An experimental analysis: The effects of security controls on human behavior in online social media*

Nelson Novaes Neto
Pontifical Catholic University of São Paulo
Brazil
nnovaes@psyzone.org

Sergio Vasconcelos de Luna
Pontifical Catholic University of São Paulo
Brazil
svluna@uol.com.br

ABSTRACT

In the context of behavioral analysis, online security control mechanisms can be classified as an aversive stimulus that is part of the contingencies that control the behavior of Internet users. The prior presentation of an aversive stimulus may decrease the likelihood of an user emitting a response or have other behavioral effects that can affect the user, the online community and/or the services of online social media. Taking the viewpoint of an experimental analysis of behavior as reference, this paper demonstrates empirically how the manipulation of a security control in the behavior contingencies of an online social chat service can considerably affect the behavior pattern of users in a social setting. The results may contribute to understand of the effects of aversive stimuli on the Internet and to assist in studies aiming to develop architectures that preserve the usability and security of online systems. The trend towards using this type of environment is growing considerably and, in general terms, we believe that this study may contribute to the science of behavior analysis and the development of security controls that necessarily involve the understanding of human behavior to perceive, understand and act upon the risks and threats involved in these environments.

Categories and Subject Descriptors

H.1.2 [**Models and Principles**]: User/Machine systems—*systems–human factors, human information processing*; K.4.1 [**Computers and Society**]: Public Policy Issues—*human safety*; K.6.5 [**Management of Computing and Information Systems**]: Security and protection

General Terms

Experimentation, Human Factors, Security

*This research was sponsored by UOL (www.uol.com.br)

Keywords

Behavior Analysis, Online Social Networks, Security Controls

1. INTRODUCTION

With the technological advances of recent years, the Internet hit the mark back in 2012 of more than 2.4 billion[1] people connected through computers, smart phones[2] or tablets. Once connected to the Internet, users are increasingly accessing social network sites (SNSs) to exchange information in real time, producing numerous social episodes[13].

It should be made clear that online interactions affect users' lives in the "real world" – interactions established through the Internet can go on to control people's behavior in different ways. For example, a social network provider can provide users with certain stimuli, such as displaying images and news that can have a reinforcing function for them, and making them more likely to access their pages in the future; the users themselves, in turn, can provide social reinforcers for other users of the service. If the contingencies are reinforcing for both users, the exchange is maintained and may produce new behaviors that would not be available if not for interaction within social networks.

The great mass of online users fosters consequences that easily exceed the total of the consequences that could be produced if the members acted separately, disconnected from each other. By joining a group, the individual increases his or her ability to get reinforcement[14]. It can be considered that the overall reinforcing effect is greatly increased and millions of cases provided by online social media create the opportunity for obtaining social reinforcers at a low response cost and the group effects also sustain a huge trend for users to behave. For SNS services, there is a notable preference for choosing services that have the greater number of users who are registered and make use of the service, indicating a greater availability of access to reinforcers.

Internet use has become as commonplace as having a conversation or reading a magazine. Understanding the variables that affect the behavior of Internet users, and the reinforcement contingencies that keep them making use of this tool, can provide an advantage when it comes to the prediction and control of human behavior, including issues concerning the proper and effective development of new tech-

[1]http://mashable.com/2013/01/17/the-internet-in-2012-634-million-websites-2-4-billion-users-1-3-trillion-google-searches/
[2]http://edition.cnn.com/2013/01/30/tech/social-media/facebook-mobile-users

nologies that provide benefits to academia, science, society and business. Behavior analysis is a science that seeks to identify these variables.

One of the issues in Internet use concerns security. Attacks on users and/or online services are increasing and changing in line with changes and trends in the virtual scene and the market. The aim of an attack or fraud may be to damage the online service, organizations, government or users, among others. For example, due to the large number of Facebook users – more than 1 billion active accounts[3] – this service has become a target of several attacks[4] and constant discoveries of vulnerabilities[5] that could undermine the privacy and security of users[6, 9, 16, 10]. According to the Brazilian Federation of Banks, electronic fraud, including Internet banking scams among other things, cost the banks about US$ 703 million in 2012. A large figure, although less than 0.007% of all transactions in Brazil[6]. This statistical increase is directly reflected in the damages to security controls and the need for investments in new ones on the part of the SNS and online service providers in order to minimize the likelihood that users and their services are targets for fraud.

With the development and growth in the use and benefits obtained from the Internet, the online scene is increasingly the target of criminal practices that can affect the security of users and/or online services. Studies on human behavior while using the Internet may allow better understanding of the contingencies that control inappropriate behavior in relation to security and promote the appropriate development of controls for online environments.

For example, it is possible to study the effects of punishment that is currently imposed on users who have flouted the rules of use or security policy of a SNS, or to control the response cost of users who are dependent[7] on Internet access.

Regardless of how much investments in security controls increase, with the evolution of attacks, a particular control may become ineffective by not supporting a change that has occurred in the modus operandi of a fraudulent technique, i.e., the security control will no longer be effective against the new fraudulent technique and the online service provider will have to tailor new controls to minimize the likelihood of future fraud. For example, some years ago, online chat services had no CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)[1], security control illustrated in Figure 1, for access to the chat room .

No matter how much more efficient these security controls may be, requiring such user responses can undermine accessibility to an environment, increasing the response cost for a user who wants to access an online service.

2. RELATED WORK

[3]http://mashable.com/2012/10/04/facebook-one-billion/
[4]http://arstechnica.com/tech-policy/news/2011/11/researcher-shows-how-to-friend-anyone-on-facebook-within-24-hours.ars
[5]http://thehackernews.com/2011/10/how-facebook-ticker-exposing-your.html
[6]http://blogs.wsj.com/digits/2013/01/30/cyber-criminals-exploit-brazil-nightclub-tragedy/
[7]http://www.forbes.com/sites/alicegwalton/2012/10/02/the-new-mental-health-disorder-internet-addiction/

Figure 1: Wikipedia captcha example.

CAPTCHA is a type of human interactive test that minimizes the likelihood of automated systems, such as robots, gaining access to certain online services. With a considerable increase in fraudulent messaging managed by automated systems, many online services now use it. Currently, CAPTCHA is penetrating hundreds of online services, whether they may be commercial or not, including Google[8], UOL[9] and Yahoo[10], which use this control in an attempt to block automated interactions with their websites. Each organization may have a different type of coding[15] and displaying tests, such as text, sound, image[5], videos[7] or a combination of these.

According to the vulnerability[11] published by MITRE[12], CAPTCHA undermines the accessibility and usability[4] of users and goes against the principle of Psychological Acceptability[12], according to which it is essential that the interfaces between users and systems are designed so that security controls are applied automatically and transparently, because errors are minimized when the perception of the security needs of a user match the security controls provided by the systems. Around 200 million CAPTCHAs are solved by humans worldwide each day, and it takes around 10 seconds to answer each test, which corresponds to little more than 150,000 hours per day used to reply to CAPTCHA[13] tests.

The development and use of a CAPTCHA that is robust and without security vulnerabilities[2], and that has the lowest likelihood of an automated system successfully answering the test, should follow a systemic analysis and a proper balancing of security and other criteria that may undermine the accessibility of a user to a service. For example, using a CAPTCHA in the form of a distorted image with random characters and a very high level of background noise can increase the difficulty for automated systems to answer the test, but it is likely that users will have difficulty discriminating this stimulus, resulting in an increased likelihood of error in the test and hindering user access to the environment (room).

From the perspective of behavior analysis, the use of a CAPTCHA can be classified as an aversive condition which is part of the contingency of access to the chat room by an user. The presentation of a prior aversive stimulus may decrease the likelihood of a user issuing a response or can have other behavioral effects that can affect the user, the online community and/or service provider. Data from the literature of behavior analysis[8] indicates that the change-

[8]http://www.google.com
[9]http://www.uol.com.br
[10]http://www.yahoo.com
[11]http://cwe.mitre.org/data/definitions/655.html
[12]http://www.mitre.org
[13]http://recaptcha.net/learnmore.html

over-behavior (preference/alternation) is also controlled by the cost of response change and the reinforcers available.

The aim of this paper is to analyze the negative effects that security controls can exert on users' online behavior when controls are deliberately inserted into the contingencies for the use of online services. Among the many problems faced to study this effect, consideration was given to the convenience of taking the CAPTCHA as an independent variable (IV) that can be manipulated to assess the effects of this stimulus on room-change behavior for users of an online social chat service. Our findings may contribute to understand the effects of aversive stimuli on the Internet, minimize the vulnerability of the failure to satisfy Psychological Acceptability and assist in studies for the development of architectures that preserve the usability and security of systems.

3. METHOD

3.1 Enviroment

The online service used in this study was chat. Chat is a real-time application that allows users connected to the Internet to access a chat room – classified by theme, age, city, gender, religion, among other things – to exchange interactive and multimedia messages with other users who are connected to this service. The online social chat service used in this study[14] has more than 7500 online chat rooms, where more than 375 thousand people can talk at the same time.

3.2 Participants

This study included a selection of 700 chat service participants and (authenticated) subscribers to an ISP, split into four groups according to behavior patterns and the stability criterion.

3.3 Procedure for recording accesses to the room and recording variables

The chat system records all logins and logouts of a service participant. This set of records is called an "access log" (logs), which is used to describe the process of registering relevant events and variables that involve the interactions of participants, service and systems, such as: screen name, date and time, IP address, name and code of the room and subscriber ID. The authentication process involves the validation of the digital identity of the subscriber, checking that the subscriber name and password provided by the participant match the provider's records, given that the password is exclusive to the subscriber. All actions of a participant in the chat service are recorded automatically with the inclusion of a new line in the log file, each line representing a certain action and having the value of variables that are registered by the service.

3.4 Privacy criteria for the variables in the log file

As a premise of confidentiality and privacy for this study, all records provided by the service provider were protected. A security process[3] for protecting the variables contained in the log file was set up before even receiving the data for performing this study, thus making it impossible to discover the identity of a participant who uses the chat service. The manipulation of the CAPTCHA independent variable did not represent any change in security and privacy policy of the online chat service provider and rights of participants in the service.

[14]http://batepapo.uol.com.br

Table 1: Product of forming the groups by correlation between the median split for the operation and time variables.

Grouph	Description
1	Operations: below median Time: below median
2	Operations: below median Time: above median
3	Operations: above median Time: below median
4	Operations: above median Time: above median

3.5 Stability criteria and procedure for selecting participants

First, the behavior pattern of a group of 12,841 users who met the criteria was analyzed – under the effect of natural conditions of access to the environment (presence of the CAPTCHA variable). The variables used to determine the selection of participants were:

a) Number of days of Internet access (> 40 days);

b) Total number of operations for each participant;

c) Total session time (permanence in a room) for the number of days for a participant.

The selected users were split into groups with similar profiles in terms of the three selected variables. A multivariate hierarchical classification technique was used to construct typologies (clusters). Four groups were formed, as will be seen in the results section, Table 1.

The stability criterion was determined by the behavior pattern of each group, represented by the minimum, maximum, mean and standard deviation for the three variables used in the design.

3.6 Control group and test group

For the control group, seven participants were selected from each of the four groups, making a total of 28 participants. The test group corresponded to a participant registered by the researcher who had a subscription with the provider. This participant was used for a daily validation of the integrity of logs and to identify any anomalies that could affect the results of this research. The test consisted of the daily access of the participant to a randomly chosen room of the chat service with a stay of 10 minutes. This log was used as a control to assess whether the entry and departure operations, presence or absence of the independent variable, and length of stay were intact.

3.7 Experimental Procedure

Three experimental phases were designed to assess the influence that the manipulation of the CAPTCHA (independent variable) could have on the behavior of access (entry) to the rooms of a chat service by participants.

- **Phase 1**: Baseline – all participants who came to the chat service during 13 days;
- **Phase 2**: Removal of the CAPTCHA stimulus for participants for 15 days;
- **Phase 3**: Reintroduction of the CAPTCHA stimulus for participants for 15 days;

The procedure for changing the experimental phase was carried out when a stable behavioral pattern was reached (analyzed during data collection).

4. RESULTS

The aim of this research was to analyze whether the manipulation of the CAPTCHA stimulus in Phases 2 and 3 would establish some effect on room access behavior, evaluated by the following measurements:

a) number of room accesses for each participant (access to a room), called Operations (Operations Variable);

b) time spent in a room per day for each participant, called Time (Time Variable).

The study hypothesis of the research was based on the common opinion in the online environment that the need to answer the CAPTCHA test for each access to rooms on the chat service is considered a nuisance. Starting from this premise, the hypothesis was that, for most participants, removing the CAPTCHA would increase the likelihood of changing rooms by removing the nuisance. According to the procedure described in Method, the 700 participants were split into four groups using the medians of operations and time as the criteria for the division, as shown in Table 1.

The participants in the four groups were split to assess whether their behavior pattern had been influenced by the experimental variable, i.e., a check was made of whether a participant assigned to a particular group in Phase 1 changed groups in Phases 2 and 3. For example, a group of 10 participants was classified in Group 1 in Phase 1 (Time and Operations below the median), but when subjected to Phase 2, some of the users in this group demonstrated behavior corresponding to Group 3 (operations above the median and time below the median).

If CAPTCHA had aversive properties and these were controlling the behavior the participants, the results presented in Phase 2 would show the migration of a larger number of participants from Groups 1, 2 and 4 to Group 3 (Operations above the median and Time below the median) and in Phase 3, a migration of a larger number of participants to Groups 2 and 1, respectively.

Table 2 shows the results of splitting the 700 participants into the four groups and the number of participants who migrated to other groups between the experimental stages. The first column shows the number of participants in each group in Phase 1 and the second column (Change to Phase 2) indicates how many participants migrated from each group to one of the four groups between Phase 1 and Phase 2. For example, of the 281 participants in Group 1 in Phase 1, 65 migrated to Group 3 when submitted to Phase 2.

Figure 2 shows the number of participants in each group for each phase.

In Table 2 and in Figure 2, in Phase 1, Group 1 had the largest number of participants (281), followed by Group 4

Table 2: Participants split into four homogeneous groups with regard to the median for the variables of "number of operations" and "time", and the number of participants who moved from one group to another in each experimental phase.

Phase 1: Change to Phase 2			**Phase 2: Change to Phase 3**			**Phase 3:**
Group 1	Group 1	216	**Group 1**	Group 1	230	**Group 1**
n= 281	Group 2	0	**n=352**	Group 2	38	**n=291**
	Group 3	65		Group 3	19	
	Group 4	0		Group 4	65	
Group 2	Group 1	46	**Group 2**	Group 1	0	**Group 2**
n=72	Group 2	0	**n=0**	Group 2	0	**n=60**
	Group 3	25		Group 3	0	
	Group 4	1		Group 4	0	
Group 3	Group 1	18	**Group 3**	Group 1	61	**Group 3**
n=69	Group 2	0	**n=326**	Group 2	22	**n=58**
	Group 3	51		Group 3	39	
	Group 4	0		Group 4	204	
Group 4	Group 1	72	**Group 4**	Group 1	0	**Group 4**
n=278	Group 2	0	**n=22**	Group 2	0	**n=291**
	Group 3	185		Group 3	0	
	Group 4	21		Group 4	22	

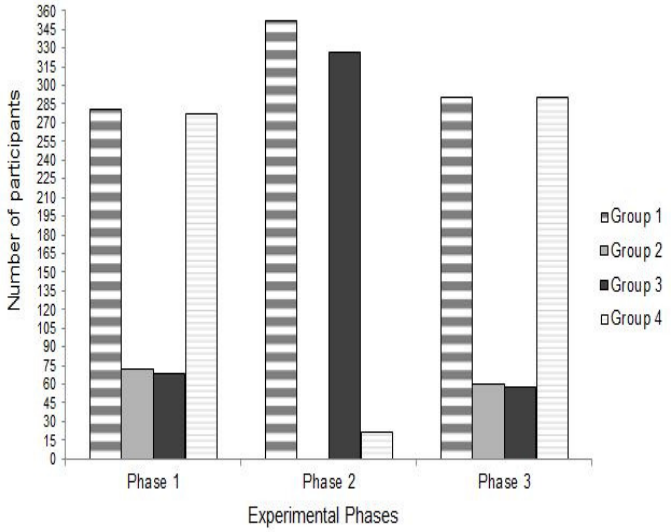

Figure 2: Number of participants in the groups for each experimental phase.

(278 participants). Having analyzed the migration of participants between Phases 1 and 2, four observations can be made:

1. first, it is noted that Group 1 underwent little change;
2. in Phase 2, Group 2 no longer exists – the participants in this group migrated mainly to Group 1, but there was also migration to Group 3;
3. Group 3 received the largest number of participants in Phase 2 (intervention by removing the CAPTCHA independent variable), being the second largest group in Phase 2, with an increase of 257 participants;
4. Group 4 changed to only 22 participants, with a decrease of 256 participants in Phase 2 – its participants mostly migrating to Group 3.

In the migrations of participants from the Phase 2 to the Phase 3 the four groups returned to values close to those in Phase 1, i.e., the change in the number of participants for Groups 2, 3 and 4 suggests that participants in these groups were influenced by the effects of the independent variable, corresponding to expectations. The analysis is not conclusive for Group 1.

4.1 Analysis of Friedman and t-test statistical tests

The aim of this analysis was to check statistically whether the differences between the magnitudes of the measurements taken so far could be considered statistically significant, thus demonstrating that the participants had been influenced by the manipulation of the independent variable in Phases 2 and 3.

The nonparametric *Friedman* test for three dependent samples (same participants) and the t-test were used to check whether the changes were significant. The aim of the Friedman test was to identify if there had been significant changes to operations and time in the comparison between phases; the *t-test* was intended to check if it was possible to demonstrate a significant change for the individual differences of each participant between phases.

Table 3: *Friedman* test result for the three experimental phases.

	X^2	*p*
Mean Operations	32,376	0,000
Mean Time	10,289	0,006

Table 3 shows significance in the difference between the means of operations and time for the participants between the three phases. The X^2 value represents the test result: the larger this value, the greater the difference of the change in this comparison. The p value represents the significance level: values less than 0.05 indicate a significance that reasonably supports the validation of changes between phases, i.e., the difference between the comparison between phases was significant.

With the validation of differences between phases, the *t-test* was used to assess whether it was possible to demonstrate a significant change in the individual differences of each participant between phases.

Table 4 shows the result of the *t-test*. Comparisons that showed $p<0.05$ (numbers in red) had a significant change. The first column in Table 4 shows the variable name and the name of the comparison between the phases for the variable[15].

Table 4: Results of the statistical *t-test* for comparing differences between variables between the phases.

	t	*df*	*p*	Mean Difference
Mean Operations: Phase 1 - Phase 2	-0,9857	699	0,162	-0,26
Mean Time: Phase 1 - Phase 2	-1,2356	699	0,109	-2470,02
Mean Operations: Phase 2 - Phase 3	4,89188	699	0	1,25
Mean Time: Phase 2 - Phase 3	4,1443	699	0	11298,17
Mean Operations: Phase 1 - Phase 3	4,01592	699	0	0,99
Mean Time: Phase 1 - Phase 3	3,13252	699	0,001	8828,15

For example, the first line shows the variable Mean Operations for the comparison between Phase 1 and Phase 2. The t value shows the difference between Phase 1 and Phase 2; negative values indicate an increase in the number of operations in Phase 2. The larger this value, the greater the difference. The value of df indicates the number of participants analyzed; p indicates the significance level; and finally the Mean Difference is shown. The results with $p<0.05$, in red, show that there were significant changes when comparing the measurements for the participants between the two phases.

The results for the measurements between Phase 1 and Phase 2 show that the mean values were increased when participants were subjected to Phase 2; however, statistically, this increase was not significant for the group of 699 participants. This shows that the removal of the CAPTCHA variable produced an increase in the measurement of operations for some participants, but this effect was not sufficient to statistically prove the study hypothesis for the group of 699 participants. The increase in the time measurement also did not confirm the hypothesis of a decrease in the time measurement when the independent variable was removed.

Comparing Phase 2 and Phase 3, the results revealed a significant change for both measurements, indicating a confirmation of the hypothesis that the reintroduction of the CAPTCHA independent variable in Phase 3 significantly changed the room-accessing behavior of the participants. The time measurement also showed a decrease when compared to Phase 3, indicating that the mean session time did not match the study hypothesis of an increase in the mean session time in Phase 3.

Comparing Phase 3 and Phase 1, it was possible to iden-

[15]For the construction of the clusters, one participant with (40 ID) was removed because he showed a very high number of operations and time as compared to other participants for all stages. This procedure was necessary to avoid hindering the division of participants into three clusters, because the ID 40 produced an isolated cluster.

tify a significant change in all dependent-variable measurements. This change shows that when participants underwent Phase 3 – reintroduction of CAPTCHA – the values of the operations and time measurements of this phase showed a significant decrease relative to the baseline values (Phase 1). This proves that the reintroduction of the CAPTCHA variable exerted an effect on access and retention in the chat service rooms.

The conclusion of the statistical tests indicated that there was a change in the behavior pattern of the participants when undergoing Phase 2 and Phase 3, for the operations and time measurements changed significantly with the reintroduction of the CAPTCHA independent variable in Phase 3.

5. DISCUSSION

One of the main aims of this research was to present a proposal for experimental procedure to assess whether the room-change behavior for participants in an online social chat service can be changed by the inclusion or removal of a stimulus (CAPTCHA) in the chat environment. Multidisciplinary resources were used to conduct the study, including, for example, the sciences of behavior analysis, computer engineering and statistics, and law. This study also showed the ethical issues and the care with security and privacy, which are key requirements for the Internet to be able to be used as a laboratory or clinical environment. Particularly noteworthy are the results directly related the use of the online chat environment to assess whether the room-change behavior for participants in an online social chat service can be changed by the inclusion or removal of a stimulus (CAPTCHA) in the environment.

In summary, the results indicated that the behavior pattern for room entry by participants was influenced by the effect of manipulating the CAPTCHA variable. However, the results were not adequately significant to prove the hypothesis that the removal of CAPTCHA would increase the probability of changing rooms by eliminating the need to answer the test. The measurements of entry behavior, number of accesses to rooms and permanence time in the rooms were significantly modified only when the CAPTCHA variable was reintroduced (Phase 3) to participants after a period of 15 days without the IV (Phase 2).

In general, the expectations for changes in numbers of room-accessing operations were met, but these changes were only statistically significant in Phase 3. This result demonstrates that when the CAPTCHA variable ceases to be part of the contingency for accessing rooms, for the majority of participants the room-change behavior is not influenced significantly by manipulating the IV. However, when the CAPTCHA variable was reintroduced into the access contingency, restoring a component in the room-accessing chain of events, participants' behavior was influenced significantly, showing that the process of reintroducing the IV, Phase 3, presented partially aversive properties.

On the other hand, it is important to note that this study did not assess the influence of competing reinforcers in the environment that could alter the likelihood of a change in room-change behavior. Therefore, considering that the core of a chat service is to provide an opportunity to have access to social reinforcers for its users with a low response cost, the conclusion is that the simple room-change behavior can be directly influenced by aspects that control it, such as the presence of competing reinforcers within or outside a room.

6. CONCLUSION AND FINAL CONSIDERATIONS

This research presented a study to demonstrate the possibility of using the Internet as an experimental laboratory for the study of behavior. This research also helped to answer some of the seven necessities and implications for online interventions for psychology[11].

The results of this research indicate the opportunity for conducting further research into understanding human behavior on the Internet and highlight the need to invest in the study and improvement of the basic procedures presented here, and also have support from computer science, statistics and engineering for the use of appropriate techniques that could deepen the analysis of online behavior. Thus, it is essential, however, that further studies to investigate the contingencies that are part of the Internet with the greatest possible experimental control, and this research may be useful for this purpose.

In summary, it is important to emphasize that, when conducting future studies that use the Internet as an experimental laboratory, it must be ensured, as mandatory principle, that the research information is protected with strict confidentiality criteria that meet current legislation, ethical codes and privacy contracts determined by online service providers.

7. ACKNOWLEDGMENTS

The authors would like to thank UOL and its staff for their support in providing online environments, servers, data and development. The authors thank all PEXP PUC-SP's researchers and professors who were involved in this research, and also Natalia Mesquita, Yara Castro, Denis Zamignani, Roberto Banaco and Alexandre Biancalana, who collaborated with their multidisciplinary skills.

8. REFERENCES

[1] R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2008.

[2] E. Bursztein, M. Martin, and J. Mitchell. Text-based captcha strengths and weaknesses. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 125–138, 2011.

[3] V. T. Chakaravarthy, H. Gupta, P. Roy, and M. K. Mohania. Efficient techniques for document sanitization. In *Proceedings of the 17th ACM conference on Information and knowledge management*, pages 843–852, 2008.

[4] L. Cranor and S. Garfinkel. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly Media, 2008.

[5] R. Gossweiler, M. Kamvar, and S. Baluja. What's up captcha?: a captcha based on image orientation. In *Proceedings of the 18th international conference on World wide web*, pages 841–850, 2009.

[6] J. He, W. W. Chu, and Z. (victor Liu). Inferring privacy information from social networks. In *IEEE International Conference on Intelligence and Security Informatics*, 2006.

[7] K. A. Kluever and R. Zanibbi. Balancing usability and security in a video captcha. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 14:1–14:11, 2009.

[8] J.-S. 'Milo, F. C. Mace, and J. A. Nevin. The effects of constant versus varied reinforcers on preference and resistance to change. *J Exp Anal Behav*, 93(3):385–94, 2010.

[9] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel. You are who you know: inferring user profiles in online social networks. In *Proceedings of the third ACM international conference on Web search and data mining*, pages 251–260, 2010.

[10] J. P. Pesce, D. L. Casas, G. Rauber, and V. Almeida. Privacy attacks in social media using photo tagging networks: a case study with facebook. In *'Proceedings of the 1st Workshop on Privacy and Security in Online Social Media*, pages 4:1–4:8, 2012.

[11] L. M. Ritterband, L. A. Gonder-Frederick, D. J. Cox, A. D. Clifton, R. W. West, and S. M. Borowitz. Internet interventions: In review, in use, and into the future. *Professional Psychology Research and Practice*, 34(5):527–534, 2003.

[12] J. Saltzer and M. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278 – 1308, 1975.

[13] B. F. Skinner. *Science and human behavior*. New York: Macmillan, 1953.

[14] B. F. Skinner. *Science and human behavior*. Martins Fontes, 2003.

[15] J. Yan and A. S. El Ahmad. Usability of captchas or usability issues in captcha design. In *Proceedings of the 4th symposium on Usable privacy and security*, pages 44–52, 2008.

[16] E. Zheleva and L. Getoor. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles. In *18th International World Wide Web conference (WWW)*, 2009.