Theoretical security evaluation of the Human Semantic Authentication protocol

Hélène Le Bouder, Gaël Thomas, Edwin Bourget, Mariem Graa, Nora Cuppens-Boulahia, Jean-Louis Lanet

Theoretical security evaluation of the Human Semantic Authentication protocol

Hélène Le Bouder[1], Gaël Thomas[2], Edwin Bourget [1], Mariem Graa[1], Nora Cuppens[1], and Jean-Louis Lanet [3]

[1]*IMT-Atlantique SRCD, Cesson-Sévigné, France*
firstname.name@imt-atlantique.fr
[2]*DGA Maitrise de l'Information, Bruz, France*
[3]*High Security Laboratory - INRIA, Rennes, France*
{*f_author, s_author*}*@ips.xyz.edu, t_author@dc.mu.edu*

Keywords: PIN code, Human Semantic Authentication protocol, graphical password, shoulder surfing attack, dynamic password, authentication

Abstract: Using a secret password or a PIN (Personal Identification Number) code is a common way to authenticate a user. Unfortunately this protection does not resist an attacker that can eavesdrop on the user (shoulder surfing attack). The Human Semantic Authentication (HSA) protocol proposes a solution against this attack. The main idea is to have concept passwords and to propose images that the user must correctly select in order to authenticate. A concept can be represented by different pictures, so one observation is not enough to retrieve the secret. In this paper, the security/efficiency trade-off in the HSA protocol is evaluated. A probabilistic approach is used. Under the assumption that the picture/concept database is known to the attacker, we show that HSA is barely more resistant to shoulder surfing attacks than a PIN code. More precisely we show that the probability to retrieve the secret concept password increases rapidly with the number of observations. Moreover the constraints on the size of the picture/concept database are very difficult to satisfy in practice.

1 Introduction

PIN (Personal Identification Number) codes or login/password pairs are common authentication methods. For instance, these methods are used in payment cards or SIM cards. Therefore, PIN and passwords are targets of choice for malicious adversaries. The security of PIN codes or passwords relies on them being kept secret. Many attacks exist to retrieve PIN codes or passwords with keyloggers, smudge marks on the screen etc. In the case where an attacker eavesdrops on the user's authentication, the security is broken. This kind of attacks are called shoulder surfing attacks.

Motivation and Contribution. To deter different types of attacks, most smartphones use new methods to authenticate users. For example graphical passwords require the user to memorise a graphical sequence and not a number sequence. The HSA protocol introduced in (Zouinar et al., 2016; Salembier et al., 2016), appears as an efficient countermeasure against many attacks, particularly shoulder surfing attacks. The main idea of the HSA protocol is to have a concept password. At each authentication, pictures are presented to the user. She has to select images that embody her concepts in order to validate her password. For example, the concept yellow could be represented with many different images, e.g. a lemon, a sun, an American taxi etc. The authors of HSA protocol are interested by human reactions and comprehension of this solution.

In this paper, the goal is to evaluate the security of this protocol. A statistical analysis of the HSA protocol against shoulder surfing attacks is presented. We show why this solution does not offer a stronger enough security with respect to the efficiency of the scheme.

Organization. The paper is organized as follows. The state of the art is described in section 2. The HSA protocol is presented in section 3. Statistical tools to evaluate the security of this protocol are given in section 4. The evaluation of this protocol is given in 5. Finally the conclusion is drawn in section 6.

2 State of the art

2.1 Authentication methods

The most common computer authentication method is the login/password pair. The vulnerability of this method is well-known, i.e. the difficulty of remembering passwords, and it resists poorly to shoulder surfing attacks. Alternative schemes are token-based and biometric-based authentication. Token-based authentication provides strong security. It requires that the user owns a token e.g a *smart card*. However, such a token needs to be unlocked by the user, often by requiring a PIN code. In such a case, the user needs to have the token and to know something. The biometric-based authentication is often classified in behavioural-based or physiological-based method. In the behavioural scheme, the user is authenticated thanks to the voice, the keystrokes and so on; and can be performed remotely. The physiological scheme analyses the face, fingerprinting, iris etc. The sensor can only be local and thus it requires the presence of the user. Its drawbacks are accuracy, (*false positive, false negative*) and the variability of the user's characteristics mainly related to its health.

Password schemes do not resist against shoulder surfing attack, but it has been demonstrated that many other attacks can cause damages with this scheme. Unfortunately, when using a screen keyboard it is possible to guess a cell phone PIN due to several side channels. The first obvious one is related with the smudge marks on the screen. Those smudge marks indicate the four PIN digits, so an attacker knows that the PIN is one of the 24 possible permutations of those digits. At Black Hat in (Yue et al., 2014), the authors have demonstrated a new attack using video footage (thanks to Google glasses), they claim to be able to automatically recognize 90 percent of PIN code up to nine feet from the target. The used side channel is the relative motion of the victims' fingers over the touchscreen, analysing shadow formation around the fingertip as it strikes the touch screen, and using computer vision techniques.

Modern smart phones use sensors that enable a wide range of interactions, but some of these sensors can be employed as a side channel to learn about user input. In (Aviv et al., 2012), authors demonstrate that the accelerometer sensor can also be employed as a high-bandwidth side channel. Particularly, they use the accelerometer sensor to learn user tap and gesture-based input as required to unlock smart phones using a PIN/password or Android's graphical password pattern.

2.2 Side Channel, Key-logger and Observation Attacks

The security issue is probably the most important one, when accessing banking services using a smart phone. The user must be correctly authenticated using the touchscreen. Passwords and PIN code are highly sensitive assets and handling them over to third-party applications raises the following question: how a user can be sure that an application properly handles their assets? The recent discovery of password-stealing applications and other vulnerabilities in Android demonstrates that users have reason to be concerned (Felt et al., 2011). A trusted information-flow monitor such as TaintDroid (Enck et al., 2010) can track the propagation of password data, but data must be tagged before it can be tracked. Unfortunately TaintDroid does not prevent data from leaking through covert channels such as a program's control flow or timing information.

The user can upload inadvertently a spyware application in its cell phone or this latter can be shipped with a pre installed key-logger (Stavrou et al., 2017). There are a lot of programs for Android-based cell phones that are able to monitor the information sent or received by the phone. A key-logger is able to run completely in stealth mode. After it is installed it should not show up in the start-up icons or anywhere else on the phone that is being monitored. Other important features are also location tracking and remote control.

In (Xu et al., 2012) the authors describe a side channel that employs the gyroscopic orientation sensor to determine broadly where a user touches on a large keypad. They were able to infer PIN data while using the telephone keypad. Accelerometers have been used in (Owusu et al., 2012) and (Aviv et al., 2012) to infer sensitive data with an acceptable success rate.

The camera and microphone sensors are used in (Simon and Anderson, 2013) with the PIN skimmer application to retrieve the value of SIM PIN code. Every time the user touches the screen, their tool takes a photo of the user's eyes, with the front camera and saves the image along with its associated digit. The pairs (photo/digit) are sent to a server. The user photos are associated to each digit. These side channel attacks succeed because there is a direct mapping between the inferred position and the value to guess.

Randomized virtual keypads seem to be a promising solution to thwart such side channel attacks be-

cause there are no more links between position and value. Unfortunately, there is still a possibility that an installed application with enough privilege can obtain a snapshot of the screen; thus the used keyboard and obtain the link between position and value. The difficulty resides only in luring the user while the application requires permission for screen shot. Another solution, a bit more complicated, requires acquiring root privileges. As a conclusion, to avoid side channel or key logging attacks, one can use graphical password schemes. But even this solution is still vulnerable to shoulder surfing attacks.

2.3 Graphical password

The graphical password mechanism requires from the user to memorize a sequence of graphical representations instead of an alphanumeric string. Human visual memory preserves the security of the system and improves usability. Several studies evaluate the usability of graphical authentication schemes and only a few studies have focuse on the security aspects (Renaud et al., 2013). Graphical passwords are typically classified as recall-based, recognition-based, or cued recall-based.

2.3.1 Recall-based schemes

Users are either required to draw a shape from memory or repeat a sequence of actions. Examples of recall schemes are Draw-A-Secret (DAS) (Jermyn et al., 1999) and `Pass-Go` (Tao and Adams, 2008), as well as Android's Pattern Unlock.

A DAS password is a free-form picture drawn on an NxN grid. The grid is denoted by discrete rectangular coordinates (x,y) which are used to indicate the cells that are crossed by the user's drawn secret. In order for a drawn secret to be accepted in authentication, it needs to cross the same grid of cells while ensuring the breaks between the strokes occur in the same place. DAS does not rely on drawings from a semantic perspective but on the underlying grid sectors.

`Pass-Go` improves DAS's usability by encoding the grid intersection points rather than the grid cells. It overcomes the limitation of the DAS scheme, where strokes too close to adjacent cell edges could be incorrectly assigned to multiple cells.

Such pattern-based authentication mechanisms are vulnerable to attacks based on observations of smudges on the device touchscreen. Moreover, recall is a cognitively difficult task (same as a PIN code). Therefore, users tend to resort to coping strategies.

2.3.2 Recognition-based schemes

Users have to recognize a sequence of images or shapes, usually embedded in a grid of decoy images to detract attention of observers. It is the least cognitively demanding and particularly suitable for use with images.

Dhamija and Perrig (Dhamija et al., 2000) propose `Déja Vu` a recognition-based graphical authentication mechanism. Each image is abstract in nature and the collection is generated using a mathematical formula. In fact, the output depends on an initial seed. The advantage relies on the fact that the actual images do not need to be stored, just the small initial seed.

A typical scheme is `Passfaces` (Brostoff and Sasse, 2000) where a user selects a portfolio of faces from a database while creating a password. During authentication, a panel of candidate faces is presented for the user to select the face belonging to her portfolio. This process is repeated in several rounds, each round with a different panel. A successful login requires correct selection in each round.

Use Your Illusion (UYI) (Hayashi et al., 2008) relies on the human ability to recognize a degraded version of a previously seen image. UYI utilizes an image process filter to eliminate most details in an image, while preserving some features such as colour and rough shapes.

2.3.3 Cued-recall-based schemes

Users have to select target points in an image or a sequence of images. The image serves as a cue to support memory recall. Ideally, cues are only helpful to the legitimate user but not to observers.

In (Wiedenbeck et al., 2005) the authors propose a mechanism called `PassPoints`. In `PassPoints` the user is expected to select five click points on an image. The sequence of click points is the authentication secret. The image can be selected from a library or provided by the user, the only requirement being that the image is complex enough to inspire users and protect the secret. In (Suo et al., 2005) the author propose a variant which is somewhat resistant to shoulder-surfing: Cued Click Points, where images are changed after each click; with the next image selected by a deterministic function. The next image displayed is based on the previous click point so users receive immediate implicit feedback as to where they are on the correct path when logging in.

Most graphical password schemes solve the problem of key-logging attacks but remain sensitive to shoulder surfing attacks or side channel attacks.

3 The Human Semantic Authentication protocol

3.1 Definition

In (Salembier et al., 2016), the authors present the HSA protocol. They claim to be a mix between recall and cued-recall based schemes. For the authentication, the system proposes a sequence of a images set. The user selects the sequence of images that remind her its secret password. The originality of this scheme relies on the fact that the secret is not an image or a part of an image but a concept. In this paper, we suppose that the user selects an image and not a part of the image. Indeed, selecting a picture or a part of a picture is the same in the sense that a multi-parts picture could be reduced to multiple pictures in an equivalent whole pictures only scheme.

A Concept Password (CP) is a sequence of concepts, as a PIN code is a sequence of digits. On the screen, different pictures are presented to the user. Each picture contains several concepts. The user selects a sequence of pictures which contains her concept sequence in order to be authenticated.

This implies that the user must decode how the concept has been represented into the image. The authors of (Salembier et al., 2016) claim that only a human can act as a good decoder. They give some examples. An image where the concepts *yellow colour*, *tool*, *animal* and *food* are the sequential elements of the CP. Any element of the CP can be instantiated with different pictures. For example, *yellow* can be a sun, a car, a wall. Any animal can either be an *animal* or a *food* and a *bee* can be an *animal* and the item *yellow*. Several concepts can be embedded into one image, an element can represent different concepts and a concept can be in different successive images. The main feature behind the HSA protocol is to obfuscate the secret elements through diversity and redundancy. The authors pay a lot of attention to the usability of the scheme leading to studies capturing different parameters as the time to recognition, the recognition ratio, etc. They claim a strong resistance against over the shoulder attacks performed either by human or by a machine. We investigate in section 4 and 5 the resistance of the HSA protocol from a mathematical point of view either for a human attacker or a machine based attacker.

3.2 Threat model

During the authentication process, HSA presents a challenge set to the user that contains both decoy concepts and CP embedded into a set of images. The user is required to choose all concept passwords to pass the authentication. A threat model in which the adversary performs a shoulder-surfing attack is assumed. A shoulder surfing attacker intends to capture the legitimate user's concept passwords through observing the user's selection with any technical recording device.

The attacker can use any device (a camera for example) to record all the images and all the attempts. As a consequence the entire set of images is known by the attacker. In the following, we suppose that the set of concepts is publicly known.

In summary the attacker can see the different pictures selected by the user. Is she able to retrieve the CP? If so, in how many observations? What are the limits of this identification scheme?

On the other hand, in this paper we want to keep a security as strong as the one offered by a PIN code. That means that the probability of selecting the good pictures by chance has to be the same as that of testing by chance PIN code.

3.3 Mathematical description

In this section, the objective of this paper is given, with a mathematical formalisation. Let be a Concept Password CP of size n (number of concepts the user has to memorize):

$$CP = c_1, c_2, ..., c_n.$$

The set of all concepts is denoted $\mathbb{D}$ with a cardinal equal to D. The set of pictures in the database is denoted by $\mathbb{P}$. At each authentication a subset of p pictures (taken from $\mathbb{P}$) are presented to the user. Each picture can be mapped to a subset of $\mathbb{D}$ with only l concepts (each picture contains l concepts).

An attacker can have a divide an conquer approach and attack one concept at a time. So in the following, the attacker tries to find a single concept c_i (e.g. the i-th concept of the concept password) within a sequence of observed pictures. In this paper $\mathbb{D}_j$, denotes the set of l concepts included in the picture selected by the user at the j-th authentication for a given concept c.

3.3.1 Main questions.

In the rest of this paper, we want to know if an attacker can easily retrieve the concept password according to the number of concepts and its repartition. In other words, for a strong security implementation of HSA, we want to answer the following main questions:

1. How many concepts in total (D size of $\mathbb{D}$)?
2. How many concepts in a picture (l)?

3. How many pictures should be presented to the user for one authentication (p)?

4 How to evaluate the number of concepts required ?

In this section various probability constraints are introduced in order to have an approximation for a good pair D and l. More precisely, this paragraph gives the tools to answer the questions 1 and 2.

4.1 Probability to select a good picture

The number of concepts by picture is fixed and noted l. Extreme values of l do no make sense. If $l = 1$ it is equivalent to a classic PIN. If $l = D$, all pictures contain all concepts: any sequence of pictures validates the *CP*. It is preferable to strike a better balance between these two extreme values.

Let be Q the probability of the event:
The attacker selects a picture associated to the concept c by chance.

$$Q = \frac{l}{D} \quad . \tag{1}$$

This probability shows that a picture does not have to contain too many concepts.

To have the same security as a PIN or better, it means that

$$Q = \frac{l}{D} \leqslant \frac{1}{10}.$$

Thus, l the number of concepts by picture has to be:

$$l \leqslant \frac{D}{10} \quad .$$

4.2 Probability to retrieve a concept

The attacker has a set of N observed pictures for the concept c, obtained from the shoulder surfing attack.

Let $\mathcal{P}(N)$ be the probability of the event: "the attacker has retrieved the concept c", with N observations. There are two cases:

1. The event A:

$$\bigcap_{j=1}^{N} \mathbb{D}_j = \{c\} \quad \text{and} \quad \mathcal{P}(N) = 1 \quad .$$

   The attacker is sure that she has retrieved the good concept.

2. The event $\overline{A}$:

$$c \subsetneq \bigcap_{j=1}^{N} \mathbb{D}_j \quad ;$$

   but the intersection is not equal to the singleton $\{c\}$ so:

$$\mathcal{P}(N) = \frac{1}{k}, \quad \text{with} \quad k = \#\bigcap_{j=1}^{N} \mathbb{D}_j \quad .$$

Finally:

$$\mathcal{P}(N) = \sum_{k=1}^{l} \frac{1}{k} \cdot P\left[\#\left(\bigcap_{j=1}^{N} \mathbb{D}_j\right) = k\right] \quad . \tag{2}$$

As c is the common concept of all observations of the attacker, the following notations are introduced:

$$\mathbb{D}^* = \mathbb{D}\backslash\{c\} \quad \mathbb{D}_j^* = \mathbb{D}_j\backslash\{c\}$$
$$D^* = D-1 \quad l^* = l-1 \quad .$$

With these new notations, $\mathcal{P}(N)$ is a sum of $\mathcal{P}_k(N)$ with the factor $\frac{1}{k+1}$;

$$\mathcal{P}(N) = \sum_{k=0}^{l^*} \frac{1}{k+1} P_k(N) \quad ; \tag{3}$$

with:

$$\mathcal{P}_k(N) = P\left[\#\bigcap_{j=1}^{N} \mathbb{D}_j^* = k\right] \quad . \tag{4}$$

Estimation by recurrence

The goal of this part is to write the probability $\mathcal{P}(N+1)$ with $\mathcal{P}(N)$.

The probability $\mathcal{P}_k(N)$ defined in equation (4) is used.

If $N = 2$, the attacker can see only two observations, $\forall k, \quad \mathcal{P}_k(2)$ can be computed.

$$\mathcal{P}_k(2) = P\left[\#\left(\mathbb{D}_2^* \bigcap \mathbb{D}_1^*\right) = k\right] \quad ;$$
$$\mathcal{P}_k(2) = \frac{\binom{l^*}{k} \cdot \binom{D^*-l^*}{l^*-k}}{\binom{D^*}{l^*}} \quad .$$

This corresponds to a hypergeometric distribution. This distribution describes the probability of drawing k "successes" in l^* draws, *without* replacement, from a population of D^* objects that contains l^* objects labelled "success". $\mathcal{P}_k(2)$ can be seen as drawing l^* concepts to form $\mathbb{D}_2^*$, k of which should be taken from $\mathbb{D}_1^*$ (success).

Then, a recurrence relation can be defined:

$$\mathcal{P}_k(N+1) = \sum_{k'=0}^{l^*} \frac{\binom{k'}{k} \cdot \binom{D^*-k'}{l^*-k}}{\binom{D^*}{l^*}} \cdot \mathcal{P}_{k'}(N) \quad . \tag{5}$$

This is also a hypergeometric distribution : draw l^* concepts to form $\mathbb{D}_N^*$, k of which should be taken from $\bigcap_{j=1}^{N} \mathbb{D}_j^*$, assuming the latter is of size k'. Then, summing of all the values of k'. Thanks to the relation 5, $\mathcal{P}(N)$ can be computed in practice.

5 Evaluation of the protocol HSA security

5.1 Security conditions

5.1.1 Consequences of $\mathcal{P}(N)$

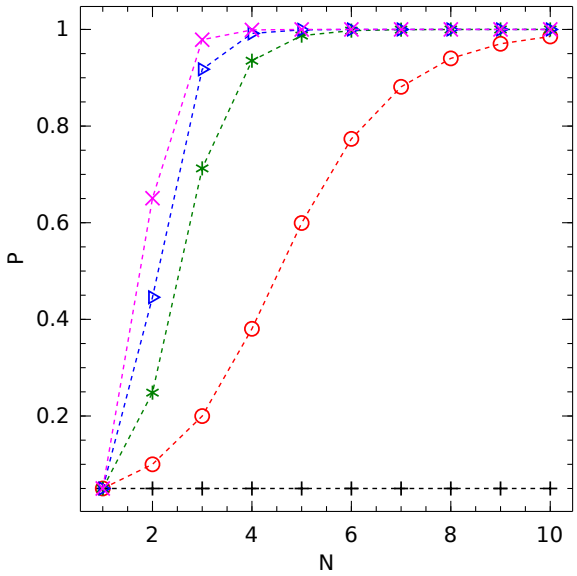

Figure 1: Probability $\mathcal{P}$ according to N, for $l = 20$ and $D = 20$ in black $+$, $D = 40$ in red $\circ$, $D = 100$ in green $*$, $D = 200$ in blue $\triangleright$, $D = 400$ in magenta $\times$.

Figure 1 illustrates the probability according to different values of the number of observation N, for the number of concepts l by picture fixed to 20, and different values of the total number of concepts D.

The black $+$ curve is the extreme case where $D = l = 20$; it means that a picture contains every concept. So it is impossible to retrieve the concept c and $\mathcal{P} = \frac{1}{D}$; but this makes no sense from the HSA protocol point of view. Indeed, all pictures validate all concepts.

The blue $\triangleright$ curve represents the case with the same security as a PIN code for $N = 0$. More precisely: $D = 10 \cdot l = 200$.

There is a $\frac{1}{10}$ chance to select a picture which contains the correct concept. Figure 1 shows that $\mathcal{P} > 0.9$ after only $N = 3$ observations.

For all different values of $D > l$, $\mathcal{P}$ rapidly increases.

Figure 2 and Figure 3 illustrate the shoulder surfing security for various values of l and D. The dashed lines are the line $D = 10 \cdot l$. They represent $Q = \frac{1}{10}$, the probability to select a correct image by chance; for a PIN code, it is equal to $\frac{1}{10}$ as explained in 4.1.

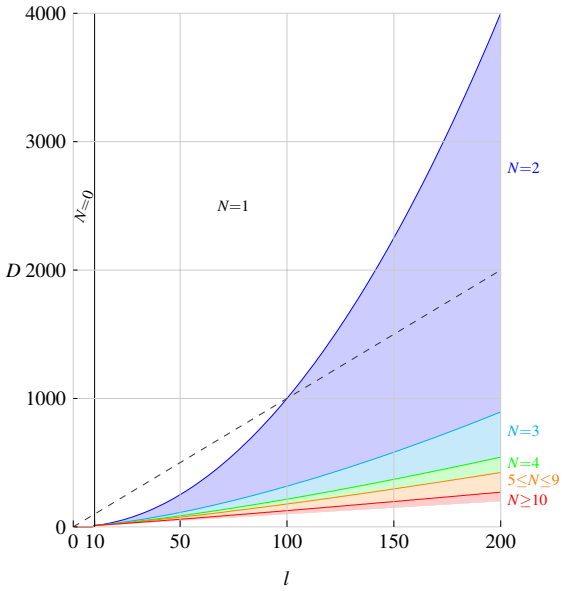

Figure 2: **The shoulder surfing security:** Maximum number N of observations made by an attacker such that they can correctly guess the right concept with probability $\mathcal{P}(N) \leq \frac{1}{10}$, as a function of the number l of concepts per picture, and of the total number D of concepts. All points inside the region of the same colour share the same value of N. The dashed line is the line $D = 10l$.

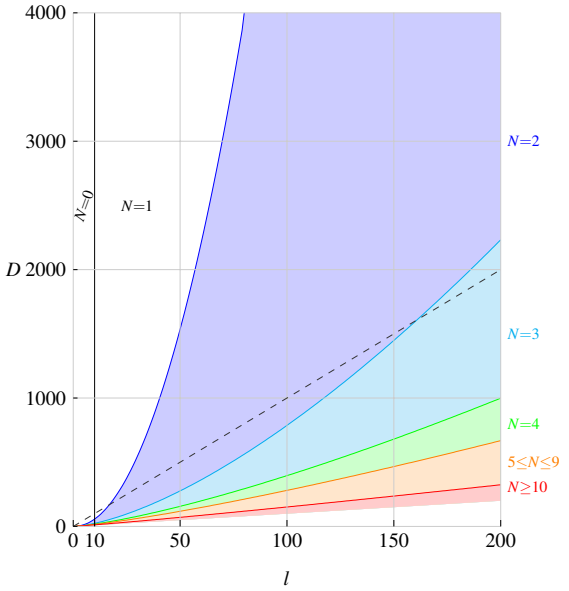

Figure 3: **The shoulder surfing security:** Maximum number N of observations made by an attacker such that they can correctly guess the right concept with probability $\mathcal{P}(N) \leq 0.5$, as a function of the number l of concepts per picture, and of the total number D of concepts. The dashed line is the line $D = 10l$.

Figure 2 gives the maximum value of N for which

$\mathcal{P} \leq 0.1$, holds. For example if $l = 150$ and $D = 1000$, then until $N = 2$ observations $\mathcal{P} \leq 0.1$; and with $N = 3$ observations $\mathcal{P} \geq 0.1$. Every point inside the region of the same colour share the same value of N. The dashed curve represents a limit not to cross to keep PIN code security with $N = 0$ observation. If the dashed curve is used; if $l = 150$ then D has to be equal to at least 1500.

In conclusion of this Figure 2, in order to have $\mathcal{P} \leq 0.1$ with $N = 2$ observations, $D = 1000$ concepts are required and every picture has to contain $l = 100$ concepts.

Figure 3 is the same as Figure 2, but with $\mathcal{P} \leq 0.5$. With $D = 2000$ and $l = 200$, with $N = 4$ observations, the probability $\mathcal{P}$ to retrieve the concept is bigger than 0.5.

5.1.2 Constraints

To avoid sieve attacks, all concepts have to be present on screen authentication. In order to not have some concept password more secure than others, each concept have to be contained in the same number of pictures on the same screen. Moreover, to keep the same security as a PIN code for $N = 0$ observation, each concept has to appear in $\frac{1}{10}$ of the pictures at most . On the other hand, every picture has to contain the same number of concepts l in order to not introduce any new bias.

The estimation of l implies that a compromise is required. Indeed, the bigger the number of concepts l by picture, the better is $\mathcal{P}(N)$ the probability to retrieve a concept. On other hand, the smaller the number of concepts l by picture, the better is Q the probability to select a good picture by chance.

Finally, we try to answer to the questions 1,2 and 3 of paragraph 3.3.1.

- If $l = 200$ concepts per image, 2000 concepts are required to have a good security up to $N = 3$ observations. A picture is a random subset of l concepts in D concepts.

$$\binom{D}{l} = \binom{2000}{200} \approx 10^{280}$$

  There are $\approx 10^{280}$ possible concept subsets.

- If $l = 100$ concepts by pictures, 1000 concepts are required to have a good security up to $N = 2$ observations. There are $\approx 10^{140}$ possible concept subsets.

5.2 Security/efficiency trade-off

In the previous section, the human limits and the hardware limits have not been taken into account.

Store 10^{140} pictures is impossible. Is it possible to have fewer pictures and keep the same security ? Studying how many pictures are enough is another subject of research for a future work. A solution would be to generate pictures on the fly. Another solution could be that pictures are stored on cloud, but that means that a connexion is required for authentication.

It is important that the HSA protocol can be used by real people. This protocol has to stay practical.

A human limit is for example the number of pictures which are printed on the screen. In (Zouinar et al., 2016; Salembier et al., 2016), the authors use only 4 concepts by pictures. One has to remark than 4 is very small.

Another problem is the capacity for a user to retrieve concepts in a picture. If a concept is obvious then the attacker can discover it very fast. For example a colour is a too obvious concept. On the other hand, concepts should not to be too abstract, since users must be able to retrieve them in a picture. Furthermore, according to the culture, abstract concepts can be seen differently. For example the concept *wisdom* could be represented by an elephant or an owl in different cultures.

6 Conclusion

The HSA protocol is better than a simple PIN code against shoulder surfing attacks. Unfortunately its improvement is minimal.

In (Zouinar et al., 2016; Salembier et al., 2016), the authors use only 4 concepts by pictures, so the security is broken for 2 observations. Indeed, in practice even if many concepts are used to generate the different pictures, this solution is not secure after 2 or 3 observations by the attacker. If $l = 200$ concepts by pictures, 2000 concepts are required to have a good security up to $N = 3$ observations and $\approx 10^{280}$ pictures are possible. If $l = 100$ concepts by pictures, 1000 concepts are required to have a good security up to $N = 2$ observations and $\approx 10^{140}$ pictures are possible. This represents many possible pictures with many concepts in each picture just to resist to only 2 or 3 observations.

Moreover, human limits and hardware limits are not taken into account in this paper. But they represent important limitation in the implementation. Generating pictures on the fly would be an interesting solution, as it would solve many problems of HSA. An attacker won't be able to know the picture database since it does not exist and the device won't have to store all pictures. So she would need detect concepts in pictures. To our knowledge the best methods involve machine learning algorithms. That requires a characterisation step, with a numerous data samples.

Another question is how to generate a picture with 100 concepts such that a human is able to retrieve her concept in this picture?

In practice, it is often better to have no security at all and be fully aware of it rather than having a false feeling of protection relying on weak security. An HSA user is less alert than a standard PIN code user against shoulder surfing attacks. Since they feel protected against this kind of attacks, they are more careless in hiding their authentication. Yet security breaks down quickly (3 observations), so they should not relax their attention.

REFERENCES

Aviv, A. J., Sapp, B., Blaze, M., and Smith, J. M. (2012). Practicality of accelerometer side channels on smartphones. In *Proceedings of the 28th Annual Computer Security Applications Conference*, ACSAC '12, pages 41–50, New York, NY, USA. ACM.

Brostoff, S. and Sasse, M. A. (2000). Are passfaces more usable than passwords? a field trial investigation. In *People and Computers XIVUsability or Else!*, pages 405–424. Springer.

Dhamija, R., Perrig, A., et al. (2000). Deja vu-a user study: Using images for authentication. In *USENIX Security Symposium*, volume 9, pages 4–4.

Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., and Sheth, A. N. (2010). Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones. In *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation*, OSDI'10, pages 1–6, Berkeley, CA, USA. USENIX Association.

Felt, A. P., Finifter, M., Chin, E., Hanna, S., and Wagner, D. (2011). A survey of mobile malware in the wild. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '11, pages 3–14, New York, NY, USA. ACM.

Hayashi, E., Dhamija, R., Christin, N., and Perrig, A. (2008). Use your illusion: secure authentication usable anywhere. In *Proceedings of the 4th symposium on Usable privacy and security*, pages 35–45. ACM.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D. (1999). The design and analysis of graphical passwords. USENIX Association.

Owusu, E., Han, J., Das, S., Perrig, A., and Zhang, J. (2012). Accessory: Password inference using accelerometers on smartphones. In *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*, HotMobile '12, pages 9:1–9:6, New York, NY, USA. ACM.

Renaud, K., Mayer, P., Volkamer, M., and Maguire, J. (2013). Are graphical authentication mechanisms as strong as passwords? In *Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on*, pages 837–844. IEEE.

Salembier, P., Zouinar, M., Héron, R., Mathias, C., Lorant, G., and Wary, J.-P. (2016). Experimental studies of a graphical authentication system based on semantic categorisation. In *Actes de la 28ième conférence francophone sur l'Interaction Homme-Machine*, pages 134–143. ACM.

Simon, L. and Anderson, R. (2013). Pin skimmer: Inferring pins through the camera and microphone. In *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, SPSM '13, pages 67–78, New York, NY, USA. ACM.

Stavrou, A., Benameur, A., and Johnson, R. (2017). All your sms and contacts belong to adups and others. *Proceedings of the Black Hat USA*.

Suo, X., Zhu, Y., and Owen, G. S. (2005). Graphical passwords: A survey. In *Computer security applications conference, 21st annual*, pages 10–pp. IEEE.

Tao, H. and Adams, C. (2008). Pass-go: A proposal to improve the usability of graphical passwords. *IJ Network Security*, 7(2):273–292.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., and Memon, N. (2005). Passpoints: Design and longitudinal evaluation of a graphical password system. *International journal of human-computer studies*, 63(1-2):102–127.

Xu, Z., Bai, K., and Zhu, S. (2012). Taplogger: Inferring user inputs on smartphone touchscreens using onboard motion sensors. In *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WISEC '12, pages 113–124, New York, NY, USA. ACM.

Yue, Q., Ling, Z., Fu, X., Liu, B., Yu, W., and Zhao, W. (2014). My google glass sees your passwords! *Proceedings of the Black Hat USA*.

Zouinar, M., Mathias, C., Lorant, G., and Wary, J.-P. (2016). Evaluation ergonomique d'un système d'authentification graphique.