Life-Experience Passwords (LEPs)

Simon S. Woo
Computer Science Dept
Univ of Southern California
Los Angeles, CA, USA
simonwoo@usc.edu

Jelena Mirkovic
Information Sciences Institute
Univ of Southern California
Marina Del Rey, CA, USA
sunshine@isi.edu

Ron Artstein
Institute for Creative Technologies
Univ of Southern California
Playa Vista, CA, USA
artstein@ict.usc.edu

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

ABSTRACT

User-supplied textual passwords are extensively used today for user authentication. However, these passwords have serious deficiencies in the way they interact with humans' natural ability to form memories. Strong passwords that are hard to crack are also often hard for humans to remember, while memorable passwords are easily brute-forced or guessed. We propose a novel password design – *life-experience passwords* (LEPs). We explain how to use users' existing episodic memories about defining life events to create memorable and hard-to-guess passwords and discuss challenges involved in design and use of LEPs.

1. INTRODUCTION

User-supplied textual passwords are extensively used today for user authentication, both for personal devices and for remote servers. Such passwords usually consist of at least 8 characters, chosen from alphanumeric characters and special symbols. An ideal password would be hard for others to guess, whether they are strangers or close to the user, and easy for the user to remember. A user should ideally have a different password for each device/server a user access, to minimize the damage from password theft or guessing. However, current practice shows that user-supplied textual passwords fail to meet these requirements[3]. The main problem with current password approaches is that it forces a user to create new and complex memories that need to be accurately retrieved after long stretches of time.

We propose a novel password design – *life-experience passwords* (LEPs). Instead of requiring a user to form new memories, LEPs would be built from a user's episodic memories about past memorable, one-time events, such as weddings, births, graduations, vacations, etc. We specifically chose to base LEPs on events rather than user preferences (e.g., likes and dislikes), since memories of past events should be more stable than preferences. To ensure memorability we use only those experiences that occurred a number of years ago, and have thus already been memorable enough for a user to recall them at password generation.

LEPs consist of several *factoids* related to a user-chosen personal experience. The verification process prompts the user with questions about chosen factoids and the user's answers represents the password. Factoids are event details that a human is likely to recall with high consistency, such as time, location, people, conversations and activities. Given a user's life event such as a 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. Moreover details remembered by users attending the same event may differ, because different facts about that event were memorable to them. 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. In this short paper we compare our approach to existing approaches and outline challenges and our progress on addressing them.

2. CURRENT APPROACHES

Besides authentication methods based on textual passwords, graphical approaches, where a user draws a password, have been proposed to improve security and memorability. While graphical passwords appear easier to remember than textual ones, they still require users to form new memories about the precise order and the content of their drawing. Article [1] shows that many user-chosen graphical passwords have low entropy, and that gender and race influence the choice of a graphical password, increasing its guessability.

Cognitive or knowledge-based authentication approaches are similar to LEPs and base a password on personal facts,

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11, 2014, Menlo Park, CA.

interests, and opinions that are thought to be easily recalled by a user. But approaches that use interests and opinions suffer from inconsistent user recall, while approaches that use information about recent activities focus on those activities that can be captured by digital devices[2]. Our work aims to use memories about a greater diversity of events that happened at least a few years in the past, and that a user needs to aid to remember.

The ideas in LEPs are similar to current security questions used for secondary authentication, e.g. for password retrieval. However, LEPs differ from security questions, in two ways. First, security questions are chosen from a limited set, with many questions not being applicable to majority of users. We expect to produce more diverse passwords because our user input prompts are more open-ended. This will result in passwords that are more customized to each user, and thus more memorable and harder to guess by a stranger. Second, security questions contain one factoid about a chosen event and are thus easily guessed using public information about a user or using brute-force techniques. Our passwords will contain several factoids from episodic memories, which will make them harder to guess or to research using publicly available information about the user.

Article [4] presents an idea of using narratives for user authentication. However, narratives they use are generated using dialogues between human and computer, and requires users to associate imaginary objects with past memories (e.g., contents of a drawer from a childhood bedroom). Also, narratives can be fictional. In contrast, LEPs use user memories about events, and we believe that such details are more easily recalled by users and less easily guessed by strangers.

3. LIFE-EXPERIENCE PASSWORDS

We believe that LEPs provide the following benefits:

1. **Easy to remember** – a user is prompted about 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 different purposes.

We have identified the following list of topics for LEPs: (1) Milestone events, (2) Memorable events, (3) Trips, (4) Learning experiences, (5) First-time meeting an important person in one's life, (6) Flashbulb events, such as 9/11, etc. For each of these events, relevant factoids would speak about the details that a human is likely to recall with high consistency, such as time, location, people and activities. However, we specifically avoid use of feelings and preferences for factoids, as humans tend to remember this type of information inconsistently.

3.1 Implementation and Evaluation

The first step in our research is to investigate how LEPs compare to traditional passwords. To this end we have implemented LEP generation and verification, and obtained an IRB approval to conduct a user study to evaluate LEP memorability, guessability, and diversity. This study is publicly accessible at `http://steel.isi.edu/LEPstudy` and we welcome new volunteers. The study investigates two approaches to LEP generation:

1. *Prompted input*: a user is prompted by a series of questions to write about a chosen life event.
2. *Free-form input*: a user is prompted to write about a chosen event in natural language.

In both cases we plan to use NLP techniques to extract factoids from user input. We use the tool in [5] for question generation. Questions of type "who", "what", "where" and "when", and answers to them, are extracted from user input and stored in a database for future verification. Our study asks each user to return after one week, one month, and three months, and attempt authentication using LEPs. During authentication, the system prompts the user with stored questions and compares the answers to those stored in the database.

Use of natural language poses unique challenges to LEP generation and verification. First, humans use many terms to refer to the same fact in their mind. This introduces synonyms into the verification process that must be properly identified and handled. For example, Father, Dad, and John may all refer to the same person in a user's memory. Also, a user may recall only a portion of their original answer, e.g., they may claim they went to a party with Sally and Mary but provide only one of those names during verification. The second challenge lies in determining how much guidance is needed for users to provide quality input stories and to increase the usability, and reduce burden of LEP generation. The third challenge lies in identifying factoids that are easily mined from public sources or easily guessable and discouraging their use for LEPs. The fourth challenge lies in protecting the user from choosing potentially compromising factoids for their passwords, such as those based on illicit relationships or illegal activities. Our user study will provide initial data for us to evaluate the extent of these challenges and to design potential solutions.

4. REFERENCES

[1] D. Davis, F. Monrose, and M. K. Reiter. On user choice in graphical password schemes. In *USENIX Security Symposium*, volume 13, pages 11–11, 2004.

[2] 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.

[3] 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*, pages 317–324. ACM, 2013.

[4] A. Somayaji, D. Mould, and C. Brown. Towards narrative authentication: or, against boring authentication. In *Proceedings of the 2013 workshop on New security paradigms workshop*, pages 57–64. ACM, 2013.

[5] X. Yao, E. Tosch, G. Chen, E. Nouri, R. Artstein, A. Leuski, K. Sagae, and D. Traum. Creating conversational characters using question generation tools. *Dialogue & Discourse*, 3(2):125–146, 2012.