Cryptanalysis of the Convex Hull Click Human Identification Protocol*

Hassan Jameel Asghar[1], Shujun Li[2], Josef Pieprzyk[1], and Huaxiong Wang[1,3]

[1] Center for Advanced Computing, Algorithms and Cryptography, Department of Computing, Faculty of Science, Macquarie University, Sydney, NSW 2109, Australia
{hasghar, josef, hwang}@science.mq.edu.au

[2] Department of Computer and Information Science, University of Konstanz, Mailbox 697, Universitätsstraße 10, Konstanz 78457, Germany
Shujun.Li@uni-konstanz.de

[3] Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, 50 Nanyang Avenue, 639798, Singapore
hxwang@ntu.edu.sg

Abstract. Recently a convex hull based human identification protocol was proposed by Sobrado and Birget, whose steps can be performed by humans without additional aid. The main part of the protocol involves the user mentally forming a convex hull of secret icons in a set of graphical icons and then clicking randomly within this convex hull. In this paper we show two efficient probabilistic attacks on this protocol which reveal the user's secret after the observation of only a handful of authentication sessions. We show that while the first attack can be mitigated through appropriately chosen values of system parameters, the second attack succeeds with a non-negligible probability even with large system parameter values which cross the threshold of usability.

Keywords. Human Identification Protocols, Observer Attack

1 Introduction

In a human identification protocol, a human user (the prover) attempts to authenticate his/her identity to a remote computer server (the verifier). The user has an insecure computer terminal under the control of an adversary. The adversary can view the computations done at the user's terminal as well as the inputs from the user. In addition, the adversary has passive or active access to the communication channel between the user and the server. Designing a secure human identification protocol under this setting is hard, since the user can no longer rely on the computational abilities of the terminal and has to mentally perform any computations. The problem, then, is to find a secure method of identification that is not computationally intensive for humans.

* This paper has been published in *Information Security: 13th International Conference, ISC 2010, Boca Raton, FL, USA, October 25-28, 2010, Revised Selected Papers*, *Lecture Notes in Computer Science*, vol. 6531, pp. 24-30, 2011, Springer. The full edition is available at http://eprint.iacr.org/2010/478.

In [1], Sobrado and Birget proposed a graphical human identification protocol that utilizes the properties of a convex hull. A variant of this protocol has later appeared in [2]. In [3] Wiedenbeck et al. gave a detailed description of the protocol from [1], with a usability analysis employing human participants. Since the work reported in [3] is more comprehensive, we will adhere to the protocol described therein for our security analysis in this paper. Following the term used in [3], we call the protocol Convex Hull Click or CHC in short. In this paper, we describe two probabilistic attacks on the protocol and show its weaknesses against a passive eavesdropping adversary.

Related Work. The identification protocol of Matsumoto and Imai [4] was the first attempt at designing a human identification protocol secure under the aforementioned setting. The protocol, however, was shown to be insecure by Wang et al. [5] who proposed some fixes but which render the resulting protocol too complex to execute for most humans. Matsumoto also proposed some other protocols in [6]. However, the security of these protocols can be compromised after a few authentication sessions [7, 8]. Some other proposals for human identification protocols that have been shown to be insecure were proposed by the authors in [9, 10, 11]. These protocols were cryptanalysed in [12, 13, 14].

Hopper and Blum proposed the well-known HB protocol, which is based on the problem of learning parity in the presence of noise [8]. The protocol has some weaknesses as it requires the user to send a wrong answer with a probability between 0 and 0.5, which is arguably hard for most humans. Li and Teng's protocols [15] seem impractical as they require a large size of secret (3 secrets of 20 to 40 bits). Li and Shum's protocols [7] have been designed with some principles in mind, such as using hidden responses to challenges. This loosely means that the responses sent to the server are non-linearly dependent on the actual (hidden) responses. However, the security of these protocols has not yet been thoroughly analysed. Jameel et al. [16, 17] have attempted to use the gap between human and artificial intelligence to propose two image-based protocols. The security, however, is based on unproven assumptions. More recently, Asghar, Pieprzyk and Wang have proposed a human identification protocol in [18]. The usability of the protocol is similar to Hopper and Blum's protocols. But an authentication time of about 2 to 3 minutes is still not practical.

2 The CHC Human Identification Protocol

Denote the convex hull of a set of points Π by $\mathsf{ch}(\Pi)$. If a point P lies in the interior or on the boundary of a polygon, we say that the point P is contained in the polygon, or the polygon contains the point P. We denote the membership relation "contains" by $\in$. The convex hull of 3 points is a triangle and the two terms will be used interchangeably.

2.1 The Protocol

In the CHC human identification protocol, the human prover $\mathcal{H}$ and the remote (computer) verifier $\mathcal{C}$ choose k graphical icons from a set of n as a shared secret in the setup phase. When $\mathcal{H}$ wants to prove its identity to $\mathcal{C}$, the following protocol is carried out.

CHC Protocol.

1: $\mathcal{C}$ randomly samples a set of m graphical icons out of n, where m is a random positive integer between n and some lower bound $m_{\min}$. $\mathcal{C}$ ensures that at least 3 of the k secret icons are included in these m graphical icons. These icons are distributed randomly on the screen of the user's computer terminal within a rectangular frame and aligned in a grid.

2: $\mathcal{H}$ mentally forms the convex hull of any 3 secret icons displayed on the screen and randomly clicks a point contained in this convex hull. Notice that this is equivalent to clicking on the convex hull of all the secret icons present in the screen.

3: $\mathcal{C}$ repeats the process a certain number of times and accepts or rejects $\mathcal{H}$ accordingly.

□

For the ease of analysis, we assume m to be fixed. In fact, we will later see that once n and k are fixed, we do not have much freedom in choosing m, if a certain attack is to be avoided. Furthermore, we replace graphical icons by non-negative integer lattice points on a real plane, enclosed within a rectangular area. The lattice points are identified by a unique integer label from the set $\{1, 2, \ldots, n\}$ as shown in Figure 1. Therefore, throughout this text, we will use the terms, icons and labels, interchangeably. We shall call the area enclosed in the rectangle as the rectangular lattice area or simply the rectangle.

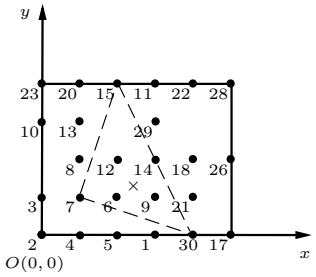

Fig. 1. One round of the convex hull protocol. Here, $n = 30$, $m = 25$ and the user's secret is $\{7, 15, 27, 30\}$. The symbol $\times$ denotes the response point $P \in \mathbb{R}^2$.

2.2 Description of the Adversary

The adversary considered here is a passive shoulder-surfing adversary, $\mathcal{A}$. The goal of the adversary is to impersonate $\mathcal{H}$ by initiating a new identification session with $\mathcal{C}$, after observing a number of identification sessions between $\mathcal{H}$ and $\mathcal{C}$. It is assumed that the adversary cannot view the setup phase of the protocol. However, every subsequent identification session can be viewed by the adversary as a sequence of challenge-response pairs. The number of challenges in an authentication session, denoted by r_0, is chosen such that the probability of $\mathcal{A}$ impersonating $\mathcal{H}$ with random clicks is very small. We assume that this probability is less than $(\frac{1}{2})^{r_0}$.

3 Attack 1: Difference in Distributions

Our first observation is that $\mathcal{C}$ has to ensure that at least 3 out of k secret labels are displayed on the screen. There is no such restriction on the non-secret labels. Naturally, this may lead to two different probabilities for the secret and non-secret labels. The probability that a secret label appears in a challenge is

$$\frac{1}{k\,(k-2)}\left(\frac{k\,(k+1)}{2}-3\right)$$

On the other hand, the same probability for a non-secret label is

$$\frac{1}{k-2}\frac{1}{n-k}\left(m\,(k-2)-\frac{k\,(k+1)}{2}+3\right)$$

So for instance, when $n = 112, m = 70$ and $k = 5$, in $r = 100$ challenges, the expected number of times a secret label appears is 80, compared to 61.68 for a non-secret label. This observation immediately leads to the following probabilistic attack.

Attack 1.
Input: r challenges.
Output: k labels.
1: Count the number of times each label appears in the r challenges.
2: Output the top k most frequently occuring labels.

□

The above algorithm has a high success rate provided the two aforementioned probabilities differ considerably. We performed 1000 simulated attacks for two different sets of system parameter values and the results are shown in Table 1. As can be seen, the attack, on average, outputs almost all the secret labels even with only 100 given challenges. This means only $\frac{100}{r_0} = \frac{100}{10} = 10$ identification sessions. To avoid this attack, the two probabilities should be equal, which gives the rule: $n = \frac{2km}{k+3}$. This limits allowable values of system parameters.

Table 1. Simulation Results for Attack 1

n	m	k	r	Average Number of Secret Labels	Probability of Finding all k Secret Labels
112	70	5	100	4.6	0.622
500	200	12	100	11.4	0.554

4 Attack 2

In the CHC protocol, the user only has to form a convex hull of 3 labels. Thus, in theory, there could possibly be an attack of complexity $O(\binom{m}{3})$. Our second attack runs within this bound and outputs one of the k secret labels with high probability.

4.1 The Attack

Let $\Gamma_1, \ldots, \Gamma_{\binom{m}{3}}$ denote all the possible 3-combinations of m labels.

Attack 2.

Input: r challenge-response pairs with response points $P_1, \ldots, P_r$, respectively, and a threshold τ.

Output: Label(s) with maximum frequency.

1: *Test Set.* Initialize $C \leftarrow \emptyset$. For $1 \leq i \leq \binom{m}{3}$, if $P_1 \in \mathsf{ch}(\Gamma_i)$, then $C \leftarrow C \cup \{\Gamma_i\}$.
2: *Frequency List.* For each $\Gamma \in C$, initialize $\mathsf{freq}(\Gamma) \leftarrow 1$.
3: **for** $i = 2$ to r **do**
4: For each $\Gamma \in C$, if $P_i \in \mathsf{ch}(\Gamma)$, then $\mathsf{freq}(\Gamma) \leftarrow \mathsf{freq}(\Gamma) + 1$.
5: *Thresholded Subset.* $C^{(\tau)} \leftarrow \{\Gamma \in C | \mathsf{freq}(\Gamma) > \tau\}$.
6: *Frequency of labels.* For each distinct label l in $C^{(\tau)}$ compute:

$$\mathsf{freq}(l) \leftarrow \sum_{\Gamma \in C^{(\tau)} | l \in \Gamma} \mathsf{freq}(\Gamma)$$

7: Output all labels l' such that $\mathsf{freq}(l') = \max_{l \in C^{(\tau)}} \{\mathsf{freq}(l)\}$.

□

The simulation results for Attack 2 are shown in Table 2, where the Test Set is chosen from a given set of challenge-response pairs such that the response point is closest to the boundaries of the rectangle. As can be seen, with a non-trivial probability at least one of the secret labels appears with the highest frequency, i.e., the output of Attack 2. This is true even for large system parameter values used to mitigate brute force attack. The value of τ, or the threshold, is chosen such that the size of $C^{(\tau)}$ is at least 50. There is no particular reason for this choice of τ, except to ensure that the size of $C^{(\tau)}$ is reasonably large. In all the simulation runs the bounding rectangle had end coordinates: $(0, 0), (13, 0), (0, 13), (13, 13)$.

Table 2. Output of Attack 2

Simulation Number	n	m	k	r	Secret Appeared	Sessions
1	112	90	5	20	$77/100 = 0.77$	10
2				30	$83/100 = 0.83$	14
3				50	$95/100 = 0.95$	20
4	320	200	12	20	$46/100 = 0.46$	83
5				30	$46/100 = 0.46$	125
6				50	$59/100 = 0.59$	163

4.2 Why does Attack 2 Work

The reason for the high success probability of Attack 2 is due to the following qualitative result.

Result 1 *Let $P \in \mathbb{R}^2$. Draw a line $\overline{R_1R_2}$ that intersects P and divides the rectangular lattice area into 2 partitions such that the two contain an almost equal number of lattice points. Suppose $\overline{R_1P}$ is shorter than $\overline{R_2P}$. Then the labels of the lattice points around the vicinity of $\overline{R_1P}$ will have higher values of* $\mathsf{freq}(.)$. *Furthermore, the labels of the lattice points around the vicinity of $\overline{R_2P}$ will have lower values of* $\mathsf{freq}(.)$.

Since the convex hull of any 3 secret labels is a triangle, on average, at least one secret label has a higher probability to have a high value of $\mathsf{freq}(.)$. This explains why Attack 2 is successful with high probability. Once one or more secret labels are obtained through Attack 2, the adversary can attempt to impersonate $\mathcal{H}$. The adversary can do this even with fewer than k labels, in the hope that a challenge will contain at least one of the secret labels obtained by the adversary. This can happen with a non-negligible probability.

5 Conclusion

We have shown two attacks on the CHC protocol. The first attack outputs the secret icons with high probability after observing a few authentication sessions. We have proposed a formula which allows to find values of system parameters for which this attack can be avoided. The second attack outputs a secret icon with high probability after observing only a handful of identification sessions. The attack can be used to impersonate the user with a non-trivial probability. While in its current form, the protocol does seem to have significant weaknesses, research can be done to find some variants of the protocol that are easy for humans to compute while being secure at the same time.

Acknowledgements. We thank Jean-Camille Birget for useful comments and suggestions for improvement on an earlier draft of the paper. Hassan Jameel Asghar was supported by Macquarie University Research Excellence Scholarship

(MQRES). Shujun Li was supported by a fellowship from the Zukunftskolleg ("Future College") of the University of Konstanz, Germany, which is part of the "Excellence Initiative" Program of the DFG (German Research Foundation). Josef Pieprzyk was supported by the Australian Research Council under Grant DP0987734. The work of Huaxiong Wang was supported in part by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03 and the Singapore Ministry of Education under Research Grant T206B2204.

References

[1] L. Sobrado and J. C. Birget. Graphical Passwords. *The Rutgers Scholar*, 4, 2002.

[2] H. Zhao and X. Li. S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical. In *AINAW '07*, pages 467–472. IEEE Computer Society, 2007.

[3] S. Wiedenbeck, and J. Waters, and L. Sobrado, and J. C. Birget. Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme. In *AVI '06*, pages 177–184. ACM, 2006.

[4] T. Matsumoto and H. Imai. Human Identification through Insecure Channel. In *EUROCRYPT '91*, pages 409–421. Springer-Verlag, 1991.

[5] C. H. Wang, and T. Hwang, and J. J. Tsai. On the Matsumoto and Imai's Human Identification Scheme. In *EUROCRYPT '95*, pages 382–392. Springer-Verlag, 1995.

[6] T. Matsumoto. Human-Computer Cryptography: An Attempt. In *CCS '96*, pages 68–75. ACM, 1996.

[7] S. Li and H. Y. Shum. Secure Human-Computer Identification against Peeping Attacks (SecHCI): A Survey. *Technical report*, 2003.

[8] N. J. Hopper and M. Blum. Secure Human Identification Protocols. In *ASIACRYPT '01*, pages 52–66. Springer-Verlag, 2001.

[9] D. Weinshall. Cognitive Authentication Schemes Safe Against Spyware (Short Paper). In *SP '06*, pages 295–300. IEEE Computer Society, 2006.

[10] X. Bai, and W. Gu, and S. Chellappan, and X. Wang, and D. Xuan, and B. Ma. PAS: Predicate-based Authentication Services against Powerful Passive Adversaries. In *ACSAC '08*, pages 433-442. IEEE Computer Society, 2008.

[11] M. Lei, and Y. Xiao, and S. V. Vrbsky, and C. C. Li. Virtual password using random linear functions for on-line services, ATM machines, and pervasive computing. *Computer Communications*, 31: 4367–4375, 2008.

[12] P. Golle and D. Wagner. Cryptanalysis of a Cognitive Authentication Scheme (Extended Abstract). In *SP '07*, pages 66–70. IEEE Computer Society, 2007.

[13] S. Li, and H. J. Asghar, and J. Pieprzyk, and A. R. Sadeghi, and R. Schmitz, and H. Wang. On the Security of PAS (Predicate-based Authentication Service). In *ACSAC '09*, pages 209–218. IEEE Computer Society, 2009.

[14] S. Li, and S. A. Khayam, and A. R. Sadeghi, and R. Schmitz. Breaking Randomized Linear Generation Functions based Virtual Password System. In *Proceedings of 35th IEEE International Conference on Communications (ICC)*. 2010.

[15] X. Y. Li and S. H. Teng. Practical Human-Machine Identification over Insecure Channels. *Journal of Combinatorial Optimization*, 3:347–361, 1999.

[16] H. Jameel, and R. Shaikh, and H. Lee, and S. Lee. Human Identification Through Image Evaluation Using Secret Predicates. In *CT-RSA '07*, pages 67–84. Springer-Verlag, 2007.

[17] H. Jameel, and R. A. Shaikh, and L. X. Hung, and Y. Wei Wei, and S. M. K. Raazi, and N. T. Canh, and S. Lee, and H. Lee, and Y. Son, and M. Fernandes. Image-Feature Based Human Identification Protocols on Limited Display Devices. In *WISA '08*, pages 211–224. Springer-Verlag, 2008.

[18] H. J. Asghar, and J. Pieprzyk, and H. Wang. A New Human Identification Protocol and Coppersmith's Baby-Step Giant-Step Algorithm. In *ACNS '10*, pages 349–366. Springer-Verlag, 2010.