Recall-A-Story, a story-telling graphical password system

Yves Maetz
Thomson Security Labs
Cesson Sévigné, France
yves.maetz@thomson.net

Stéphane Onno
Thomson Security Labs
Cesson Sévigné, France
stephane.onno@thomson.net

Olivier Heen
INRIA/IRISA
Rennes, France
olivier.heen@inria.fr

Strong text-based passwords are often hard to remember. Several graphical password systems have already been developed to overcome this problem. Xiaoyuan Suo [1] widely surveys graphical password systems like Blonder, Passpoint, Passfaces, Draw-A-Secret, Recall-A-Formation.
We propose *Recall-A-Story*, a graphical password method with the following properties: a "story-telling based" memorization method, a larger password space for strong robustness, the ability to customize the graphical elements and the ability to print out the graphical password without fully revealing it. We illustrate the relevance of *Recall-A-Story* in several use cases, such as unlocking a touch screen device (e.g. mobile phone) or accessing encrypted data storage.

1. PRINCIPLE

With *Recall-A-Story*, the user builds a graphical password through a "story-telling" mechanism:

1. He sets the framework of the story by selecting a background picture,
2. He picks images and places them successively onto the background picture to populate the framework and therefore tells the story given by the sequence and position of the images.

The resulting password is calculated as following:

$$Password = background + \{(image, position)_1,.. \{(image, position)_n\}$$

This password value may be hashed and completed by a salt before being used in traditional cryptographic systems.

Figure 1 illustrates a password that may tell the following story: "After having started the fire in the barbecue, I went to the other side of the house to play soccer. Then the dog approached the barbecue too close and burnt his tail". The resulting password would be based on the sequence "house; barbecue on the grass; ball near the house; dog near the barbecue".

2. USER INTERFACE CONSIDERATIONS

When the user needs to enter his password, an authentication screen is displayed. This screen is composed mainly of an area where the background picture is shown and an area displaying a set of small images. Appropriate means allow browsing through a set of background pictures and selecting one, and allow browsing through sets of images, selecting one image, and placing it onto the background.

Figure 1 depicts an implementation of *Recall-A-Story* for a tactile mobile phone with a typical "touch & slide" user interface where browsing through the images is done through horizontal sliding. To enter the story introduced in section 1, the user first selects the frame of his story. This is done by sliding horizontally the upper area until displaying the house. Then he slides horizontally the image ribbon until the barbecue image is shown. He selects the barbecue image from the image ribbon and places it on the grass. Same operation is done for the soccer ball image that is placed near the house, and the dog image placed near the barbecue. The user validates this password by pressing the unlock button.

Figure 1: unlocking a touchscreen device

The position of the images will be simply given by a grid. To avoid the ambiguous problem of placing an image at the limit between two cells of the grid, the system highlights the chosen grid during the image placement.

The number of graphical elements, their size, the number of grid positions should be chosen regarding the level of security to achieve (See Table 1), the device rendering and selection capabilities and the user dexterity and memorization capacity.

Each time the authentication screen is displayed, a random background picture is selected and the icons are placed onto the ribbon at random places to prevent replay attacks using simple key-loggers.

Symposium On Usable Privacy and Security (SOUPS) 2009, July 15-17, 2009, Mountain View, CA, USA.

3. USE CASES

Unlocking a touchscreen device

As detailed in previous section, *Recall-A-Story* replaces advantageously the unlock mechanism of touch screen devices (mobile phones, portable media players, web tablets...). Unlocking these devices is generally done by entering a pin code, an optimal solution when the device includes a real keyboard. When it doesn't, a virtual keyboard has to be displayed which often does not fit to the overall "touch & slide" style. With our solution, we can improve the robustness compared to the four digit code while only requiring the user to recall three elements (see Table 1) and keeping the overall look and feel.

Authenticating to online service

Recall-A-Story may be used also for online authentication. The authentication screen can be seamlessly integrated in the application itself, using graphical elements related to the service. This is particularly interesting for online games where the graphics are specific to each game. The customization could also address a wide range of population. For children or elderly people, the number of images and places can be tuned quite low, while still providing minimal level of security.

Accessing encrypted data storage

Recall-A-Story applies to removable storage devices hosting encrypted files. The *Recall-A-Story* application and its graphical elements are stored in the clear on the device. The application is launched when the device is plugged on a computer. When the user enters the correct graphical password, the application generates a secret value used to encrypt and decrypt files on the fly. Background pictures and images may use user's own pictures locally stored on the device, therefore allowing personalizing the context of the story and possibly improving the recall success rate.

4. ADVANTAGES

Large password space

Recall-A-Story exhibits a high theoretical resistance to brute force attacks: the theoretical password space is larger than with text passwords of the same length. Similarly, for a given resistance, *Recall-A-Story* requires fewer elements than classical textual passwords. This is shown in Table 1 for our three typical uses cases.

	Backgr.	Images	Places	Length	Text password space	*Recall-A-Story* password space
Touchscreen	4	16	4	3	242 235	1 048 576
Online	4	16	9	4	15 018 571	$\approx 1.7\ 10^9$
Data storage	10	20	16	5	$\approx 9.3\ 10^8$	$\approx 3.4\ 10^{13}$

Table 1: comparison of theoretical password spaces

The text password space is computed for a password of length at most l over an alphabet of s symbols. In table 1, we use a 62 symbols alphabet: [a-z][A-Z][0-9]. The general formula is:

$$Text\ password\ space = (s^{l+1} - 1) / s - 1$$

The *Recall-A-Story* password space is computed for a password of length exactly l ordered images among i, over p places and b backgrounds. The formula is:

$$Recall\text{-}A\text{-}Story\ password\ space = b \cdot (i \cdot p)^{l}$$

Although "Touchscreen" use case proposes few backgrounds and images, its theoretical password space is larger than its text equivalent. The "Online" use case is meant to be used on a PC with better grid precision, hence the larger number of places. The "Data storage" device could store more internal graphic elements, thus enable higher security level.

Ease of recall

Shepard [2] stated that it is easier to remember images than text. In *Recall-A-Story*, we add a semantic level created by the user himself, based on a story that may be very personal. The personalization goes further if the user's personal images are used.

Printable

When the password is only used sporadically (e.g.: once every 6 months for archiving purpose), it could be useful to print the password. The printed image does not completely reveal the password since the order is unknown. The resistance to brute force is not very strong for short passwords (length: 5! = 120 combinations for 5 icon long password) but much better than a printed text-based password.

An interesting feature is the possibility to print some of the first images of a complex story to help the user to bootstrap and remember the rest of the story.

5. PERSPECTIVES

Recall-A-Story raises many questions that should still be studied. The strong intuition that a personalized story-telling picture is easier to recall than existing graphical password systems shall be verified and quantified. How does the fact that passwords are not random decrease the effective password space? A paper printed copy of the password surely helps the user to remember the correct order of images position, but is it still true after a long time?

A proof of concept is being implemented and will be used in future usability tests.

6. REFERENCES

[1] Xiaoyuan Suo, *A design and analysis of graphical password*, Master of Science Thesis, Georgia State University, 2006

[2] R. N. Shepard, *Recognition memory for words, sentences, and pictures*, Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967R.

Symposium On Usable Privacy and Security (SOUPS) 2009, July 15-17, 2009, Mountain View, CA, USA.