracker can help identify different visual scan patterns which can effectively guide computational modeling of human cognitive tasks. The eye-tracking assisted cognitive modeling approach allowed us to not only reproduce some previously-observed behavioral patterns of human users reported in [24], but also to reveal more unexpected observations of related human behaviors. While our work mainly focuses on a specific system, the insights we learned from the eye-tracking assisted cognitive modeling suggest eye-tracking should be used more widely in cognitive modeling of any cyber security systems with some visual elements in their UIs. We are developing a software tool as an extension version of CogTool, which will cover (semi-)automated fast prototyping and (semi-)automated application of eye-tracking data to adapt cognitive models.

Acknowledgments. This work was supported by the UK part of a joint Singapore-UK research project "COMMANDO-HUMANS: COMputational Modelling and Automatic Non-intrusive Detection Of HUMan behAviour based iNSecurity", funded by the Engineering and Physical Sciences Research Council (EPSRC) under grant number EP/N020111/1.

References

1. ACT-R Research Group: ACT-R. http://act-r.psy.cmu.edu/ (2016), accessed: Aug 25, 2016
2. Al Galib, A., Safavi-Naini, R.: User authentication using human cognitive abilities. In: Financial Cryptography and Data Security: 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 8975, pp. 254–271. Springer (2015)
3. Alsharnouby, M., Alaca, F., Chiasson, S.: Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies 82, 69–82 (2015)

4. Anderson, J.R.: How Can the Human Mind Occur in the Physical Universe? Oxford University Press (2007)
5. Belk, M., Germanakos, P., Fidas, C., Samaras, G.: A personalization method based on human factors for improving usability of user authentication tasks. In: User Modeling, Adaptation, and Personalization: 22nd International Conference, UMAP 2014, Aalborg, Denmark, July 7-11, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8538, pp. 13–24. Springer (2014)
6. Byrne, M.D.: ACT-R/PM and menu selection: Applying a cognitive architecture to HCI. International Journal of Human-Computer Studies 55(1), 41–84 (2001)
7. Byrne, M.D., Anderson, J.R., Douglass, S., Matessa, M.: Eye tracking the visual search of click-down menus. In: Proceedings of 1999 SIGCHI Conference on Human Factors in Computing Systems (CHI '99). pp. 402–409. ACM (1999)
8. Card, S.K., Moran, T.P., Newell, A.: The keystroke-level model for user performance time with interactive systems. Communications of the ACM 23(7), 396–410 (1980)
9. Card, S.K., Newell, A., Moran, T.P.: The Psychology of Human-Computer Interaction. L. Erlbaum Associates Inc., Hillsdale, NJ, USA (1983)
10. Castelluccia, C., Duermuth, M., Golla, M., Deniz, F.: Towards implicit visual memory-based authentication. In: Proceedings of 2017 Network and Distributed System Security Symposium (NDSS 2017). Internet Society (2017)
11. Cavoukian, A., Dixon, M.: Privacy and security by design: An enterprise architecture approach. Online white paper https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf (2013)
12. Fleetwood, M.D., Byrne, M.D.: Modeling the visual search of displays: A revised ACT-R model of icon search based on eye-tracking data. Human-Computer Interaction 21(2), 153–197 (2008)
13. Gray, W.D., John, B.E., Atwood, M.E.: Project ernestine: Validating a GOMS analysis for predicting and explaining real-world task performance. Human Computer Interaction 8(3), 237–309 (1993)
14. Hornof, A.J.: Cognitive strategies for the visual search of hierarchical computer displays. Human-Computer Interaction 10(3), 183–223 (2004)
15. Hornof, A.J., Halverson, T.: Cognitive strategies and eye movements for searching hierarchical computer displays. In: Proceedings of 2003 SIGCHI Conference on Human Factors in Computing Systems (CHI 2003). pp. 249–256. ACM (2003)
16. John, B.E.: CogTool. https://cogtool.com/ (2016), accessed: Aug 25, 2016
17. John, B.E., Kieras, D.E.: The GOMS family of user interface analysis techniques: Comparison and contrast. ACM Transactions on Computer-Human Interaction 3(4), 320351 (1996)
18. John, B.E., Prevas, K., Salvucci, D.D., Koedinger, K.: Predictive human performance modeling made easy. In: Proceedings of 2004 SIGCHI Conference on Human Factors in Computing Systems (CHI 2004). pp. 455–462. ACM (2004)
19. Kim, S., Yi, H., Yi, J.H.: FakePIN: Dummy key based mobile user authentication scheme. In: Ubiquitous Information Technologies and Applications: CUTE 2013. Lecture Notes in Electrical Engineering, vol. 280, pp. 157–164. Springer (2014)
20. Kwon, T., Shin, S., Na, S.: Covert attentional shoulder surfing: Human adversaries are more powerful than expected. IEEE Transactions on Systems, Man, and Cybernetics: Systems 44(6), 716–727 (2014)
21. Laird, J.E.: The Soar Cognitive Architecture. MIT Press (2012)
22. Miyamoto, D., Blanc, G., Kadobayashi, Y.: Eye can tell: On the correlation between eye movement and phishing identification. In: Neural Information Processing: 22nd

International Conference, ICONIP 2015, Istanbul, Turkey, November 9-12, 2015, Proceedings Part III. Lecture Notes in Computer Science, vol. 9194, pp. 223–232. Springer (2015)
23. Patton, E.W.: The stochastic activity network laboratory for cognitive modeling (SANLab-CM). https://github.com/CogWorks/SANLab-CM/ (2012), accessed: Aug 25, 2016
24. Perković, T., Li, S., Mumtaz, A., Khayam, S.A., Javed, Y., Čagalj, M.: Breaking Undercover: Exploiting design flaws and nonuniform human behavior. In: Proceedings of 2011 7th Symposium on Usable Privacy and Security (SOUPS 2011). ACM (2011)
25. Rao, R.P.N., Zelinsky, G.J., Hayhoe, M.M., Ballard, D.H.: Eye movements in iconic visual search. Vision Research 42(11), 1447–1463 (2002)
26. Salvucci, D.D.: Predicting the effects of in-car interfaces on driver behavior using a cognitive architecture. In: Proceedings of 2001 SIGCHI Conference on Human Factors in Computing Systems (CHI 2001). pp. 120–127. ACM (2001)
27. Sasamoto, H., Christin, N., Hayashi, E.: Undercover: Authentication usable in front of prying eyes. In: Proceedings of 2008 SIGCHI Conference on Human Factors in Computing Systems (CHI 2008). pp. 183–192. ACM (2008)
28. Sasse, M.A., Steves, M., Krol, K., Chisnell, D.: The great authentication fatigue – and how to overcome it. In: Cross-Cultural Design: 6th International Conference, CCD 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8528, pp. 228–239. Springer (2014)
29. Soar Research Groups: Soar cognitive architecture. http://soar.eecs.umich.edu/ (2016), accessed: Sept 18, 2016
30. Sun, R., Slusarz, P., Terry, C.: The interaction of the explicit and the implicit in skill learning: A dual-process approach. Psychological Review 112(1), 159–192 (2005)
31. The MITRE Corporation: A cognitive modeling calculator. http://cogulator.io/ (2014), accessed: Aug 25, 2016
32. Tobii AB: Tobii EyeX. http://www.tobii.com/xperience/products/ (2016), accessed: Aug 25, 2016
33. Čagalj, M., Perković, T., Bugarić, M.: Timing attacks on cognitive authentication schemes. IEEE Transactions on Information Forensics and Security 10(3), 584–596 (2015)