Survey: Social Navigation as a way to improve decision-making process and reduce security risks

Survey Paper

Orkhan Muradov
Department of Computer Science
University of British Columbia
Vancouver, BC, Canada
omuradov@cs.ubc.ca

ABSTRACT

The use of community feedback and hints helps people to make everyday decisions easy. In this paper we discuss how social navigation improves decision-making process during information exploration and how it reduces risks of security attacks. We discuss drawbacks of social navigation and explore how community effort helps to achieve usable systems with low risk of security breaches.

1. INTRODUCTION

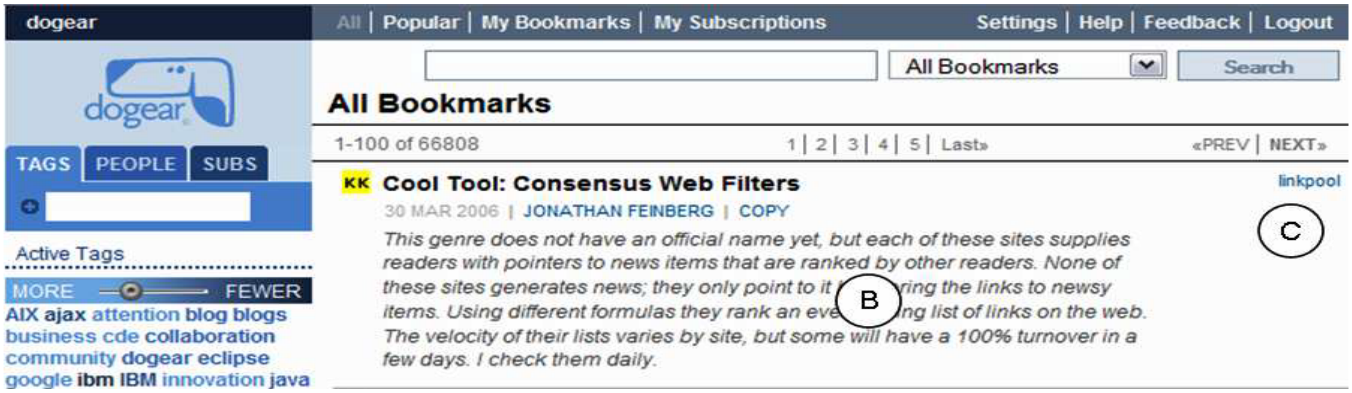
We see social navigational cues every day when we try to find a good restaurant and judge its quality by the number of customers. Number of customers in a restaurant is a social design cue for users, which indicates how customers are satisfied with dishes, service and prices. But it does not mean that every restaurant that has many customers will be good, since people have different tastes and opinions on what makes a restaurant to their satisfaction.

Dourish and Chalmers presented social navigation as a way to design interaction [1]. Since then it was well defined and explored by a number of other researchers. Social Navigation is an approach of using knowledge and experience of an audience to help guide users through actions and choices [2]. It has been used by a large number of well-known companies such as Amazon, Google, Wikipedia and eBay. These companies incorporated social navigation strategy in online searching, collaborative writing, and shopping recommendations. For example, Google uses an algorithm that ranks pages by number of links pointing to it. This allows big audience to vote on which page provides the best help in certain field [3]. Wikipedia is a free service and the best example of collaborative work that shows how community effort can benefit every user [4]. eBay‘s user ranking system shows how collaborative decision cues help users to decide whether they want to do more business with certain buyers and sellers.

We discuss two approaches that social navigation can take to make decision-making: information exploration and security management. The first approach improves everyday browsing experience such as exploring for new information or online shopping. For instance, collaborative filtering helps users to find the most popular items on websites or look up interesting links from your friends and people with similar interests [5]. However studies showed that collaborative filtering raises many privacy questions and might leak information about individual users [12]. Svensson et al. a created an online food shopping system that allows users to communicate with current and previous buyers while shopping for recipes [6]. The second approach of social navigation involves the security of user‘s sensitive information and privacy while sharing information. When users feel desperate and do not know how to set certain privacy configurations, they start searching online for possible solutions. Because many people are indifferent to configuring their security and privacy settings [16, 17] and ignore technical problems associated with security management [18, 19], social navigation systems can provide simple and easy-to-use approaches to making informed choices. For instance, from previous research it can be concluded that users repeatedly prefer to delegate security and privacy configurations to others [16], however when using social navigation they can simply use community‘s majority decision.

Paul DiGioia and Paul Dourish argued that the biggest problem for users is to match security settings to user‘s needs and practical concerns. Empirical studies showed that software systems couldn‘t have aspects of security and usability at the same time, rather having both of them as main aspect of design [10, 11, 13]. But with the lack of knowledge in security and without any help many users might be victims to security attacks. The annual CompTIA survey found that nearly 60% of security breaches were cause by human lack of knowledge in security and errors [14]. Several systems were developed to warn users about possible security breaches while browsing, connecting to services and transferring information. For example, Goeks and Mynatt created Acumen system that uses community‘s activity information to aid other users in configuring rules for cookies [8, 9, 15].

This survey paper is structured as follows. First we introduce several systems developed using information from community by giving social navigational cues. Then we talk about the results of these systems‘ evaluations and discuss possible problems of social navigation. In addition, we discuss problems associated with the collaborative filtering and possible ways of attacking.


dogear
All | Popular | My Bookmarks | My Subscriptions
Settings | Help | Feedback | Logout
dogear
All Bookmarks
Search
TAGS
PEOPLE
SUBS
All Bookmarks
1-100 of 66808
1 | 2 | 3 | 4 | 5 | Last»
«PREV | NEXT»
KK
linkpool
C
B
Active Tags
MORE
FEWER
AIX ajax attention blog blogs
business cde collaboration
community dogear eclipse
google ibm IBM innovation java

Cool Tool: Consensus Web Filters

30 MAR 2006 | JONATHAN FEINBERG | COPY

This genre does not have an official name yet, but each of these sites supplies readers with pointers to news items that are ranked by other readers. None of these sites generates news; they only point to it ring the links to newsy items. Using different formulas they rank an eve ng list of links on the web. The velocity of their lists varies by site, but some will have a 100% turnover in a few days. I check them daily.

Figure 1: Dogear interface

Next, we introduce systems developed to improve security configurations and privacy of users using social navigational element in the design. At last, potential solutions to password security are discussed that use social navigational cues as a feedback to users.

2. APPLYING SOCIAL NAVIGATION

2.1 Usability

Miller D et al. introduced a social navigation system, Dogear, that allows users to share personal bookmarks [5]. This application is browser-based, installed as a toolbar button add-on for a browser. Figure 1 shows the Dogear interface that includes users‘ bookmarks with the title, creation date, related tags and Metadata related to the content and context of the bookmark. This system shows most active users and most popular bookmarks in a side bar. In addition, Dogear displays a tag cloud of bookmarks, which allows everyone to visualize most popular bookmarks in a small window. User also gets a choice of seeing only his/her own bookmarks and statistics about them. In order to see how this social navigation feature for bookmarks enhances users‘ information exploration, researchers decided to run a user study by recording data through the log files, online surveys and questionnaires, e-mail and blog comments, and feedback about the service.

After running the user study, results suggested that approximately 60% of the Dogear service users utilized bookmark collection navigational elements using at least one pivot web link of other people‘s bookmarks. This implies that experiment results confirmed that user enhance their social navigation through the bookmark collection by tags, people and both tags and people. Qualitative study results showed that users are more likely to use other people‘s bookmark collection rather than browsing through the tag collections. All results conclude that social navigational cues in Dogear system significantly improved usability of the system.

2.2 Direct and Indirect Social Navigation

Social navigational cues can appear directly to a user by letting him/her communicate with the administrator of any other user. For example, communicating with an agent via chat helps user to answer some of their questions. On the contrary, indirect social navigation combines community information into one majority decision and is displayed to the user through system interface. Svensson M et al. created an online food store, EFOL (European Food On-Line), which is based on recipe ingredient clustering. Instead of selling ingredients separately, the store has a big selection of recipes [6]. When user adds a recipe of the dish to the cart, ingredients required for the recipe get added too. Each recipe page acts as a social meeting place where users, represented with avatars, can communicate with each other through chat. Figure 2 shows EFOL interface with user avatars on the top left corner, chat room in the top right corner and recipe list in the bottom. Researchers define this as a direct social navigation and believe that direct communication with other users helps people make better decisions. Indirect social navigational tools can help users give suggestions on how many people have used certain ingredient for a recipe. These suggestions are represented as number of users who bought certain recipe and as a result, list of recipes is then sorted by number of people who purchase the recipe. In addition, EFOL users can see what next recipe page a person moves to. This allows users to make further decisions and suggestions as to where to go next.

Qualitative exploratory user study has shown that users found navigational cues, as well as social aspects such as chat room very helpful. Participants found movement log from one recipe room to another also very helpful to their search. The study also revealed some design issues such as the snowball effect. This means that users can start following other peoples‘ decisions down the wrong path. Another design issue of social navigation tools is privacy problem. Some users did not like being stalked by other users when they were changing recipe rooms, while others did not find it bothersome. Many users pointed out that direct social navigation through the chat room was very intrusive.

2.3 Collaborative Filtering and Privacy Risks

Caladrino and Shmatikov identified the risks of using collaborative filtering in online services [12]. Collaborative filtering is a way of identifying relationship between items based on user preferences. For example, after buying certain item on Amazon website users see recommendations of what other people bought after buying the same item. Researchers identified four different types of suggestions by

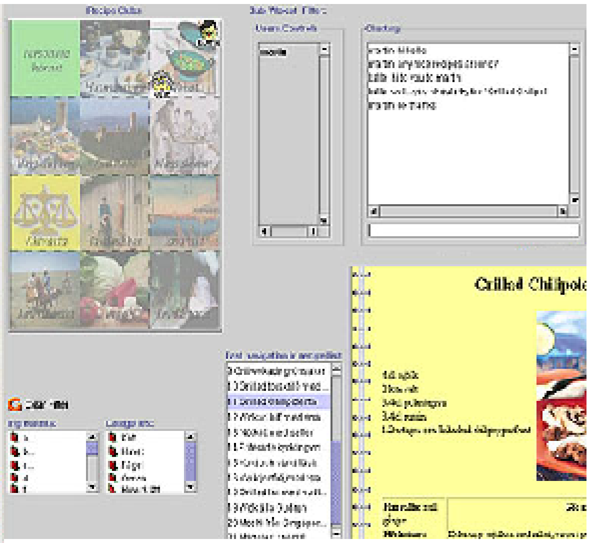


Figure 2: EFOL Interface

recommendation systems: user-to-user, item-to-user, item-to-item and user-to-item. The study was performed on three online recommendation services: Hunch, LibraryThing and Last.FM. Hunch is a popular personalization and recommendation website, LibraryThing is an online service for book recommendations and Last.FM is an online music recommendation engine. The simulation experiment used algorithm with passive inference attack where the system was observed over time. During this experiment, all changes in the public outputs of recommendation services were captured over some period of time. During the attack, known similarity list items to be associated with the target user were observed. Researchers looked for items, which either appeared in the list or moved up, indicating increased similarity with the auxiliary item. Moreover, if the same target item t appeared and moved up in the related-items lists of a sufficiently large subset of the auxiliary items, then t has been added to the user‘s record. In addition to passive inference attack, an active k-nearest neighbor attack was performed on the same recommender services. kNN attack used k nearest sybil users to determine items specific to a user.

Results of this experiment suggest that public recommendations by systems based on collaborative filtering may leak information about the behavior of individual users to an attacker with limited auxiliary information. Also, the bigger number of customers, the harder to use inference attacks. There are several solutions to stop privacy leakage in collaborative filtering recommender systems. By limiting the length of related item lists it becomes impossible for attackers to determine similarities. Limiting the speed and rate of data access makes it harder to run inference attacks. Limiting the frequency of updates of less popular items may decrease attack efficiency.

3. SOCIAL NAVIGATION AND SECURITY

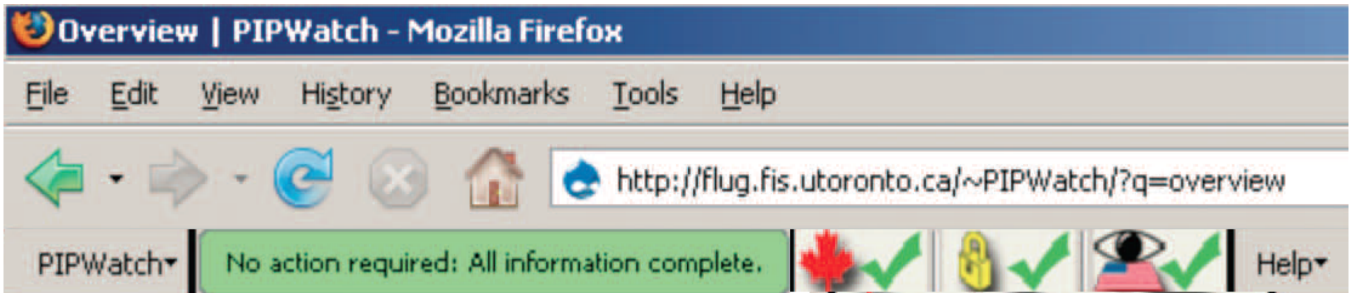
3.1 Usable security

In privacy sphere, a browser extension application described by Clement A. and Tisenbaum M. lets users visually understand, collect and share the privacy setting of website [8]. PIPWatch is a tool that assists individuals in protecting their privacy online while browsing. Information about websites is collected by users contributing through the PIPWatch tool and by website administrators who fill out the questionnaire. PIPWatch determines if the website‘s policies and procedures comply with Canadian Privacy Laws and Regulations. Secondly, website‘s policy of document and Information sharing with organizations has also to comply with Canadian Privacy Laws and regulations. At last, the information transmitted to US must not be subject to USA Privacy Act. As shown in Figure 3, there are three icons in browser toolbar corresponding to above questions. Each icon shows a green check mark if policy rules were satisfied and a red cross mark when website‘s policy rules are not satisfied. In the lower right hand corner a beaver icon shows a score out of 10 which represents overall privacy risks taken while visiting the website. All websites‘ privacy information is saved on the PIPWatch server and securely transmitted during every website visit. Above described social navigational tools in PIPWatch allow users to visualize the privacy risks while browsing. In addition, these icons help people understand more about privacy issues they can face and where their personal information might end up.

Goeks and Mynatt proposed a tool that allows user manually or automatically manage website cookies using social navigation [9, 15]. Acumen system is one of the first attempts to manage privacy management problems using social navigation. This application uses community‘s activity information that aids other users to configure rules for cookies. Acumen system‘s users can only see aggregated data of other users and cannot access any other information. Researchers divided users into two groups: ordinary users and a subset of expert users called marvens. Acument‘s social navigational toolbar in Internet Explorer gets cookie information from other users through Acumen web proxy and displays results in a small pop up window in Internet Explorer toolbar interface. The interface shows marvens‘ and simple users‘ results separately.

After running 6-week user study, participants visited 2560 websites and Acumen engine blocked 85 of them. Results of the experiment suggest that most of the 85 blocked website were in fact bad, with 91% true positive and 87% true negative rate. This suggests that Acumen system in fact works and gives correct cookie privacy management suggestions to users. Some users did not agree with the Acumen‘s settings and manually blocked some of the cookies.

Besmer A, Watson J et al. implemented a Facebook application prototype that helps users to decide access control policy for applications in Facebook [7]. The prototype was hard coded and was not placed anywhere, it was only used for user study purposes. When a user tries to access a new application in Facebook, application requires access to profile data in order for it to work. When the window pops up, users have to choose to continue or to cancel. The prototype


Overview | PIPWatch - Mozilla Firefox

http://flug.fis.utoronto.ca/~PIPWatch/?q=overview

No action required: All information complete.

Figure 3: PIPWatch interface

window has the same purpose but in an addition to the original window, it gives social navigation cues to the user. The prototype window displays each data field that application is trying to access, an example from user profile and finally a navigation cue. Each data field that the application is trying to access is checked by default, but the user has an option to uncheck any of the items. Navigational cue bar‘s value is represented as a percentage of people who gave access to a user profile‘s data field. In addition, the navigation cue bar is highlighted in green if the percentage of people who gave the permission is high, but otherwise it is highlighted in red. Researchers have not reported exact threshold numbers that define each color of a navigational cue bar.

Social network users are confronted with many policy decisions everyday where they need to decide whether they want to share their personal profile information online. Social navigation helps users to make policy and privacy decisions but it still remains unknown what is the real impact of social navigation on users‘ decisions. Researchers were interested in whether users would start sharing application more or less depending on the use of navigational cues. Results of the study suggest that navigational cues do in fact impact users‘ decision-making process. This impact might be very small, but it still exists. Moreover, social navigational design elements need to be more noticeable and need to draw more user attention. An interesting finding of this user study showed that only users who regularly make policy decisions should be included in the community information. This means that if everyone‘s decision data was aggregated in the navigational cues, then the cues would always remain very high.

3.2 Password Strength Meters and Social Navigation

Current methods of measuring password strength have limits since they are only applying rules to passwords to check its complexity. Many websites use mechanisms to check password strength and some of them even reject low complexity passwords. For example, while creating a new account in Gmail, users get visual feedback for the password strength in the highlighted bar on the right hand side. These mechanisms use rules that require using special characters, numbers and limiting minimum password length. These rules ensure that resulting password are reasonably secured, infeasible to guessing attacks and on average will be hard to crack. However, accuracy of these password testers is very low, resulting in accepting insecure passwords [24]. Castelluccia C. et al. proposed a new password checker mechanism that uses Markov model [23]. Researchers show how building adaptive password strength checkers improves accuracy of the feedback without worrying about n-gram database leaks. It is very similar to ordinary databases that hold large number of passwords where database attack does not cause breaches. Traditional way of storing password in a database hashes and salts password. However, authors argue that it is possible to reconstruct the password by searching for overlapping segment with n-grams. Paper shows how noise addition helps to prevent these kinds of attacks and results in very limited password information leakage. The model construction based on Markov models reaches much better accuracy than traditional password meters. Results show that new strength meter allows users to get much more precise feedback which may result in more secure password usage.

4. RESULTS AND DISCUSSION

Social Navigation has been used by many systems in both online browsing and security management of the systems. User study on Dogear system showed that social navigation proves to be very useful and approximately 60% of the users using bookmark-tagging functionality [5]. Results of the experiment confirm that users enhance their social navigation through the bookmark collection by tags, people and both tags and people. Qualitative study results showed that users are more likely to use other people‘s bookmark collection rather than browsing through tag collections. Qualitative exploratory user study of online food shopping system has shown than users found navigational cues, as well as direct social navigational elements such as chat room very helpful [6]. The study also revealed some design issues such as the snowball effect. This means that users can start following other peoples‘ decisions down the wrong path. Another design issue of social navigation tools is a privacy problem. Some users did not like being stalked by other users when they were changing recipe rooms, when others did not get bothered by it. This means that direct social navigation is still an issue and users prefer indirect social navigation. Collaborative filtering is used by many websites but it still open to some privacy issues. Caladrino and Shmatikov identified the risks of using collaborative filtering in online services using passive and active inference attacks [12]. Results of experiment suggest that public recommendations by systems based on collaborative filtering may leak information about the behavior of individual users to an attacker with limited auxiliary information. Researchers also studied the

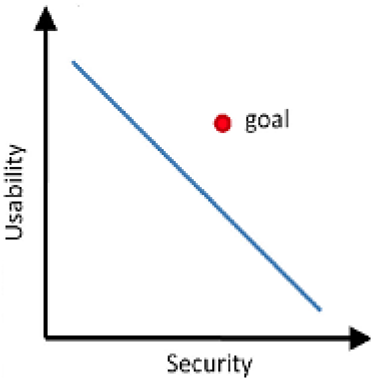


Figure 4: Usability vs Security

usability of security management using social navigational cues. Results of 6-week user study suggest that Acumen system gives accurate cookie privacy management suggestions to users [8]. Some users did not agree with the Acumen‘s settings and manually blocked some of the cookies. Thus, users always need to have a choice of manual security configuration. At last, the password strength meter model based on Markov models developed by Castelluccia C. et al, reaches much better accuracy than traditional password meters. Results show that new strength meter allows users to get much more precise feedback which may result in more secure password usage. To summarize, social navigation proved to be very useful in online browsing and security management experience. Results showed that indirect social navigational design elements help users make hard decisions, and improve security and privacy management.

5. CONCLUSION

This survey paper shows how social navigation is applied in many systems and how it helps users to improve their browsing experience, manage security configurations and overall make decision process much easier. The paper shows how direct social navigation helped users make decisions, however it is subject to many privacy issues. At last, we discuss how social navigation helps to improve security management and reduce risks related to insecure password selections. Figure 4 shows how it is hard to achieve all usability and security goals of a system. The more user friendly the system gets, the higher risk of security breaches becomes. With social navigation and community feedback users get closer to getting a usable and secure system at the same time, which makes it easier to achieve the goal.

6. ACKNOWLEDGEMENTS

This survey paper is a term project for Computer Security Course at University of British Columbia. I want to thank Professor Konstantin Beznosov for giving this opportunity to learn more about security.

7. REFERENCES

[1] Dourish, P. and Chalmers, M., *Running Out of Space: Models of Information Navigation*, Short paper presented at HCI’94 (Glasgow, UK).

[2] K. Hook, D. Benyon, and A.J. Munro., *Designing Information Spaces: The Social Navigation Approach*, London, U.K.: Springer, 2003.

[3] S. Brin and L. Page, *The anatomy of a large-scale hyper textual Web search engine*, in Seventh Int. World Wide Web Conf., Brisbane, Australia: Elsevier, 1998.

[4] A. Lih, *Wikipedia as participatory journalism: reliable sources? Metrics for evaluating collaborative media as a news resource*, in Proc. 5th Int. Symp. Online Journalism (Austin,TX), April, 2004

[5] David R Millen and Jonathan Feinberg, *Using Social Tagging to Improve Social Navigation*, 2006

[6] Martin Svensson, Kristina Hook, Jarmo Laaksolahti, Annika Waern, *Social Navigation of Food Recipes*, In: Proceedings of the SIGCHI conference on Human factors in computing systems, 20-25 Apr, Seattle, Wahington, USA.

[7] Andrew Besmer, Jason Watson, Heather Richter Lipford, *The impact of social navigation on privacy policy configuration*, Proceedings of the Sixth Symposium on Usable Privacy and Security, 2010

[8] Andrew Clement, David Ley, Terry Costantino, Dan Kurtz, and Mike Tissenbaum, *Using Social Navigation to Enhance Privacy Protection and Compliance*, Technology and Society Magazine, IEEE 2010

[9] Jeremy Goecks, Elizabeth D. Mynatt, *Supporting Privacy Management via Community Experience and Expertise*, Georgia Institute of Technology, 2005

[10] Weirich, D. and Sasse, M.A., *Pretty Good Persuasion: A first step towards effective password security for the Real World*, Proceedings of the New Security Paradigms Workshop 2001 (Sept. 10-13, Cloudcroft, NM), 2001

[11] Dourish, P., Grinter, R., Delgado de la Flor, J., and Joseph, M., *Security in the Wild: User Strategies for Managing Security as an Everyday*, Practical Problem. Personal and Ubiquitous Computing, 2004

[12] Joseph A. Calandrino, , Ann Kilzer, Arvind Narayanan, Edward W. Felten, Vitaly Shmatikov, *You Might Also Like: Privacy Risks of Collaborative Filtering*, 2 011 IEEE Symposium on , pp.231-246, 22-25 May 2011

[13] Paul DiGioia and Paul Dourish, *Social Navigation as a Model for Usable Security*, Proceedings of the 2005 symposium on Usable privacy and security, 2005

[14] *The annual Computing Technology Industry Association (CompTIA) survey* `http://www.cso.com.au/article/155941/whoops_human_error_does_it_again?fp=32768&fpid=20026681#closeme`

[15] Jeremy Goecks, W. Keith Edwards, and Elizabeth D. Mynatt, *Challenges in Supporting End-User Privacy and Security Management with Social Navigation*, Proceedings of the 5th Symposium on Usable Privacy and Security, 2009

[16] Dourish, P., Grinter, R., Delgado de la Flor, J. and Joseph, M. *Security in the Wild: User Strategies for Managing, Security as an Everyday, Practical Problem. Personal and Ubiquitous Computing*, 8 (6). 391-401

[17] Whitten, A. and Tygar, J.D. *Why Johnny can’t encrypt: A usability evaluation of PGP 5.0. 8th USENIX Security Symposium*, Usenix, 1999, 169-184

[18] Gross, J. and Rosson, M.B., *Looking for Trouble: Understanding End-User Security Management*,

Computer Human Interaction for the Management of Information Technology, (2007), ACM Press, 10.

[19] Schneier, B. *Secrets and Lies : Digital Security in a Networked World*, Wiley, 2004.

[20] Terry, D. *A Tour Through Tapestry.* Proc. ACM Conf. Organizational Computing Systems (Milpetas, CA), 21-30. New York: ACM Press, 1993

[21] Hill, W., Hollan, J., Wroblewski, D., and McCandless, J. 1992. *Edit Wear and Read Wear*, Proc. ACM Conf. Human Factors in Computing Systems CHI'92 (Monterey, CA), New York: ACM.

[22] A. Dieberger, P. Dourish, K. Hook, P. Resnick, and A. Wexelblat, *Social Navigation: Techniques for Building More Usable Systems*, Volume 7 Issue 6, Nov./Dec. 2000

[23] Claude Castelluccia, Markus Durmuth, Daniele Perito, *Adaptive Password-Strength Meters from Markov Models*, Network and Distributed Systems Security Symposium (NDSS), February 2012

[24] M. Weir, S. Aggarwal, M. Collins, and H. Stern, *Testing metrics for password creation policies by attacking large sets of revealed passwords*, In Proceedings of the 17th ACM conference on Computer and communications security (CCS 2010), ACM, 2010