Security and Usability Research Using a Microworld Environment

Noam Ben-Asher[1&3] noambena@bgu.ac.il
Joachim Meyer[1&3] joachim@bgu.ac.il
Yisrael Parmet[1] iparmet@bgu.ac.il
Sebastian Moeller[2] sebastian.moeller@telekom.de
Roman Englert[3] roman.englert@telekom.de

[1] Department of Industrial Engineering, Ben Gurion University, Beer Sheva, Israel
[2] Quality and Usability Lab, Deutsche Telekom Labs, TU Berlin, Germany
[3] Deutsche Telekom Laboratories @ BGU, Beer Sheva, Israel

ABSTRACT
Technological developments and the addition of new features to existing applications or services require the inclusion of security mechanisms to protect the user. When using these mechanisms the user faces a tradeoff between more risky and more efficient or safer and less efficient use of the system. We discuss this tradeoff and present a novel complementary experimental system which provides researchers and corporations the ability to explore and model the usability and security tradeoff in the context of user interaction with security systems and psychological acceptability, even before the actual development and implementation processes have ended.

Categories and Subject Descriptors
K.6.5 [**Management of computing and information systems**]: Security and Protection – *Invasive software*. H.1.2 [**Models and principles**]: User/Machine Systems - *Human factors, Software psychology*.

General Terms
Experimentation, Security, Human Factors

Keywords
Usability, security, experimental system, security settings, alerts.

1. INTRODUCTION
The tradeoff between usability and security will challenge researchers and system designers as long as information security processes will require user's involvement and decision making. According to the 2008 annual survey conducted by the Computer Security Institute, 43% of the respondents experienced security incidents. 50% percent of the reported incidents were virus related. Also, in 2008 it was the first time that "Theft/loss of proprietary information" and "Theft/loss of customer data" incidents had a subcategory labeled "from mobile devices", gaining 4% and 8% of the incidents respectively. Currently mobile devices are becoming the new frontier for hackers and in many cases are less protected than PC's ([9]).

Despite the significant developments and improvements in the algorithms behind security mechanisms, there are still many cases in which a human user is better equipped for making security related decisions. However, being better equipped does not necessarily ensure better performance. The consequences of users' faulty security related decisions and actions can be disastrous. Therefore, in many cases, users are referred to as "the weakest link in the chain" of information security ([11]). Additionally, since 2006 human vulnerabilities are included in SANS Top 20 Internet Security Vulnerabilities report.

MobileHCI'09, September 15 - 18, 2009, Bonn, Germany.
ACM 978-1-60558-281-8.

This evidence may seem surprising as users depend on computer systems and mobile devices to carry out important tasks and for assistance in achieving desired goals. Interviews have shown that end-users are aware to the susceptibility of their computer systems and information to security threats ([7]). Unfortunately, the same work found that the users' knowledge on security-related issues was generally dated and incomplete, something that evidently contributes to failures in the decision making process.

In this paper we will describe the usability and security tradeoff, the challenges researchers are confronted with and the approaches they take towards dealing with the issue. Finally, we will present a new approach and experimental platform for data collection with the aim to develop qualitative predictive modes of user's interaction with a security system that can be used to guide system designers', administrators' and management decisions.

2. USABILITY AND SECURITY TRADEOFF
The usability and security tradeoff is related to two partly interdependent issues. The first is part of the development cycle of a system which includes security features and the second is concerned with user's interaction with a security system or feature. During the application development cycle both usability and security are perceived as nonfunctional requirements which are usually addressed after the development process is completed. They are addressed separately by different experts. This may cause conflicts between usability and security, and the wrong assumption that they are two separate and competing goals ([3]). Moreover, applying traditional usability engineering (UE) methods to security applications will fail in many cases, due to the unique characteristics of a security-related task. For the end user security tasks are sporadically executed, their outcomes, if experienced at all, occur after long, irregular periods of time (especially an incorrect security-related decision) and hence, it is hard to perceive a specific situation (e.g. data corruption) as an outcome of a previously ignored security-related communication or a wrong action.

The other issue that profoundly influences the usability and security tradeoff is the way users interact with and perceive the security task. Users interact with computer systems in a goal oriented way and the same can be said regarding mobile devices. In some cases this interaction is interrupted by security related communications from a system which can be part of the operating system (e.g. file access or Bluetooth permission violations), embedded in a running application (e.g. a web browser) or a dedicated security application running in the background (e.g. an

anti-virus software). In such cases, the user is inevitably diverted from the current workflow and confronts a secondary, security-related decision or task.

The role of security related communications is very important for understanding usability and security tradeoffs. Usually a communication is the trigger to the interaction with a security system and it is received while the user is engaged in a different task. Cranor's ([3]) framework for reasoning about human interaction with security systems begins with a communication originated in a security system and ends with a behavioral outcome. In addition, there is extensive ongoing research dealing with various aspects of security related communication, aiming to improve risk/security communications (e.g. [7]) and alerting mechanisms (e.g. [4]).

Many user-related factors should be considered when trying to understand and improve a decision making process in response to security related communication. Users' mental models of possible risk are one of the aspects that are frequently addressed when examining interaction with security systems. Attitude towards risk, beliefs about the possibility of being attacked, beliefs in the accuracy of security indicators, the ability to understand the required security action, perceived self efficacy to interact with the security system and the efficiency of taking a security-related action are all factors which affect the mental model that directs user interaction with a security system ([3]). It seems that the security concepts implemented in applications and the level of expertise in operating the security system are the primary causes for incomplete and inadequate mental models. Evidently, not always a security related communication leads to a security behavior. Even when the user is ready to perform security operations, despite its usability costs, there is no guaranty that he or she will complete it successfully. No doubt that such an experience will affect the response to the next security communication.

Trying to apply economical approaches on usability and security tradeoffs is also not trivial. Safety, which is the aim of security features and systems, is an abstract concept which is not easily quantified. Performing security-related tasks rarely provided the user with directly observable benefits. As described by West ([12]), "The reward for being more secure is that nothing bad happens". Therefore, users lack the motivation to divert from their workflow and engage in a disturbing, unrewarding security task, which consumes time and effort.

A recent field of research known as HCISEC (Human Computer Interaction and Security) aims to incorporate usability and security, overcoming the challenges mentioned above ([8]). Making usability and security complimentary can synergistically enhance the efficiency of use and the safety of both users and information.

3. USABILITY AND SECURITY RESEARCH

3.1 Approaches

Researchers explore the relations between usability and security using different methodologies and approaches. Some conduct controlled laboratory experiments, which in many cases focus on specific aspects of a task and heavily depend on the application interface. Others evaluate and compare existing security features in commercial applications (e.g. [4]) or evaluate the usability of novel security developments (e.g. [10]). A different approach for gathering information is by surveys and interviews. These mainly focus on users' self-reported mental models, awareness, risk perception, reaction to security related communication and compliance with organizational security policies (e.g. [7]).

Alternatively, an ongoing research effort is intended to generate models of user interaction with security systems. This includes abstract behavioral models and quantitative predictive models which can be generalized beyond a specific task or interface. One of the main challenges confronted by researchers, who want to model the tradeoff between usability and security, is the difficulty to obtain real data on interaction with information security systems. Logs, security policies and other "behavioral references" are hard to obtain from organizations or individuals, as attackers can exploit such information to identify vulnerabilities ([5]).

3.2 Microworld Environment

To overcome this problem we created a novel experimental system which provides a controlled research environment for usability and security tradeoff research. It enables data collection on user responses to security-related communications and events. The microworld is a flexible experimental platform that is designed and built for running experiments in the field of usability and security in various settings. It is a research tool for studying user interaction and it provides data for both statistical analysis and modeling. Such controlled research environments can be particularly valuable when other traditional research methods cannot be used ([2]).

4. THE EXPERIMENTAL SYSTEM

The experimental system includes three main components. The first, a primary task based on a modified version of the well known computer game Tetris. The objectives of selecting a simple and popular game were (i) imitate normal and prolonged computer usage, (ii) create a motivating, fun and rewarding task, (iii) use a simple and common game which requires no previous knowledge in computers and can be played by a wide range of users types. Performance in the game, i.e. the number of completed rows, can be easily translated into a monetary incentive, delivering the ability to generalize the results beyond the game. The Tetris game itself was changed in order to make it more susceptible to security threats. Unlike the original version of the game, in the microworld completed rows are not removed automatically, but stay visible (and unsafe) until a button labeled 'Clear Rows' is pressed by the player. The 'Clear Rows' action saves the gains in a safe place and has usability costs. The player has a limited period of time for playing the game, e.g. 20 minutes. When performing the security related action, the game pauses, the player is idle and can not interact with the primary task, but the time left to play is still running. Thus, the usability cost should affect the willingness to execute such an action.

The second component of the microworld is an alerting system which provides the player with communications regarding possible threats that jeopardize his or hers gains from in the primary task (as seen in Figure 1). Such a communication triggers a decision making process which ends with security related behavior (correct or not). The alerting system operation is based on signal detection theory (e.g.[6]). Attacks are designated as signals. The experimenter controls the quality of the alert system

in terms of correct and incorrect detections. The player interacts with the front end of the alert system. As in many actual systems the user can change the setting of the security level. The level is selected from a scale ranging from *Very Low* to *Very High* security. A high security level might bring about many alerts, most of which will be false alarms, but there will be almost no missed detections. On the other hand, a low security level will lower the false-alarm rate, but will cause the system to miss some attacks. The player is required to set the desired security level before starting to play and can readjust it during the game, without any usability costs. When an alert appears, the player does not know whether the alert is justified or not. Moreover, the attack itself will occur only after a period of time which is unknown to the player.

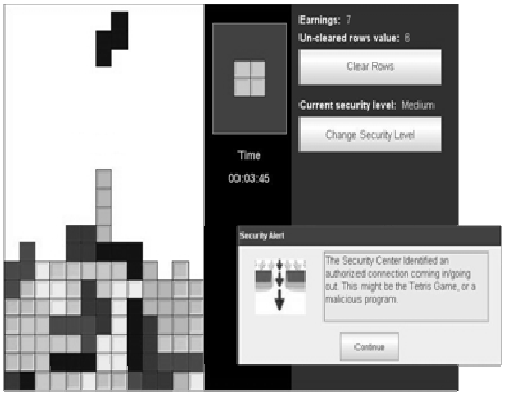

Figure 1: Screen capture of the experimental system when an alert appears.

Finally the system contains an attack generator which initiates attacks on the player's unsaved gains. The microworld possesses similar characteristics to the real-world, where attacks are unexpected and uncontrolled by the player. When an attack occurs, as seen in Figure 2, a certain proportion of the squares that appear on the screen is randomly erased, turning some of the completed rows to incomplete and accordingly decreasing the unprotected gains. The experimenter controls the severity of the damage caused by an attack through the proportion of squares erased after an attack. From the moment there is a single completed row the player can protect it by clicking the 'Clear Rows' button, an action which entails usability costs. The player decides whether to continue playing (ignoring the alert) or to execute a protective action.

The system was developed in Java, based on an open-source version of the game. It uses a client-server topology, where multiple players can participate in the experiment at the same time from various locations, allowing us to run large scale experiments over the network. In addition, each player can play several sessions. The server includes a database which logs events and players' actions.

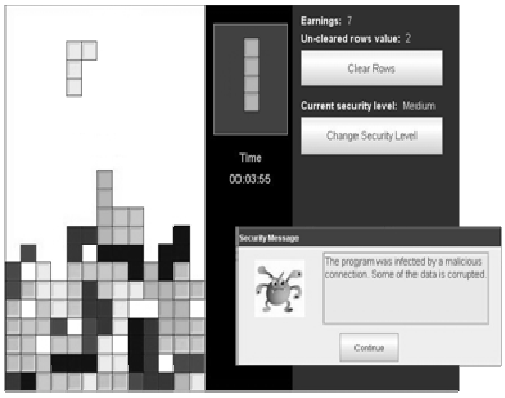

Figure 2: Screen capture of the experimental system following an attack.

4.1 Preliminary Experiment

Twenty participants participated in three 20-minutes sessions on three different days. The experiment was conducted at Deutsche Telekom Laboratories, TU Berlin, Germany. The settings of the experimental system included two levels of attack likelihood (High and Low) as an independent variable. Data regarding strategies selected by the players and interaction with the alerting system were extracted from the logs and analyzed. For a detailed description of the method and the analysis see [1]. In the following section we will demonstrate some of the findings and their implications when studying the tradeoff between usability and security.

5. RESULTS AND DISCUSSION

The number of alerts changed from session to session as a result of both changes in the settings of the alerting system performed by the participants and the random nature of the "microworld". The number of attacks was analyzed using linear models, with attack likelihood and sessions as independent variables and the number of attack as the dependent variable. In a 20 minute period players in the high likelihood condition experienced on average 11.4 attacks (SD=3.61) and players in the low likelihood condition experienced on average 3.2 attacks (SD=2.04).

The low and high attack likelihood conditions generated two significantly different environments. The first was risky with frequent attacks and the other was more relaxed with fewer attacks. As a result players who experienced more attacks presented a different interaction pattern with the alerting system. They adjusted the security level of the system more often, especially in the first session ([1]), and they set it to significantly higher levels compared to the low likelihood condition ($t=33.015$, $p<.001$, see Figure 3). Players in the low likelihood condition mostly continued to use the default (4) security level.

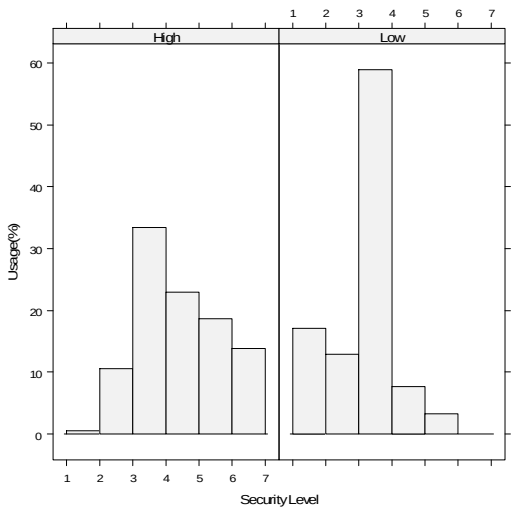

Figure 3: Security levels usage in percent for high and low attack likelihood.

In the game, players protected their gains by clearing rows. This security behavior could be triggered by a security related communication from the alert system but could also be the result of a player's spontaneous decision. A major determinant of the frequency of clearing rows is the usability costs. As seen in Figure 4, there were players that despite the low frequency of attack and the usability cost acted very cautiously and cleared rows routinely. No significant difference was found in the average number of clear rows actions (Low: Mean=16.30, SD=29.94 and High: Mean=15.23, SD=16.32). However, when looking at the number of saved rows in each security action (i.e. the gains from the security behavior) there is a significant difference. Players that are exposed to frequent attacks were willing to endure the usability costs that were required to protect relatively small gains. This finding is even clearer when looking at security related actions that occurred shortly after a security related communication ([1]).

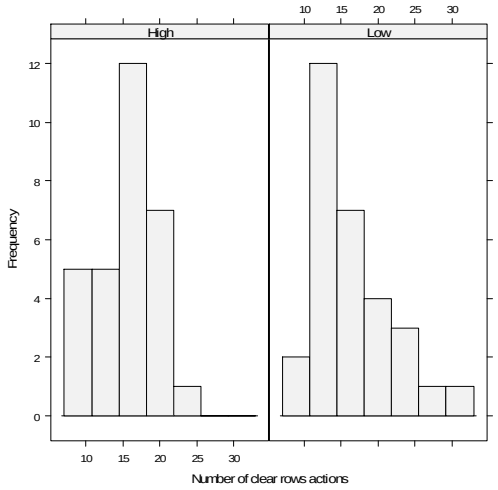

Figure 4: The number of clear rows actions for high and low attack likelihood.

6. CONCLUSIONS

The analysis of even relatively short periods of playing in the microworld revealed complex interaction patterns with the security system. Microworlds in general and specifically this experimental system can be used to quantitatively evaluate and model the acceptability of security features as a function of their efficiency, the severity of threats and the usability costs of using them. This application can also be used as a teaching tool, demonstrating possible consequences of different security behaviors. It emphasizes the role of security alerts and security related communications in information security.

7. ACKNOWLEDGMENTS

This research was funded by Deutsche Telekom AG as part of the Telekom Laboratories @ BGU activities.

8. REFERENCES

[1] Ben-Asher, N., Meyer, J., Moeller, S. and Englert, R. 2009. An Experimental System for Studying the Tradeoff between Usability and Security. In *Proceedings of the 4th International Conference on Availability, Reliability and Security (*Fukuoka, Japan, March 16-19, 2009).

[2] Cañas, J. J. and Waern, Y., 2005. Cognitive research with microworlds. In *Theoretical Issues in Ergonomics Science* vol. 6 (1), pp. 1-3.

[3] Cranor, L. F. 2008. A Framework for Reasoning About the Human in the Loop. In *Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA).

[4] Egelman, S., Cranor, L. and Hong, J. 2008. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *ACM SIG-CHI Conference on Human Factors in Computing Systems (CHI '08I)* (Florence, Italy, April 5-10, 2008).

[5] Gonzalez, J.J. and Sawicka, A., 2002. A Framework for Human Factors in Information Security. In *The 2002 WSEAS International Conference on Information Security (ICIS'02)* (Barcelona, Spain, December 15 – 18, 2002).

[6] Green, D. and Swets, J., 1966. Signal detection theory and psychophysics. New York: John Wiley and Sons.

[7] Gross, J. B. and Rosson, M. B. 2007. Looking for trouble: understanding end-user security management. In *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology* (Cambridge, Massachusetts, March 30 - 31, 2007).

[8] Johnston, J., Eloff, J.H.P., and Labuschagne, L. 2003. Security and human computer interfaces. In *Computers & Security*, Vol. 22 No.8, pp.675-84.

[9] Leavitt , N. 2005. Mobile phones: The next frontier for hackers. In *Computer*, 38(4), pp. 20-23.

[10] Renaud, K. 2005. Evaluating Authentication Mechanisms. *Security and Usability*, Cranor, L. and Garfinkel, S, ed., O'Reilly.

[11] Schneier, B. 2000. Secrets and Lies: *Digital Security in a Networked World*. John Wiley and Sons.

[12] West, R. 2008. The psychology of security. *Commun. ACM* 51, 4 (Apr. 2008)