Life-Experience Passwords

Simon S. Woo
Computer Science Department
University of Southern California
Email: simonwoo@usc.edu

Elsi Kaiser
Linguistics Department
University of Southern California
Email: elsi.kaiser@usc.edu

Jelena Mirkovic
Computer Science Department
University of Southern California
Information Science Institute
Email: sunshine@isi.edu

Ron Artstein
Institute for Creative Technologies
University of Southern California
Email: artstein@ict.usc.edu

I. Life-Experience Passwords (LEPs)

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. 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.

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.

II. 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 life-experience passwords can best be generated. 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.