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, Australia

[2]Department of Computer and Information Science, University Konstanz, Germany

[3]Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore

26 October, 2010

What’s Inside?

Chapters

1. Introduction to Human Identification Protocols
2. The Convex Hull Click Protocol
3. Proposed Attacks on Convex Hull Click
4. Conclusion

Questions

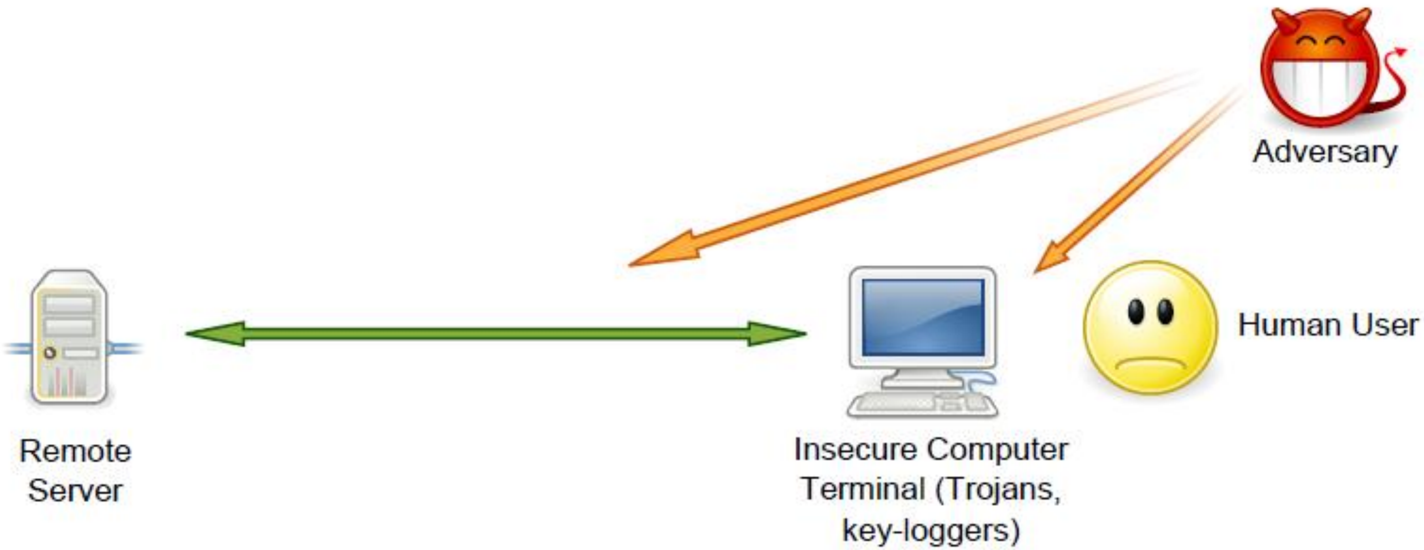
Chapter 1

Introduction to Human Identification Protocols (HIPs)

The Problem with Human Identification

How to identify a human user when

- Using an insecure terminal
- An eavesdropper is watching



The model was first conceived by Matsumoto and Imai (1991)

How Good are Traditional Solutions?

Passwords?

- Can be guessed or key-logged, etc

PINs?

- Short and often easy to guess (birthdays)
- Susceptible to shoulder surfing

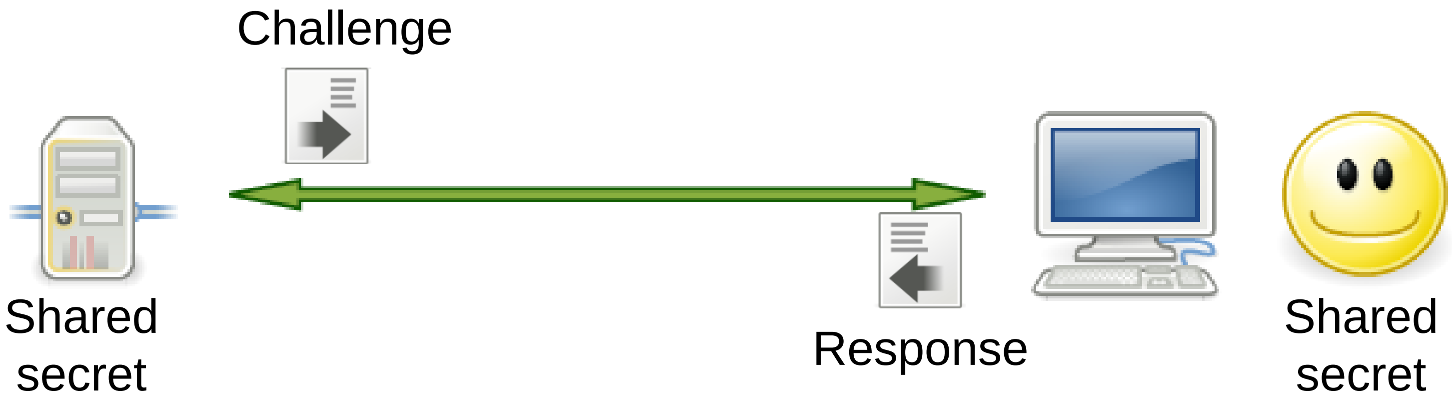
Trusted hardware or biometrics?

- Privacy concerns
- Adversary can corrupt the equipment

A Possible Solution

Challenge-response type authentication

- User *H* and computer server *C* share a secret
- *C* sends a challenge to *H*
- *H* sends a response as a function of the challenge and secret



What is a Human Identification Protocol (HIP)?

A challenge-response protocol in which the prover is a human

General Structure of an HIP

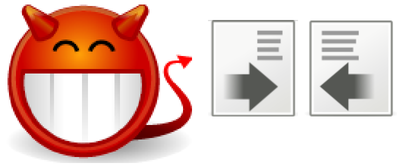
- Setup Phase: establish a shared secret
- Authentication Phase: challenge-response messages

How about Security?

No one should be able to impersonate *H*, even after observing successful authentication sessions

- Note: the adversary can see challenge-response “pairs”
- We consider passive adversaries

How can I impersonate *H*?



… And Usability?

As adversary can see everything

- Any calculations have to be done mentally

Calculations should be easy to carry out

Authentication time should be as low as possible

The Challenge

Find an identification protocol

Given a challenge and a secret, it is easy to compute response

Anyone observing challenges and responses cannot learn much about the secret

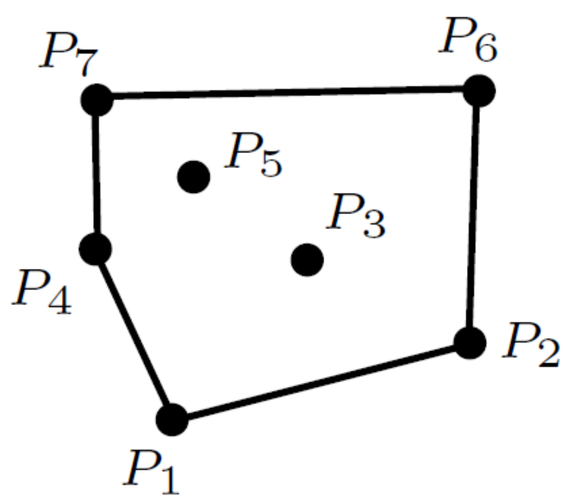
Chapter 2

The Convex Hull Click (CHC) Human Identification Protocol

Convex Hull Click Protocol

A graphical authentication protocol proposed by Sobrado and Birget (2002)

- More detailed work is done by Wiedenbeck et al. (2006)
- Based on forming convex hulls of secret icons



The Protocol

Setup Phase

Given a large pool of graphical icons

Select *k* icons as secret icons (say *k* = 5)

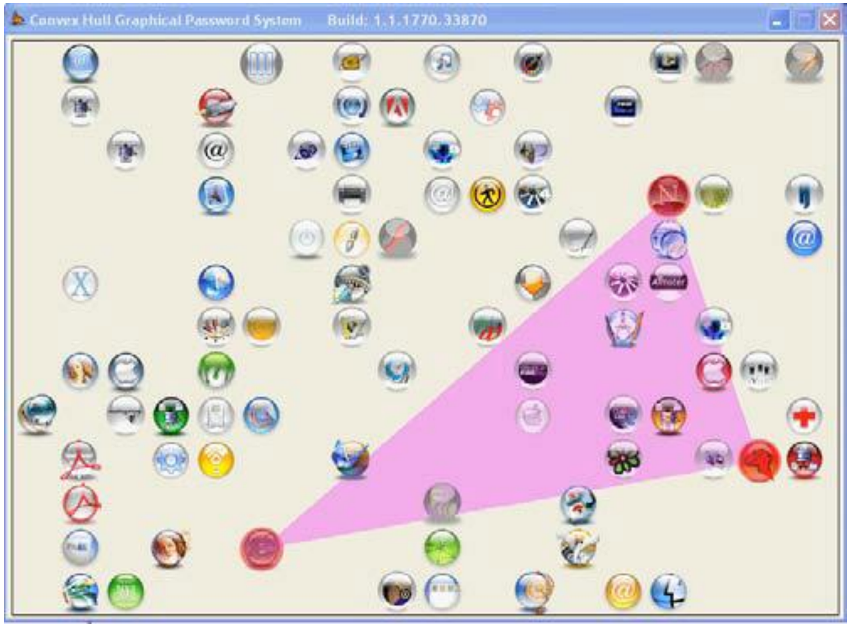
Picture source: Wiedenbeck et al. (2006)

The Protocol

Authentication Phase

- Mentally form a convex hull of any 3 secret icons
- Click a random point inside

Run 10 times to avoid random guessing



Picture source: Wiedenbeck et al. (2006)

Protocol Parameters

- Default
  - Total icons n = 112
  - Icons displayed m = 43 to 112
    - 83 on average
  - Number of secret icons k = 5
- High security
  - n = 500, m = 200, k = 12
- Convex hull formed from any 3 secret icons

Proposed by Wiedenbeck et al. (2006)

Why Convex Hull Click?

Not just a graphical password scheme

An instance of a geometric problem being used for human identification protocol

Much like finding hard mathematical problems for cryptography!

Chapter 3

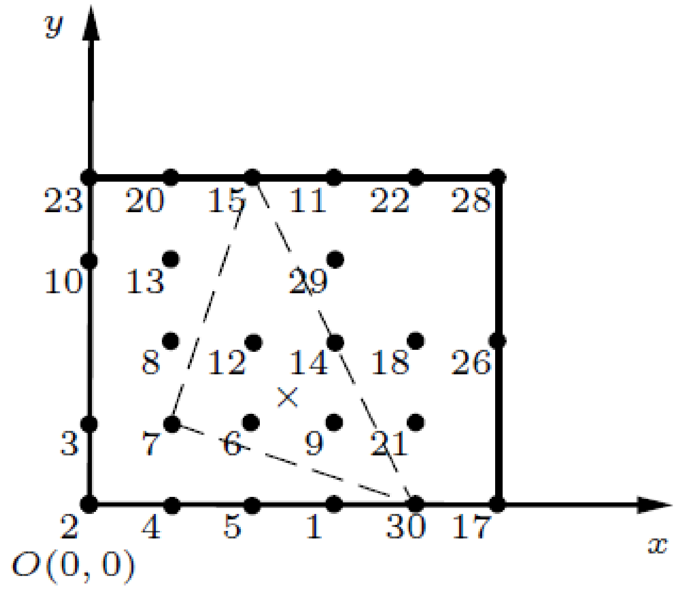
Proposed Attacks

Simplifications

Assume

Fixed *m* (number of displayed icons)

Icons are lattice points with integer labels



Attack 1

Idea

- At least 3 secret icons should be present
- Difference in probability
  - Secret vs. non-secret icons

The Attack

- Rank icons according to the frequency of appearance
- Output top *k* icons

Results

With high probability top *k* icons are the secret icons

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
112	90	5	100	0.1	0.000
500	313	12	100	0.2	0.000

How to Avoid Attack 1?

The two probabilities should be same

Rule:

$$\frac{2km}{k+3} = n$$

New System Parameter Values

If n = 112 and k = 5

- m should be 90

If n = 500 and k = 12

- m should be 313
  - Perhaps too high for comfort!

If m = 200 and k = 12

- n should be 320

Attack 2

Idea

Brute force attack works with $O(n \choose k)$

But user only uses 3 secret icons

There could be an attack with $O(n \choose 3)$

The Attack

Given a challenge and a clicked point *P*

Test Set *C*

- Find all 3-combinations of icons that contain point *P*

Make frequency lists

- For 3-combinations in *C*
- For individual icons *L* in *C*

The Attack

For r challenge-response pairs

- Increment the frequency of each 3-combination in *C* if it contains the response points
- Increment the frequency of labels

Threshold

- Find all 3-combinations in *C* that have frequency higher than threshold

Output the most frequent label in the thresholded set

Results

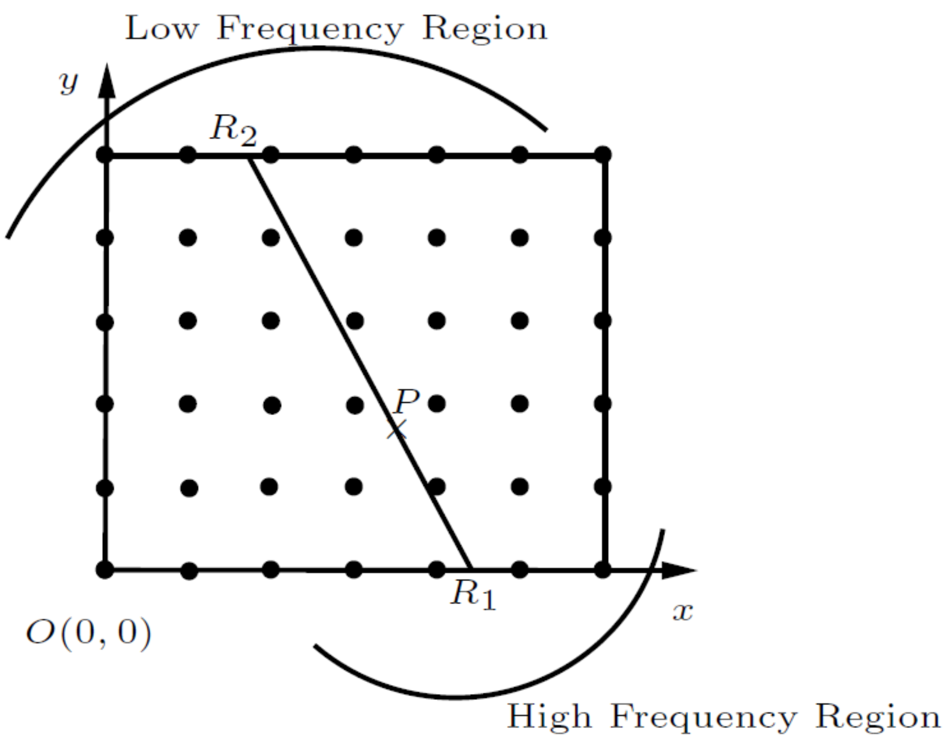
With high probability, output is one of the secret icons

Table 4. Output of Attack 2

Simulation Number	n	m	k	pairs	Secret Appeared	Average Threshold
1	112	90	5	20	$64/100 = 0.64$	6.4
2				30	$76/100 = 0.76$	7.8
3				50	$88/100 = 0.88$	10.9
4	160	100	12	20	$35/100 = 0.35$	4.8
5				30	$40/100 = 0.40$	5.6
6				50	$48/100 = 0.48$	7.2

Why Does Attack 2 Work?

Points around PR_1 can form more 3-combinations containing P



Why Does Attack 2 Work?

With high probability one of the secret icons is in the high frequency region

Because the convex hull formed is a triangle

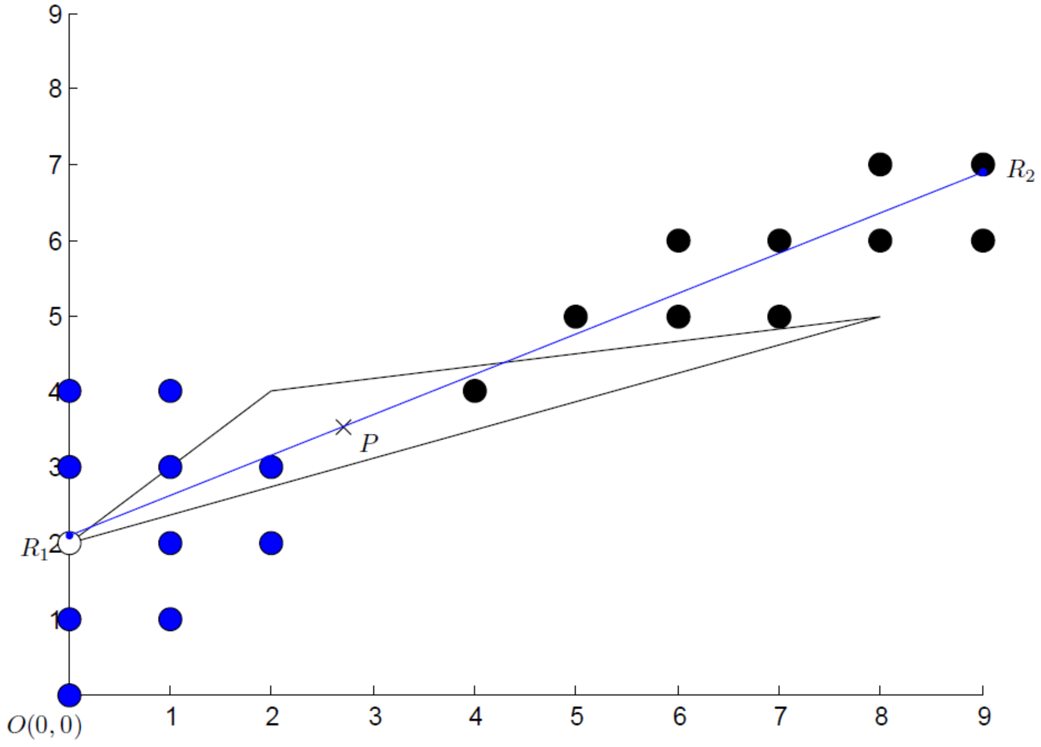
Simulation

Legends

Blue dots are icons with highest frequencies

Black dots are icons with lowest frequencies

White dot is one of the secret icons



Improved Attack 2

- Idea
  - Given r challenge-response pairs
  - Choose the challenge-response pair as the test set
    - That has the clicked point closest to the rectangle
- Call it Chosen Test Set Attack

Results

Considerable improvement

Table 5. Output of the Chosen Test Set Attack

Simulation Number	n	m	k	pairs	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	160	100	12	20	$50/100 = 0.50$	77
5				30	$67/100 = 0.67$	86
6				50	$78/100 = 0.78$	123
7	320	200	12	20	$46/100 = 0.46$	83
8				30	$46/100 = 0.46$	125
9				50	$59/100 = 0.59$	163
10	357	200	25	20	$35/100 = 0.35$	330

Impersonation

Attack 2 can be used to impersonate a user

- Adversary does not need to find all secret icons

Suppose adversary has 3 out of 5 secret icons

Impersonation Stage

If a challenge contains all 3

- Click a random point within the convex hull

If a challenge contains only 2

- Click on the line joining the two

If a challenge contains only 1

- Click on the icon

Effective security is k - 2 instead of k

Results

Suppose adversary uses Chosen Test Set Attack to find t icons

Probability that all t are secret labels and adversary succeeds in impersonating:

- $n = 112$, $m = 90$, $k = 5$, $r = 30$, $t = 2$
  - Probability = 0.59
- $n = 160$, $m = 100$, $k = 12$, $r = 50$, $t = 3$
  - Probability = 0.27
- $n = 320$, $m = 200$, $k = 12$, $r = 50$, $t = 2$
  - Probability = 0.15

r = number of challenge-response pairs

Insecurity of CHC

Probability of random clicks being successful is less than

$2^{-10} \approx 0.00098$

Convex Hull Click is not secure against an eavesdropping adversary

Can impersonate user with non-negligible probability after observing only 5 to15 sessions

Discussion and Conclusion

Problem is an inherent one

Structure of convex hulls leaks information

It is an interesting direction to find new geometric problems for human identification

Or find improvements to CHC (if possible)

References

Matsumoto, T & Imai, H 1991, ‘Human Identification through Insecure Channel’, In *Advances in Cryptology - EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science*, pages 409-421, Springer-Verlag.

Sobrado, L & Birget, JC 2002, ‘Graphical Passwords’, *The Rutgers Scholar*, volume 4, Available online at http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.

Wiedenbeck, S, Waters, J, Sobrado, L & Birget, JC 2006, ‘Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme’, In *Proceedings of the Working Conference on Advanced Visual Interfaces - AVI '06*, pages 177-184, ACM.

Questions

... ?