Life-Experience Passwords

Simon S. Woo
Computer Science Department
University of Southern California
Los Angeles, CA, USA
Email: simonwoo@usc.edu

Jelena Mirkovic
Computer Science Department
University of Southern California
Information Sciences Institute
Marina Del Rey, CA, USA
Email: sunshine@isi.edu

Elsi Kaiser
Linguistics Department
University of Southern California
Los Angeles, CA, USA
Email: elsi.kaiser@usc.edu

***Abstract*—User-supplied textual passwords are extensively used today for user authentication. However, these passwords have serious deficiencies in a way they interact with human natural ability to form memories. Strong passwords that are hard to crack are also hard for humans to remember, while memorable passwords are easily brute-forced or guessed. Recently, a number of alternatives to textual passwords have been proposed, such as drawing a password, selecting images from a list, learning a tune, etc. All these approaches have a common deficiency that they ask users to form new memories, which leads either to easily-remembered, easily-guessed or secure but easily-forgotten passwords. We propose novel *life-experience passwords* (LEPs). Unlike existing approaches, our passwords are built from a user's episodic memory about defining life events, and should be both more memorable and harder to guess than traditional passwords.**

I. Introduction

User-supplied textual passwords are extensively used today for user authentication, both for personal devices and for remote servers. However, current practice shows that user-supplied textual passwords fail to meet these requirements [1], [2]. It is very natural for humans to create passwords that consist only of lowercase letters and contain dictionary words, personal names or locations, which makes it easy for attackers to guess them. Even when forced to use a combination of different symbols, such as alphabet letters and numbers, users combine them in predictable ways that significantly increase the attacker's ability to guess the password. Some servers force users to create passwords that have a certain strength, e.g., a combination of lower and uppercase letters, numbers and special symbols, ensuring that they are not easily guessed. Yet such passwords are hard for users to remember, which leads to other insecure practices such as emailing the password to oneself, writing it down or reusing it at many different sites.

Several password-based authentication methods have been proposed that do not rely on user-supplied textual passwords. For example, a user may be asked to draw an image for a password, select several pleasing images from a set, learn a tune and repeat it, or answer a set of questions about her likings and preferences. Many of the alternatives have the same deficiencies as user-supplied textual passwords – users' passwords are either easy to guess or users have trouble remembering them themselves. Additionally, non-textual passwords require special effort by a user to set up, special processing by a server to be verified and are not compatible with servers that support only textual access. Thus alternatives to user-supplied textual passwords have so far failed to significantly improve the security of password-based authentication, but they have increased the user burden for set up and verification.

The main problem with current password approaches is that they force a user to create new but complex memories that can be accurately retrieved after long stretches of time. To address this issue, we propose a novel life-experience passwords (LEPs) that is built from a user's episodic memory about their personal experiences. We believe that passwords generated from personal experience and episodic memory events are significantly easier for users to remember and harder for others to guess.

II. Life-Experience Passwords (LEPs)

We propose a novel approach to user-supplied textual passwords, life-experience passwords (LEPs). LEPs are built from a user's episodic memory about their personal experiences, e.g. weddings, births, graduations, vacations, etc. To ensure memorability we would use only those experiences that occurred a number of years ago, and have thus already been memorable enough to remain in user's mind. LEPs would consist of several factoids related to a user-chosen personal experience. The verification process would prompt the user with questions about these factoids and the user answers would represent the password. We expect that providing a higher level of details memorable to the user would ensure the originality and strength of LEPs. Given a user's life event such as wedding, some of the factoids about it may be mined from social media – e.g., the location – but others should be known only by the user – e.g., why she chose the specific wedding dress, which song played for the first dance, which guest said or did what at the event, etc. Our work is similar to security questions for secondary authentication in intent, but different in details and resulting security against attacks. Security questions contain a limited set of questions, while LEPs could potentially have unlimited set of factoids. Security questions have a single factoid that may be easily researched from public sources, while LEPs have several factoids, some of which should uniquely be known only by the user.

A. Benefits

We believe that LEPs provide the following benefits:

1) **Easy to remember** – a user would be asked to only use memories that are several years old and thus have already proved significant enough to be retained in memory.
2) **Hard to guess** – while many people have similar life experiences, the details of these experiences that are memorable enough differ widely between people, even between those witnessing the same event.

3) **Abundance of memories leads to password diversity** — Humans have a large number of personal experiences they can draw on to generate diverse passwords for diverse purposes.

Thus, LEPs would address the deficiencies of current user-supplied passwords, significantly improving the security of password-based authentication.

B. Challenges

While LEPs have high potential to improve memorability and strength of textual passwords, there are multiple challenges that we seek to address as follows:

- **Scope:** Are LEPs suitable for any authentication task? Since each LEP consists of several factoids the user burden for password input is higher for LEPs than for old-fashioned one-word passwords. At which log in frequency does this burden become unacceptable to users?
- **User-friendly password generation:** How does a user generate a LEP ? How much guidance is provided by the system with regard to the suitability of the chosen life experience and factoids?
- **Dealing with synonyms:** While a fact may be memorable for a human, the narration of that fact may vary in user input. How does LEP verification recognize and handle synonyms ?
- **The right amount of private information:** Guessability of LEP by mining public information is directly proportional to the amount of private information contained in the password's factoids. How does the system guide the user to select private vs. public information in LEP generation?

III. Our Approach

In our preliminary work we have identified several approaches to password generation and verification. We are in the process of building prototypes of the system deploying these approaches, and performing security analyses and user studies to measure security, memorability and diversity of resulting passwords.

A. LEP Topics

We have identified the following list of potential topics for LEPs: (1) Milestone events, such as weddings, engagements, divorces, births, deaths, graduations, etc., (2) Travel events, (3) Learning experiences, such as learning to ski, sing, paint, play tennis, etc., (4) Flashbulb events, such as 9/11, hurricane Sandy, Fukushima disaster, etc. For each of these, relevant factoids would speak about the details that a human is likely to recall with high consistency, such as time, location, people, conversations and activities. Even if a remembered detail mismatches what truly happened, it can still be used as a factoid as long as the user consistently remembers it the same way. We specifically avoid use of information about feelings and preferences for factoids, as humans tend to remember this type of information inconsistently.

B. Password Generation and Verification

The first step in our research will be to investigate how LEPs can best be generated. Both [3] and [4] use everyday memory and autobiographical information for generating authentication questions. Only calendar events are used in [4]. However, [3] collected data from various sensors in a smartphone and further analyzed relationship between memorability and various event categories. Unlike [3] and [4] works that capture everyday memory events for password generations through digital means, we require users to actively input LEPs. This may generate a high cognitive load on a user, which would reduce usability of our passwords. We plan to investigate three methods for password generation:

1) *Prompted input*, where a user is prompted by a series of questions to speak about a chosen life event.
2) *Guided input*, where a user is prompted to list a given number of factoids for a chosen event in unstructured language.
3) *Free input*, where a user is prompted to speak about a chosen event in unstructured language.

During password verification the system prompts the user with questions about the chosen life event and compares user answers with the replies stored during password generation. We will consider two approaches to user input collection for verification: 1) *Blank verification* – A user is asked the question and required to provide the answer, and 2) *List verification* – A user is presented with a list of partial or full answers and asked to select the right one. A user may be asked to just click on the chosen answer or to also complete it, in case of partial answers. Our chosen generation and verification methods have different tradeoffs security of resulting passwords and human burden for their input.

IV. Initial Results

We obtained LEPs from 10 users in a *prompted input* and *free input* form and assessed the recall rates. Overall, about 70 percent of answers are correctly recalled by users. We found that users had difficult time recalling exact answers for events that are dynamic or not unique such as hobbies. Hobbies can be changed over the time and people usually have more than one. In addition, answers related to feeling had low recall rates because there are many ways to express feeling. With these initial findings, we are currently working on 1) categorizing and refining types of episodic events that are difficult to be guessed and not be easily found from social networking sites or web search, and 2) that can be more effectively used for LEPs. Also, we are analyzing different types of attacks on LEPs such as inference attack and random guess based on the given story context. Further, we are working on auto-generating questions from user provided stories.

References

[1] "Grammar Undercuts Security Of Long Computer Passwords," *http://www.cmu.edu/news/stories/archives/2013/januaryjan24_passwords.html/*.

[2] A. Rao, B. Jha, and G. Kini, "Effect of grammar on security of long passwords," in *Proceedings of the third ACM conference on Data and application security and privacy*. ACM, 2013, pp. 317–324.

[3] S. Das, E. Hayashi, J. I. Hong, and I. Oakley, "Evaluating the use of autobiographical memory for authentication," *http://www.cs.cmu.edu/~jasonh/publications/SOUPS2012-memoryforauth-submitted.pdf*.

[4] A. Nosseir, R. Connor, and M. Dunlop, "Internet authentication based on personal history – a feasibility test," in *Proceedings of the Customer Focused Mobile Services Workshop*. ACM, 2005.