A System for Studying Usability of Mobile Security

Liron Nehmadi
Industrial Engineering & Management
Ben-Gurion University P.O.B 653
Beer-Sheva 84105, Israel
+972526328080
nehmadi@bgu.ac.il

Joachim Meyer
Industrial Engineering & Management
Ben-Gurion University P.O.B 653
Beer-Sheva 84105, Israel
+97286472216
joachim@bgu.ac.il

ABSTRACT

The capabilities of mobile devices are rapidly evolving, but the methods to secure the devices remain relatively unchanged. This is a source for concern, as malicious attacks on mobile devices become more frequent [5]. We offer an experimental system where participants play an investment game (main task) in which money allocation is preconditioned by various security procedures (supportive task). Specifically, the system enables the researcher to compare and study Personal Identification Number (PIN) authentication, a common security method in mobile devices, to graphical password authentication, a novel security method currently used in various smart phones. Researchers can manipulate code lengths, button sizes, password expiration dates, passwords complexity and strength, system security policies and more. Moreover, the program enables the researchers to study the use of security systems under changing conditions of threats on users' assets and the reliability of the security methods being offered.

Categories and Subject Descriptors

J.4. **[Computer Applications]**: *Economics, Psychology*.

General Terms

Economics, Experimentation, Human Factors, Security

Keywords

Security systems, Authentication, PIN, Graphical passwords.

1. INTRODUCTION

Despite the different options available for increasing system security, mobile devices are suffering from inadequate protection, and as such, they become targets for malicious attacks [5]. This situation can be attributed to three main factors: (i) people store sensitive information (e.g. financial and business related information) on mobile phones; (ii) the capabilities of mobile phones have rapidly developed in the last few years, especially the ability to share information through various wireless technologies (e.g. Bluetooth, Wi-Fi, infrared, etc.). However, (iii) mobile security systems have not developed as much. Currently most mobile phone users practice minimal security, if any at all. An internal survey conducted by us at Deutsche Telekom labs in BGU included 308 participants from Germany and Israel. 75% of our respondents stated they rarely use Personal Identification Number (PIN) to protect their device (66% never use it). When examining the minority that does use PIN code protection, they are also far from being well protected, with 76% of PIN users reporting they never change their PIN code. Combining these findings with people's tendency to use easy codes (e.g., 1234), and to place their codes next to their device [1], one can understand why McAfee reports that mobile phones suffer from security breaches [5].

The fact that people do not (or hardly) practice mobile security does not origin from them being oblivious to mobile security threats. In our survey 40% of the respondents agreed with the statement that when their mobile phone is on, they are exposed to security threats. 55% of the Germans stated that they avoid using certain device functions due to security concerns (35% of the Israelis). Finally, 70% of the Germans said they would be very concerned about data stored in their device, if the device is lost (30% of the Israelis).

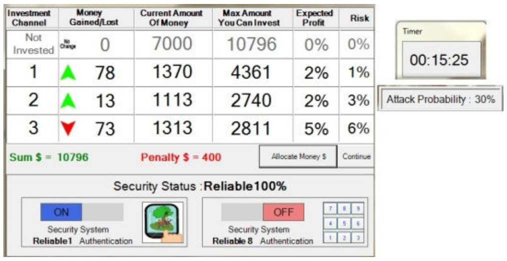
While mobile devices offer limited means of protection and provide minimal user guidance (if any at all), certain websites try to increase secure usage. They use "strength meters" to inform users regarding the ability of a code to protect them from hackers [4]. Some also prevent users from using simple codes [7]. Some government and universities websites even obligate users to change their passwords every few months [3]. However, all these efforts are meaningless if users ignore alerts, write down their codes, and use the same code for all purposes [1,2]. Hence, protecting users should not be done by imposing usage sanctions and creating new complicated workflows. Secure interaction could be attained by making it usable, personally suited to users' needs and with clear added value. We offer an experimental system that can be used by researchers who wish to study the usability of security systems, specifically, security systems in small-screen devices.

2. EXPERIMENTAL SYSTEM

The experimental system offers a game for studying the usage of security systems in small screen devices. The effective resolution of the game's screens is 590px × 286px. The system supports two authentication methods: PIN code authentication and graphical password authentication - where users need to press certain "hot spots" in a picture to be authenticated [6]. The essence of the two methods is identical - authentication by memorizing a sequence of screen areas and pressing them in the prescribed order. The experimental system embeds the authentication methods in an investments game, where users can invest money in different investments channels. The game is built from a series of investments steps. In each step the maximum amounts of money the user can invest in each channel, as well as the channels' expected profits and risks, change. The risk, profit, and max amount values of each investment step are randomly sampled from uniform distributions before each step begins. The researcher, at the beginning of the experiment, sets the range of the uniform distributions. Figure 1 presents a system screen, with three investment channels, at a given investment step in the game. As seen, the user can see the amount of money currently invested in each channel and the maximum amount that can be invested in

Third International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)
June 12, 2011, San Francisco, CA, USA

each channel at that step. The user can also see the amount of money the channel gained or lost in the last investment step, as well as the new expected profit and risk of each channel at the given step. Gains and losses are determined based on the channel's actual profit value (return value), which is randomly drawn from a normal distribution, with the channel's expected profit as its mean and its risk as the standard deviation around this mean. Figure 1 presents a game setting that utilizes the full scale of the program functionalities. In this game setting, the user has a time limit for completing the game (thus increasing the cost of authenticating). The game security policy enables the user to choose which authentication method will be active (if any at all). The program also informs the user about the probability an attack will occur on its assets (money), as well as the reliability of the different authentication methods in preventing such an attack. Users should first decide whether to activate any of the authentication methods. Then users should decide if to continue to the next investment step without changing the current money allocation, or if to change money allocation before continuing to the next step. If no authentication method is active, the user avoids the authentication process in the course of money allocation; however, this comes with the price of being exposed to malicious attacks. If a certain authentication method is active, the user will be required to authenticate before changing the money allocation, hence the user is protected but valuable time is lost in the course of money investment (main task). If the user fails in the authentication process, penalties are issued. The accumulated sum of penalties is presented to the user on the main screen.



Investment Channel	Money Gained/Lost		Current Amount Of Money	Max Amount You Can Invest	Expected Profit	Risk
Not Invested	No Change	0	7000	10796	0%	0%
1	▲	78	1370	4361	2%	1%
2	▲	13	1113	2740	2%	3%
3	▼	73	1313	2811	5%	6%

Sum $ = 10796 Penalty $ = 400

Timer 00:15:25

Attack Probability : 30%

Security Status :Reliable100%

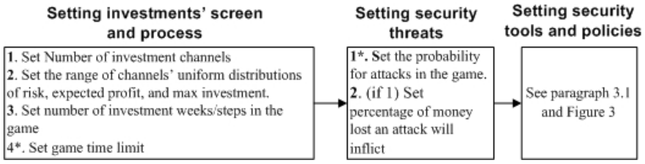
ON Security System Reliable1 Authentication

OFF Security System Reliable 8 Authentication

Figure 1. Main game screen

3. GAME SETUP

Game setup is done through three main setup screens (Figure 2)



Setting investments' screen and process

1. Set Number of investment channels
2. Set the range of channels' uniform distributions of risk, expected profit, and max investment.
3. Set number of investment weeks/steps in the game
4*. Set game time limit

Setting security threats

1*. Set the probability for attacks in the game.
2. (if 1) Set percentage of money lost an attack will inflict

Setting security tools and policies

See paragraph 3.1 and Figure 3

Figure 2: Game setup flow. * State optional settings

3.1 Setting security tools and policies

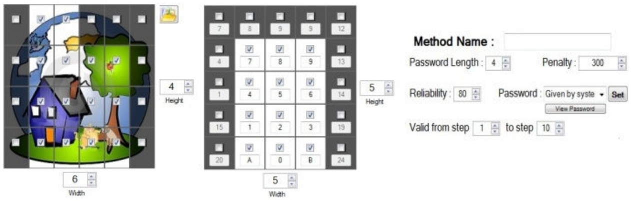
Figure 3 shows the interface elements used by the researcher to set the security system. The researcher can create up to 4 authentication methods. For each method, the researcher can set which areas in the screen will be "pressable" (by clicking them) as well as their size (by height and width spinners). For each method, the researcher assigns password properties. The researcher sets the number of investment steps the password will be valid for (thus controlling password expiration date), its reliability in stopping attacks, its length, penalties that will be issued when used incorrectly (e.g., entering the wrong password), and its source (provided by the user or set by the researcher). When the user is assigned for creating the password, the researcher can choose to prevent the user from assigning simple codes (e.g., 1-2-3-4).

3.2 Additional features

The program also allows the researcher to define the process described so far as a single game block. Therefore, in a single game several investment scenarios, each with its own unique characteristics, can be assessed. Furthermore, at the end of each block the program enables the researcher to create a custom questionnaire for the user to complete, thus besides documenting users' performance and actions, the program also documents subjective assessments.

4. FUTURE WORK

This program provides an experimental tool allowing researchers to study the usage of security systems in small screen devices under changing usage and system conditions. Upcoming work aims to finalize the program setup wizard and to conduct an extensive QA, as well as to carefully define and document the system log file. The first experiment using the system in its initial form has already been conducted, and a complete set of four additional experiments will be conducted once system development is completed. We hope our, as well as others', experiments using this system will allow security systems in mobile devices to become more usable, thus encouraging users to practice secure mobile usage.



Height: 4
Width: 6

Height: 5
Width: 5

Method Name :
Password Length : 4
Penalty : 300
Reliability : 80
Password : Given by syste
Valid from step 1 to step 10

Figure 3. Interface elements to set graphical passwords tool (left panel), PIN tool (mid panel), and authentication code

5. REFERENCES

[1] Adams, A. and Sasse, M. A. 1999. Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*. 42, 41-46.

[2] Florencio, D. and Herley, C. 2007. A large-scale study of web password habits. *16th International World Wide Web Conference (WWW),* 657-666.

[3] Florencio, D. and Herley, C. 2010. Where do security policies come from? *Proceedings of the Sixth Symposium on Usable Privacy and Security*. New York, NY.

[4] Furnell, S. 2007. An assessment of website password practices. *Computers & Security,* 26 (7-8), 445-451.

[5] McAfee. 2009. Mobile security report: http://www.mcafee.com/us/resources/reports/rp-mobile-security-2009.pdf

[6] Monrose, F. and Reiter, K. M. 2005. Graphical passwords. In: Cranor, L.F., Garfinkel, S. (Eds.), *Security and Usability*. O'Reilly, pp. 157-175 (Chapter 9).

[7] Yan, J., Blackwell, A., Anderson, R., and Grant, A. 2005. The memorability and security of passwords. In: Cranor, L.F., Garfinkel, S. (Eds.), *Security and Usability*. O'Reilly, pp. 129–141 (Chapter 7)