Changing users' security behaviour towards security questions: A game based learning approach

Nicholas Micallef

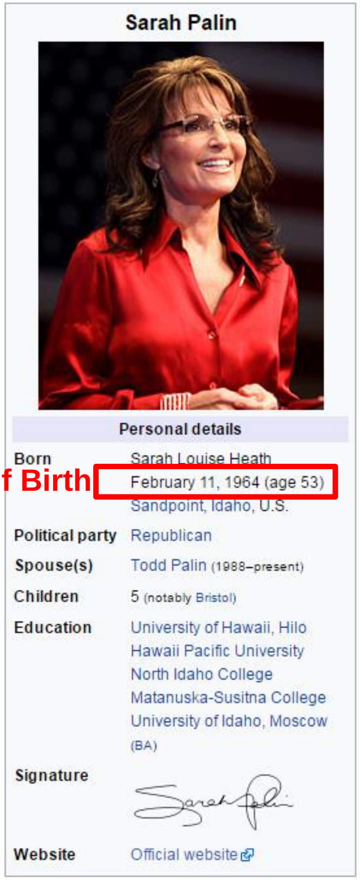
Nalin Asanka Gamagedara Arachchilage

Australian Centre for Cyber Security, School of Engineering and Information Technology,
University of New South Wales, Canberra, Australia

Bio

- Awarded PhD at Glasgow Caledonian University, UK (Topic: using ambient sensors in smartphone authentication).
- 1 year Postdoc at Heriot-Watt University, UK (focus: privacy nudges for mobile apps).
- Postdoctoral Fellow @ UNSW Canberra (focus: involving users in the design of novel fallback authentication mechanisms)
- Research interests: Usable Privacy & Security, Mobile HCI, Mobile Sensing & Mobile Health.

Introduction & Motivation (1)

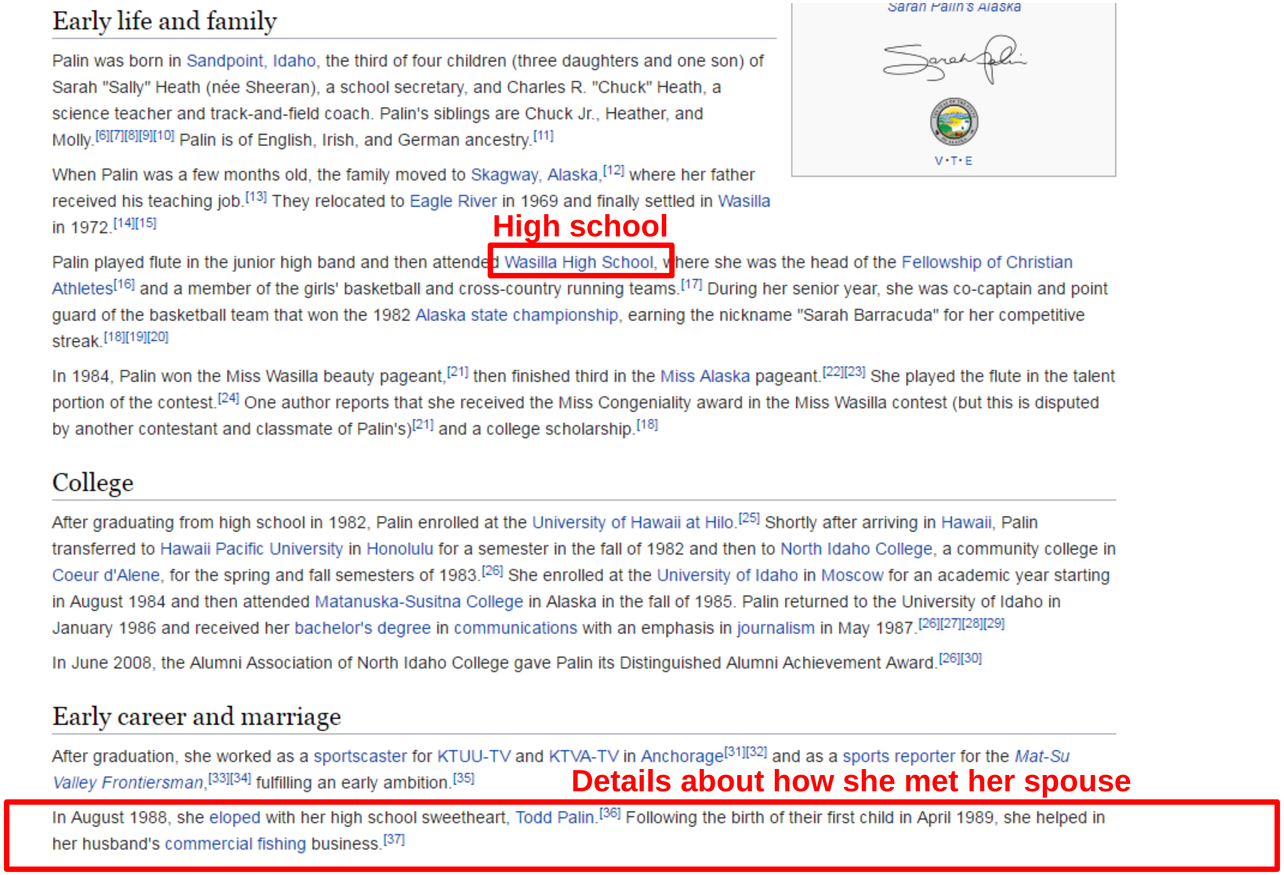


Sarah Palin

Personal details

Born	Sarah Louise Heath February 11, 1964 (age 53) Sandpoint, Idaho, U.S.
Political party	Republican
Spouse(s)	Todd Palin (1988–present)
Children	5 (notably Bristol)
Education	University of Hawaii, Hilo Hawaii Pacific University North Idaho College Matanuska-Susitna College University of Idaho, Moscow (BA)
Signature	Sarah Palin
Website	Official website

Date of Birth



Early life and family

Sarah Palin's Alaska

Sarah Palin

V·T·E

Palin was born in Sandpoint, Idaho, the third of four children (three daughters and one son) of Sarah "Sally" Heath (née Sheeran), a school secretary, and Charles R. "Chuck" Heath, a science teacher and track-and-field coach. Palin's siblings are Chuck Jr., Heather, and Molly.[6][7][8][9][10] Palin is of English, Irish, and German ancestry.[11]

When Palin was a few months old, the family moved to Skagway, Alaska,[12] where her father received his teaching job.[13] They relocated to Eagle River in 1969 and finally settled in Wasilla in 1972.[14][15]

High school

Palin played flute in the junior high band and then attended Wasilla High School, where she was the head of the Fellowship of Christian Athletes[16] and a member of the girls' basketball and cross-country running teams.[17] During her senior year, she was co-captain and point guard of the basketball team that won the 1982 Alaska state championship, earning the nickname "Sarah Barracuda" for her competitive streak.[18][19][20]

In 1984, Palin won the Miss Wasilla beauty pageant,[21] then finished third in the Miss Alaska pageant.[22][23] She played the flute in the talent portion of the contest.[24] One author reports that she received the Miss Congeniality award in the Miss Wasilla contest (but this is disputed by another contestant and classmate of Palin's)[21] and a college scholarship.[18]

College

After graduating from high school in 1982, Palin enrolled at the University of Hawaii at Hilo.[25] Shortly after arriving in Hawaii, Palin transferred to Hawaii Pacific University in Honolulu for a semester in the fall of 1982 and then to North Idaho College, a community college in Coeur d'Alene, for the spring and fall semesters of 1983.[26] She enrolled at the University of Idaho in Moscow for an academic year starting in August 1984 and then attended Matanuska-Susitna College in Alaska in the fall of 1985. Palin returned to the University of Idaho in January 1986 and received her bachelor's degree in communications with an emphasis in journalism in May 1987.[26][27][28][29]

In June 2008, the Alumni Association of North Idaho College gave Palin its Distinguished Alumni Achievement Award.[26][30]

Early career and marriage

After graduation, she worked as a sportscaster for KTUU-TV and KTVA-TV in Anchorage[31][32] and as a sports reporter for the *Mat-Su Valley Frontiersman*,[33][34] fulfilling an early ambition.[35]

Details about how she met her spouse

In August 1988, she eloped with her high school sweetheart, Todd Palin.[36] Following the birth of their first child in April 1989, she helped in her husband's commercial fishing business.[37]

Increased availability of personal info Online (social media or data breaches) → Increased vulnerability to cyber-attacks (e.g. ransomware)

Introduction & Motivation (2)

Embarrassment

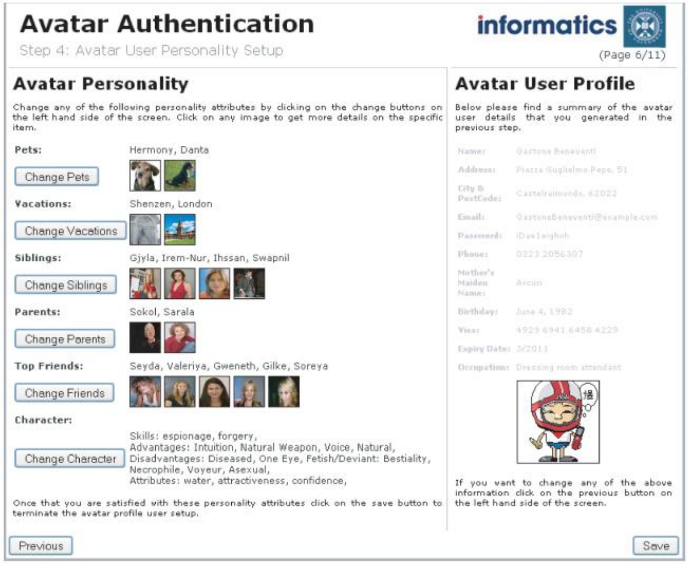
Effect reputation

Loss of money

Related work

Google

[1] security questions cannot be used as main mechanism to recover passwords.



Avatar Authentication

Step 4: Avatar User Personality Setup

informatics

(Page 6/11)

Avatar Personality

Change any of the following personality attributes by clicking on the change buttons on the left hand side of the screen. Click on any image to get more details on the specific item.

Pets: Hermony, Danta

Change Pets

Vacations: Shenzen, London

Change Vacations

Siblings: Gjyla, Irem-Nur, Ihssan, Swapnil

Change Siblings

Parents: Sokol, Sarala

Change Parents

Top Friends: Seyda, Valeriya, Gweneth, Gilke, Soreya

Change Friends

Character:

Change Character

Skills: espionage, forgery,
Advantages: Intuition, Natural Weapon, Voice, Natural,
Disadvantages: Diseased, One Eye, Fetish/Deviant: Bestiality, Necrophile, Voyeur, Asexual,
Attributes: water, attractiveness, confidence,

Once that you are satisfied with these personality attributes click on the save button to terminate the avatar profile user setup.

Avatar User Profile

Below please find a summary of the avatar user details that you generated in the previous step.

Name:	Gastone Beneventi
Address:	Piazza Guglielmo Pepe, 51
City & PostCode:	Castelraimondo, 62022
Email:	GastoneBeneventi@example.com
Password:	iDae1eighoh
Phone:	0323 2056307
Mother's Maiden Name:	Arcuri
Birthday:	June 4, 1982
Visa:	4929 6941 6458 4229
Expiry Date:	2/2011
Occupation:	Dressing room attendant

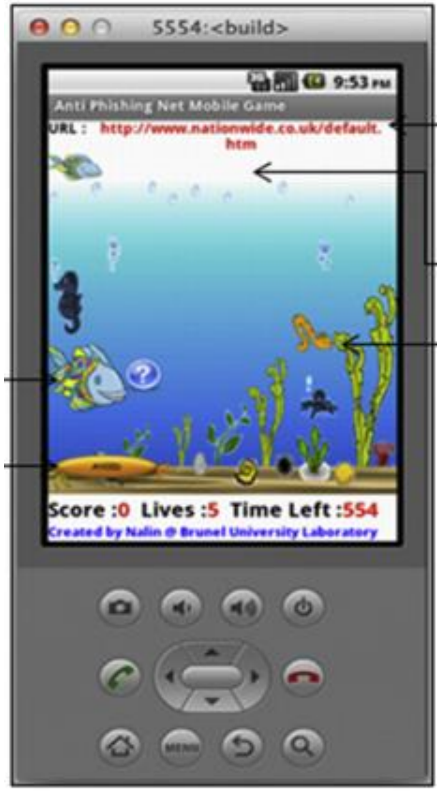
If you want to change any of the above information click on the previous button on the left hand side of the screen.

Previous

Save

[2] proposed an avatar profile - to represent system-generated data of a fictitious person

[3] [4] used autobiographical info of mobile phone usage of last few days


5554:<build>
9:53 PM
Anti Phishing Net Mobile Game
URL : http://www.nationwide.co.uk/default.htm
Score :0 Lives :5 Time Left :554
Created by Nalin @ Brunel University Laboratory
MENU

[5] successfully used gamified approach to change users' behaviour on susceptibility to phising attacks.

[1] Bonneau et al., (2015) Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In Proc. of WWW '15.
[2] Micallef and Just. 2011. Using avatars for improved authentication with challenge questions. In Proc. of SECURWARE 2011.
[3] Hang et al., 2015. I know what you did last week! do you?: Dynamic security questions for fallback authentication on smartphones. In Proc. of CHI 2015.
[4] Hang et al., 2015. Where have you been? using location-based security questions for fallback authentication. In Proc of SOUPS 2015.
[5] Arachchilage and Love. 2013. A game design framework for avoiding phishing attacks. Computers in Human Behavior, 29(3):706{714, 2013.

Contribution

Design of a serious game that enhance users' long-term memorability of answers to security questions by using:

1. Memorability concepts (e.g. graphical and verbal cues) and
2. Gamified approach (interactive, engaging nature of the game).

Memorability Concepts

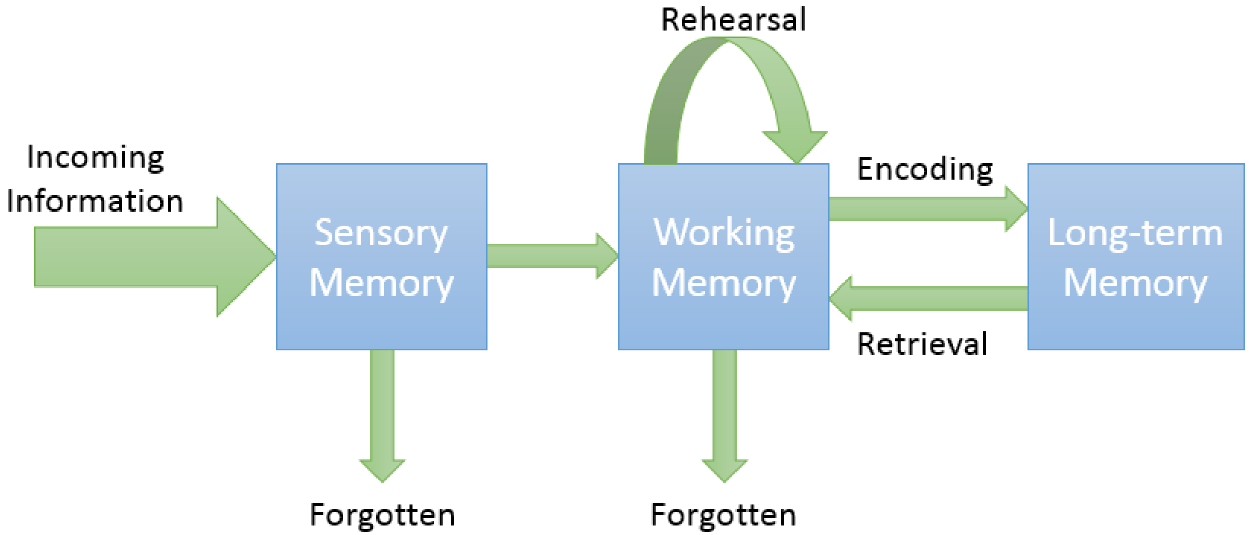


Figure 1: Atkinson and Shiffrin cognitive memory model [6]

- We use the picture superiority effect [7] since previous research which uses graphical authentication schemes [8][9][10][11] confirmed that humans are better at remembering images than textual information.

[6] Atkinson and Shiffrin. 1968. Human memory: A proposed system and its control processes. Psychology of learning and motivation, 2:89{195, 1968..

[7] Paivio et al. 1968. Why are pictures easier to recall than words? Psychonomic Science, 11(4):137{138, 1968.

[8] De Angeli et al. 2005. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies.

[9] Stobert and Biddle. 2013. Memory retrieval and graphical passwords. In Proc. of SOUPS 2013.

[10] Castelluccia et al. 2017. Towards implicit visual memory-based authentication. In Proc. of NDSS 2017.

[11] Denning et al. 2011. Exploring implicit memory for painless password recovery. In Proc. of CHI 2011.

Gamified approach

- Adapted “4 Pics 1 Word” [1] mobile game (see Figure 2).
- Selected this game due to use of pictures and cues which psychology research found to improve memorability.
- Game asks to pick word that relates the 4 given pictures.
- Adapted game to ask users to solve challenges related to system-generated data (answers of security questions).

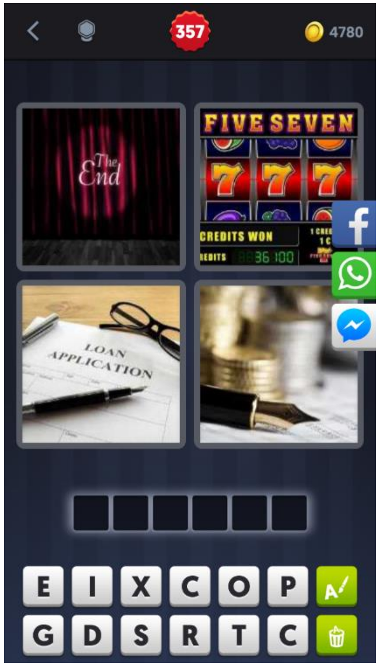


Figure 2: “4 Pics 1 Word” [1]

[1] https://play.google.com/store/apps/details?id=de.lotum.whatsinthefoto.us&hl=en

Game Design - Features (1)

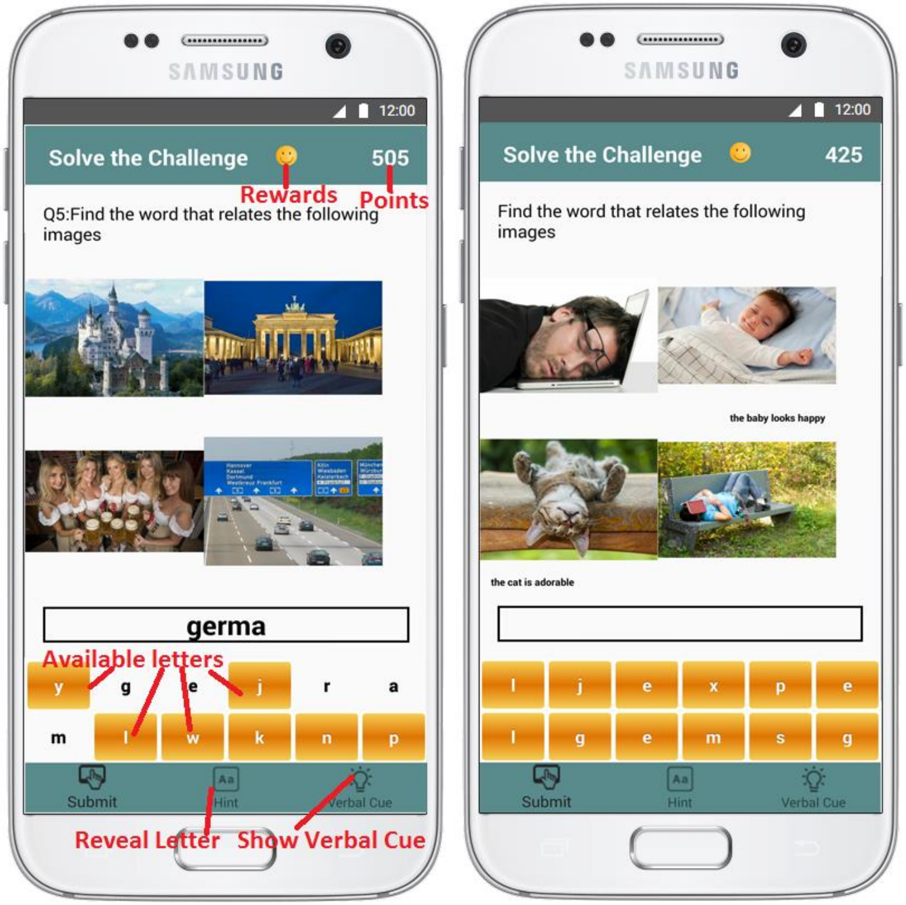
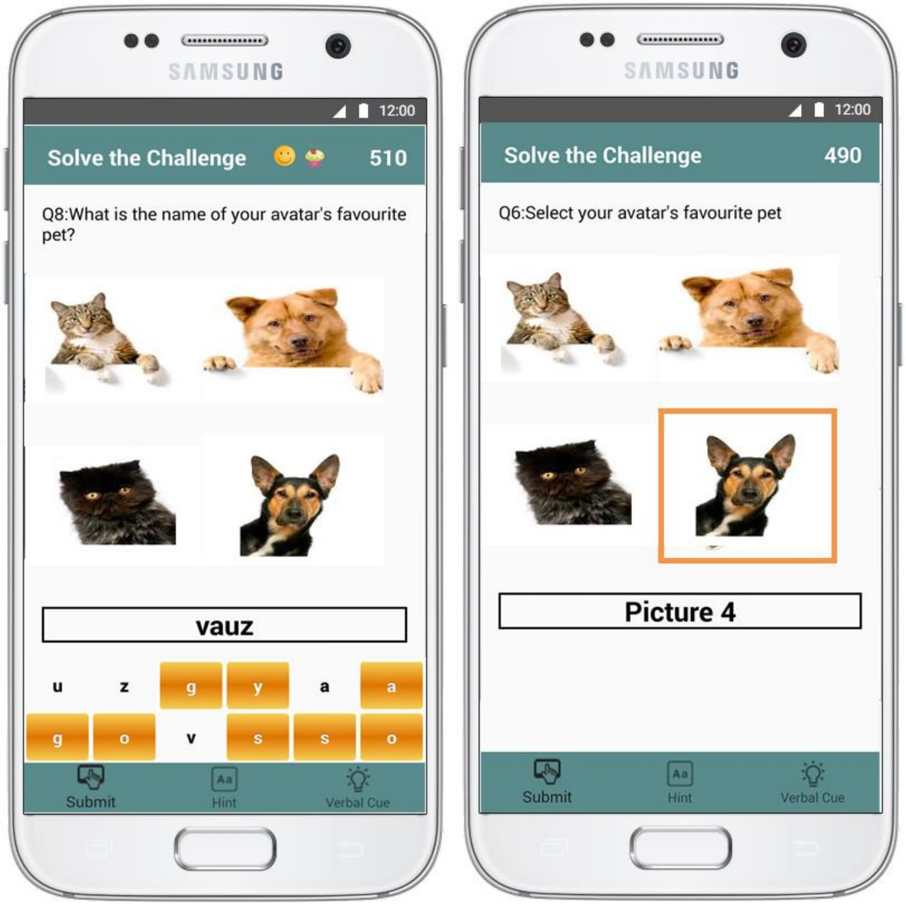


Figure 3: a) Standard Challenge, b) Standard Challenge with verbal cues

- 12 letters are provided to help the players solve the challenge.
- Points are awarded /deducted based on the type of challenge (10/15/20).
- Points could be used to obtain hints (30/50 points).
- Added feature to show verbal cues (see Figure 3b) to help memory.

Game Design - Features (2)

- At certain intervals players solve challenges related to system-generated information (see Figure 4a and 4b).
- System-generated information challenges are either recognition-based (see Figure 4b) or recall-based (see Figure 4a).
- Use of a fixed set of images and same images are always shown in the same order to help semantic priming.
- Does not show the length of the word (to improve security).



Q8:What is the name of your avatar's favourite pet?

vauz

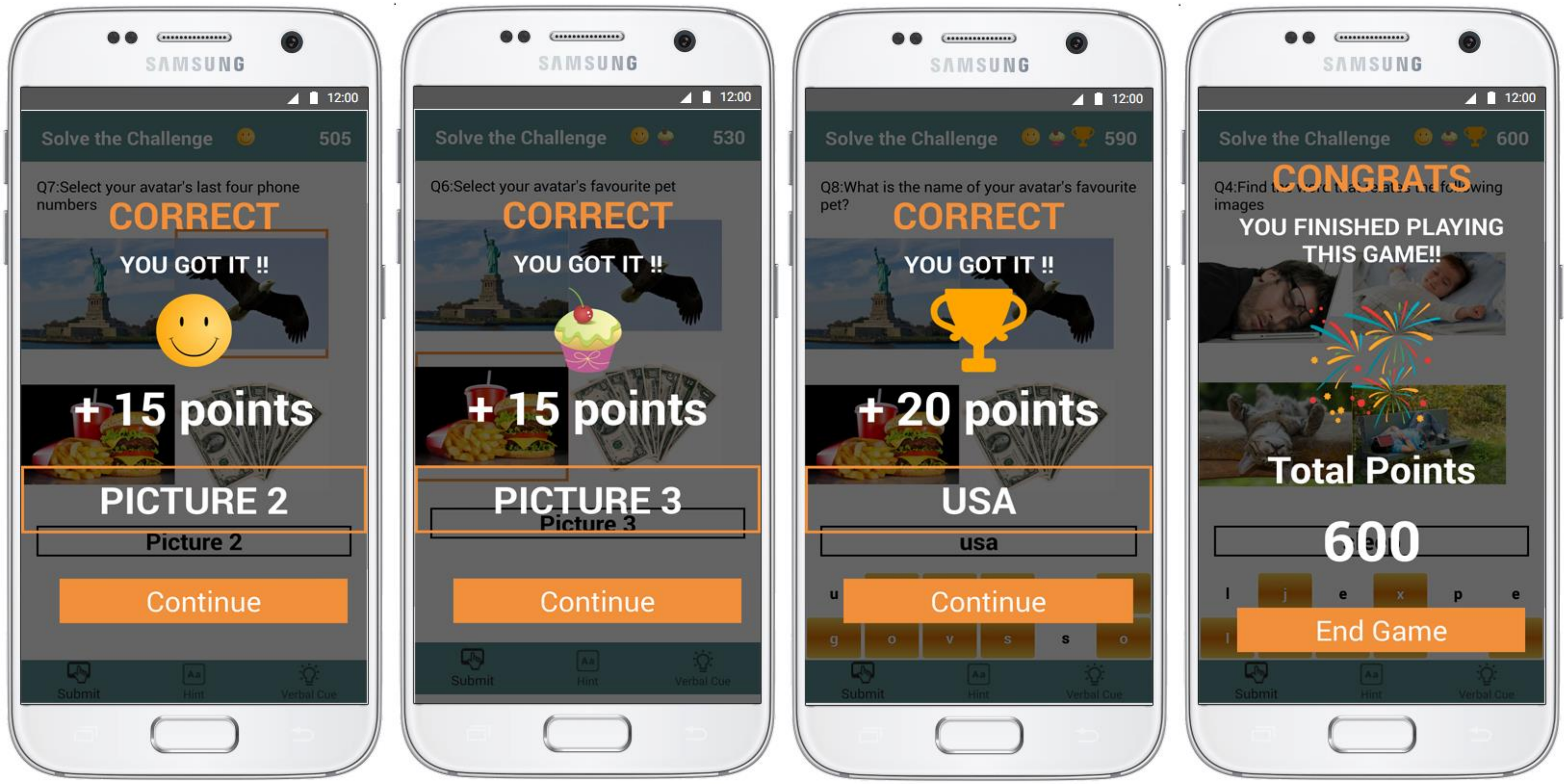
Q6:Select your avatar's favourite pet

Picture 4

Figure 4: a) recall security questions challenge, b) recognition security questions challenge

Game Design – Engagement

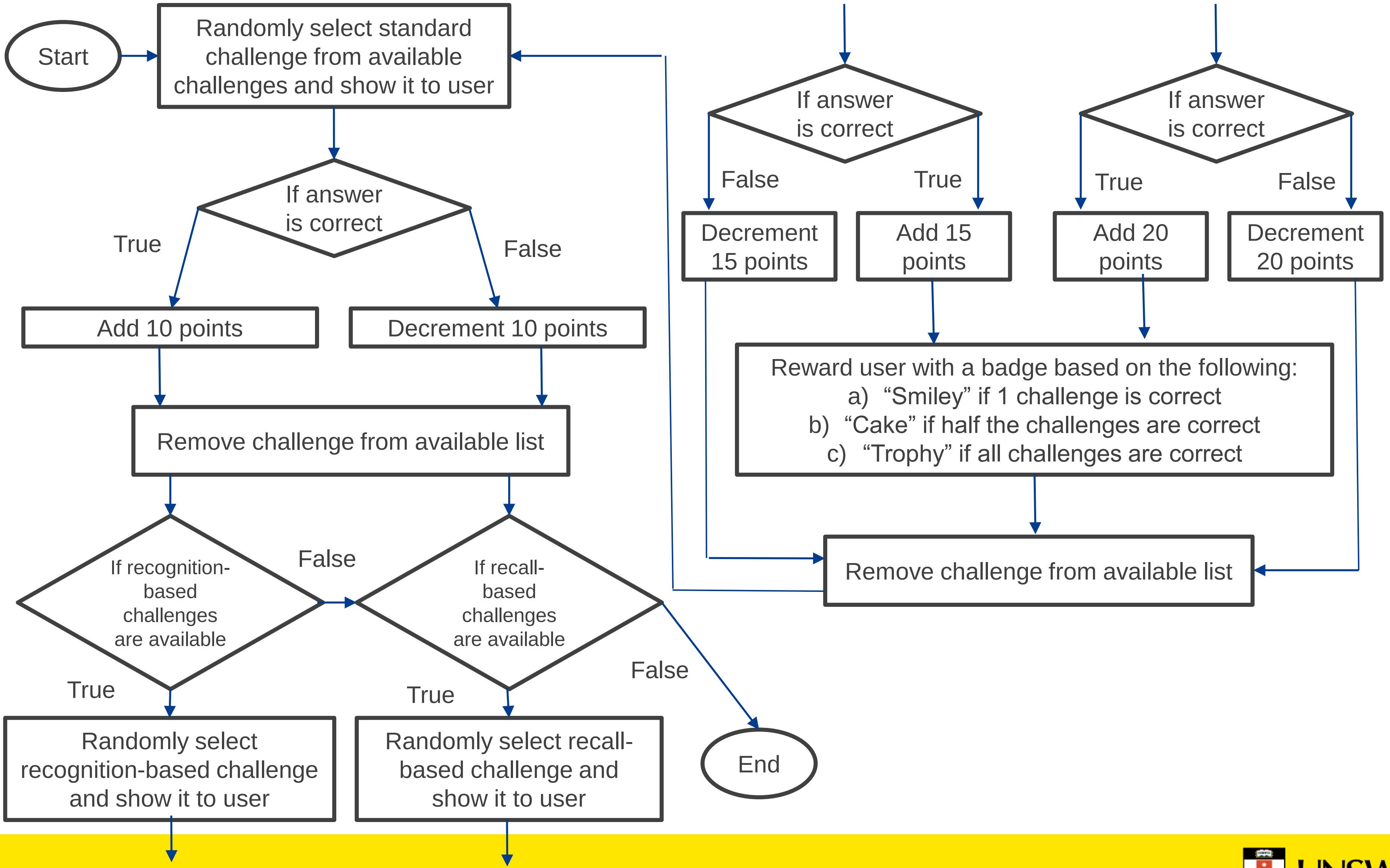
Persuasive technology principles [12]: Tunnelling, Conditioning, Suggestion, Self-monitoring, Surveillance and Social cues and Humour, Fun and Challenges.



a) "Smiley" badge reward   b) "Cake" badge reward   c) "Trophy" badge reward   d) end of game screen

[12] Fogg. 2002. Persuasive technology: using computers to change what we think and do. Ubiquity, 2002(December):5, 2002.

Proposed Game Logic


Start
Randomly select standard challenge from available challenges and show it to user
If answer is correct
True
False
Add 10 points
Decrement 10 points
Remove challenge from available list
If recognition-based challenges are available
False
If recall-based challenges are available
False
True
True
Randomly select recognition-based challenge and show it to user
Randomly select recall-based challenge and show it to user
End
If answer is correct
False
True
Decrement 15 points
Add 15 points
If answer is correct
True
False
Add 20 points
Decrement 20 points
Reward user with a badge based on the following:
a) "Smiley" if 1 challenge is correct
b) "Cake" if half the challenges are correct
c) "Trophy" if all challenges are correct
Remove challenge from available list

Future Work

- Lab study to involve users in the design of the game. (under review)
- Evaluate and address security vulnerabilities of the game. (work in progress)
- Conduct longitudinal field study to understand whether the proposed game design improves long-term memorability and investigate how much learning is required.

Conclusion

- Aims to nudge users to provide stronger answers to security questions.
- Aims to improve security by reducing vulnerability to observational and guessing attacks.
- Interacting/engaging nature of the game should help users to learn stronger answers to security questions through rehearsals.

Thank You

Questions?

Contact details:

Nicholas Micallef: n.micallef@adfa.edu.au

Nalin Asanka Gamagedara Arachchilage:

nalin.asanka@adfa.edu.au