That's Not Me! Designing Fictitious Profiles to Answer Security Questions

Nicholas Micallef, Nalin Asanka Gamagedara Arachchilage

University of New South Wales, Australia and La Trobe University, Australia

Introduction

- Security questions still have several limitations though they are widely adopted.
- Previous research revealed that using system-generated information to answer security questions could be more secure than users' own answers.
- However, using system-generated information has usability limitations.
- To improve usability, no research has studied the elements that could influence the design of fictitious profiles or systems that use them to answer security questions.

Contribution

The main contribution of this work to the usable security field is a set of recommendations that would improve the design of systems that would generate fictitious profiles for answering security questions and systems that use security questions to recover passwords.
Therefore, we conducted an empirical investigation through 20 structured interviews to investigate the elements that could influence the design of fictitious profiles and systems that would use participants to answer security questions.

- Our main findings revealed that to improve the design of fictitious profiles, users should be given the option to configure the profiles to make them relatable, interesting and memorable.
- We also found that the security questions currently provided by websites would need to be enhanced to cater for fictitious profiles.

Methodology

- Conducted structured interviews with 20 participants
  - Females = 5
  - Males = 15
  - Mean age=30, (22-45) and Median=28
- Investigated how participants' feedback would affect the design of systems that generate fictitious profiles for security questions.
- We showed participants 2 fictitious profiles (see Figure 2) and explained that the details of these profiles would be used to answer security questions.
- Then, we asked questions to understand the elements that would affect the selection of a fictitious profile, the attributes that participants would prefer, the level of configurability and availability that a fictitious profile should have.
- Used the Constant Comparative Method (CCM) approach to identify themes.
  - The interviewer recorded the participants responses to the interview questions. These notes were later coded by two researchers independently. If there was a disagreement, a third researcher was asked to break the tie.

Fictitious Profiles Design

- We defined these fictitious profiles (see Figure 2).
- A male and female profiles were selected so that participants could be provided with the two most common genders.

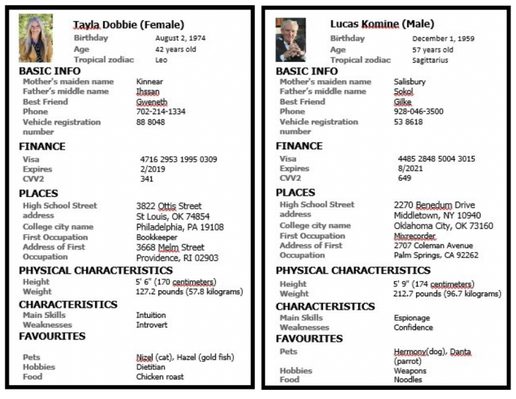
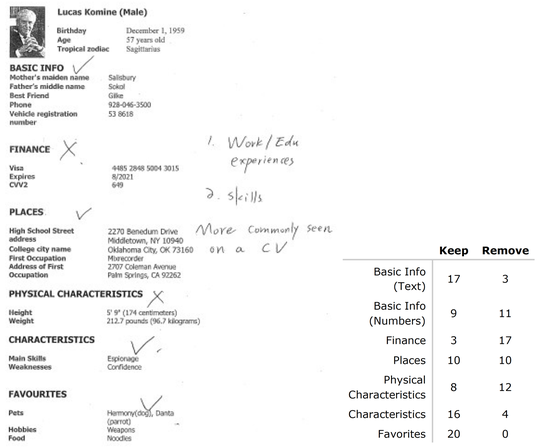


Figure 2: Fictitious profiles

Results

What elements that could influence the design of fictitious profiles and systems for participants to answer security questions (see Figure 1)?

- Relatability/connectedness
- Memorability
- Interesting attributes



	Keep	Remove
Basic Info (Text)	17	3
Basic Info (Numbers)	9	11
Finance	3	17
Places	10	10
Physical Characteristics	8	12
Characteristics	16	4
Favorites	20	0

Figure 1: Example of attributes marked by participants/Attributes selection

Discussion and Recommendations

- Improving the design of fictitious profiles - participants prefer fictitious profiles that are highly configurable, to make them relatable, interesting and memorable..
- Compatibility with current security questions - participants prefer security questions related to characteristics and favourites.
- System designers should invest a considerable amount of time and effort to implement stronger security measures (e.g. encryption and anonymization techniques) to protect these profiles.
- Improving potential adoption of fictitious profiles.

Further Research

- In our next studies, we will empirically evaluate whether the fictitious profiles designed in this research do actually improve the usability (mainly memorability) of system-generated information when answering security questions.
- Moreover, further research should be conducted to investigate the design of fictitious profiles for other application areas.
  - For example, to understand how users' would design fictitious profiles to anonymize and protect their privacy when registering to online accounts.

References

- Nicholas Micallef and Nalin Asanka Gamagedara Arachchilage. 2017. A Gamified Approach to Improve Users' Memorability of Fall-back Authentication. Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), USENIX Association.
- Nicholas Micallef and Mike Just. 2011. Using Avatars for Improved Authentication with Challenge Questions. SECURWARE 2011, The Fifth International Conference on Emerging Security Information, Systems and Technologies, 121-124.
- Arachchilage, Nalin Asanka Gamagedara, Steve Love, and Konstantin Beznosov. Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior 60 (2016): 185-197.

Contact Information

- Nicholas Micallef, Nalin A. G. Arachchilage

n.micallef@adfa.edu.au
n.arachchilage@latrobe.edu.au