Mobile Security for Dummies

Designing Mobile Security Interfaces for the Non-Expert with Predictive Human Performance Modelling

Ann-Marie Horcher
Nova Southeastern University
horcher@nova.edu

Maxine Cohen, PhD
Nova Southeastern University
cohenm@nova.edu

Abstract— **Predicting the effectiveness of user interfaces at the design stage has been extensively explored for the traditional computer workstation and the expert user. Various analytical tools, such as CogTools apply the Keystroke Level Model (KLM) approach to evaluate software designs for efficiency prior to development. The mobile platform presents additional input paths and resource constraints not present on the traditional workstation platform. This study examines a methodology to extend current predictive human performance modelling to the mobile platform and accurately model the experience of the novice user.**

Keywords— mobile; security usability; predictive human performance modeling; variable risk

I. Introduction

User Interface (UI) designers are constantly challenged by the diversity of the user they attempt to serve and the typically limited resources for developing said interface [1]. Predictive human performance modelling can provide the UI designer with a "crystal ball" to see the future of a design expressed as a quantitative measure [2]. The rapid evolution of mobile platforms puts even greater pressure on UI designers to rapidly and accurately predict usability [3].

Mobile devices increase the convenience of computing, and also the variety of an individual user's computing experience [4]. The novice user is a significant and enduring portion of the target user community [5]. Security interfaces continually evolve in response to new more sophisticated security threats [6]. Though the users may develop familiarity and expertise with the target functionality of the mobile device or application, each iteration of more complex authentication strips them of their expertise with the security interface [5].

II. Background

In comparison to the traditional workstation, there are three major resource constraints of the mobile device platform. These are power, form factors, and user expertise. To be mobile, the devices must run from a portable and renewable power source, such as a battery [7]. The battery life is an important measure of user satisfaction. UI design that accelerates the drain of battery life reduces the usability of the device [8]. Mobile devices must be small enough and light enough to carry easily. The screens must be big enough to use but small enough to fit in pocket or purse [9, 10] because users manipulate the devices in a variety of settings, often while away from a formal workstation [11].

Computer systems and especially mobile devices [6] have moved outside the context of business and research organizations to become essential in the home [12]. Without a formal organization to compensate for individual user deficiencies, the applications themselves must have reduced complexity [9].

Usable security on the mobile device requires a resource conservation priority over the organizational bias of previous design principles developed for the workstation [13]. Too much security and the users run the risk of not having access to their own devices. Moving UI design principles developed for the traditional workstation to the mobile platform has produced mixed results [14]. The reality is in the traditional workstation environment of a business or research organization ignoring certain security-usability principles has minor consequences [15]. In the resource-constrained mobile device ignoring the consequences compromises the practical functionality of the device.

Keystroke-Level Modelling (KLM) predicts the amount of time an expert user will take to execute typical tasks with a UI [2]. Amendment of the Keystroke-Level-Modeling protocols, particularly in the area of security interfaces, have been necessary to accommodate the reality of mobile [16, 17]. In the context of expert users KLM assessment of user interactions commonly combines a mental effort operator with physical operator (s) to describe an operation block [18, 19]. However for the novice or less technology literate, the mental effort may varies within that sequence of mental and physical actions [5]. Consequently, this research measures the mental effort separately from physical..

Previous research on novice users has focused on information gathering within the target functionality of an application. Information discovery about the interface is the antithesis of the goal of most security interfaces [20]. A security interface has additional usability challenge because it is perceived as an interruption of the user's progress towards the primary task [21].

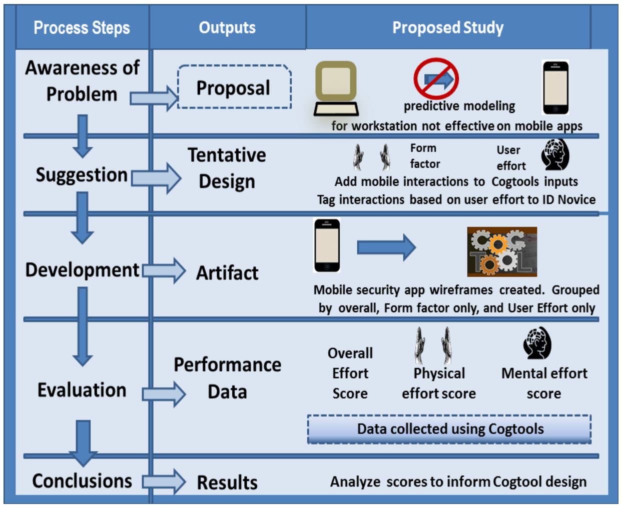
Process Steps
Outputs
Proposed Study
Awareness of Problem
Proposal
predictive modeling for workstation not effective on mobile apps
Suggestion
Tentative Design
Form factor
User effort
Add mobile interactions to Cogtools inputs
Tag interactions based on user effort to ID Novice
Development
Artifact
Mobile security app wireframes created. Grouped by overall, Form factor only, and User Effort only
Evaluation
Performance Data
Overall Effort Score
Physical effort score
Mental effort score
Data collected using Cogtools
Conclusions
Results
Analyze scores to inform Cogtool design

Figure 1: DSR used in Cogtools study

III. The Study

The objective of this research was to identify quantitative measurements for mobile security-usability at the design stage for the novice user. Unusable mobile security can result in the user avoiding the device to avoid the experience [22] or turning off the security [23]. Within the study the following research questions are examined.

- Can current predictive human performance modelling tools identify the expenditure of particular types of effort related to non-workstation design problems?
- Can current predictive human performance modelling be adapted to provide design feedback for non-expert users?

The study uses CogTools, a KLM based predictive human performance modelling tool that models the complexity of an application interface based on wireframes of the planned screens, and a mapping of the flow between these screens [1]. The current version of Cogtools predicts how much time an expert user will take to execute typical tasks with a UI [24]. Amendment of the KLM is necessary to adjust for the reality of mobile [16], particularly for security. KLM assessment of user interactions commonly combines a mental effort operator with physical operator (s) to describe an operation block [18, 19]. However for the novice or less technology literate, the mental effort may varies within that sequence of mental and physical actions [5]. This research separates mental from physical effort.

TABLE 1: Actions consuming constrained resources

Resource	Action consuming constrained resource
Form Factor	On-screen Keystrokes [19] Screen Touch/Swipe [18] Button pushes [16]
User effort	Un-cued recall of a piece of information [19] Cued mental recalls [5]

TABLE 2: Use Cases in Basic Authentication

Use Case	Knows UID	Knows Password
1	Yes	Yes
2	Yes	No
3	No	Yes
4	No	No

A. *Methodology*

The study uses Design Science Research (DSR) methodology [25] as illustrated in Figure 1. In DSR an artifact is built or created to validate the proposed model. The artifact was a set of rules to tag the actions CogTools analyzes. The rules identify constrained resources, such as cognitive effort and mobile form factors. For this study the tagged actions, seen in TABLE 1, were chosen based on the literature on mobile security interfaces and novice users.

B. *Procedure and Preliminary Results*

Three versions of the security interface to a mobile web application were created with varying amounts of user cognitive effort and screen interactions. The security interface used basic authentication, which is the most common authentication on both workstation and mobile [26]. Four use cases for navigating each version of the security interface, seen in Table 2 were used to create wireframes. When mapping the wireframes in the CogTools software, each action described in Table 1 was tagged.

The CogTools score was generated for the overall design of each version. Then scores were generated for all actions related to form factors, and scores for all actions related to user cognitive effort. A pilot study revealed a need to add the additional criteria of "success" for the next iteration of the study. An interface with a low CogTools score for complexity, but results in failure in three out of four use cases is not desirable.

C. *Discussion*

This research challenges the current bias toward the expert user for usability particularly in the area of security interfaces. The research also explores the concept that usability of a security interface is separate and has different design priorities than the software the security is protecting. Additional validation on non-security interfaces would be of interest.

References

[1] B. E. John, "Using predictive human performance models to inspire and support UI design recommendations," *Proceedings of the 2011 annual conference on Human factors in computing systems* pp. 983-986, 2011.

[2] R. Bellamy, B. John, and S. Kogan, "Deploying CogTool: integrating quantitative usability assessment into real-world software development," presented at the Proceedings of the 33rd International Conference on Software Engineering, Waikiki, Honolulu, HI, USA, 2011.

[3] D. Weir, D. Buschek, and S. Rogers, "Sparse selection of training data for touch correction systems," *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* pp. 404-407, 2013.

[4] A. Oulasvirta, T. Rattenbury, L. Ma, and E. Raita, "Habits make smartphone use more pervasive," *Personal Ubiquitous Comput.,* vol. 16, pp. 105-114, 2012.

[5] P. Gokarn, K. Gore, Devanuj, P. Doke, S. Lobo, and S. Kimbahune, "KLM operator values for rural mobile phone user," *Proceedings of the 3rd International Conference on Human Computer Interaction* pp. 93-96, 2011.

[6] L. Qing and G. Clark, "Mobile Security: A Look Ahead," *IEEE Security & Privacy,* vol. 11, pp. 78-81, 2013.

[7] A. A. Economides and A. Grousopoulou, "Students' thoughts about the importance and costs of their mobile devices' features and services," *Telematics and Informatics,* vol. 26, pp. 57-84, 2009.

[8] A. Knight, G. Pyrzak, and C. Green, "When two methods are better than one: combining user study with cognitive modeling," presented at the CHI '07 Extended Abstracts on Human Factors in Computing Systems, San Jose, CA, USA, 2007.

[9] D. Churchill and J. Hedberg, "Learning object design considerations for small-screen handheld devices," *Computers & Education,* vol. 50, pp. 881-893, 2008.

[10] A. S. Shirazi, N. Henze, T. Dingler, K. Kunze, and A. Schmidt, "Upright or sideways?: analysis of smartphone postures in the wild," *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* pp. 362-371, 2013.

[11] T. McGibbon, C. Hosmer, C. Jeffcoat, and M. Davis, "Use of Mobile Technology for Information Collection and Dissemination " 2011.

[12] M. L. Mazurek, J. P. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns*, et al.*, "Access Control for Home Data Sharing: Attitudes, Needs and Practices " *Proceedings of the 28th international conference on Human factors in computing systems* pp. 645-654, 2010.

[13] S. L. Garfinkel, "Design principles and patterns for computer systems that are simultaneously secure and usable," Massachusetts Institute of Technology, 2005.

[14] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): Demystifying security challenges in mobile environments," *Proceedings of the Eleventh Workshop on Mobile Computing Systems No. 38; Applications,* pp. 43-48, 2010.

[15] R. A. Botha, S. M. Furnell, and N. L. Clarke, "From desktop to mobile: Examining the security experience," *Computers & Security,* vol. 28, pp. 130-137, 2009/6// 2008.

[16] P. Dunphy and P. Olivier, "On automated image choice for secure and usable graphical passwords," presented at the Proceedings of the 28th Annual Computer Security Applications Conference, Orlando, Florida, 2012.

[17] E. v. Zezschwitz, P. Dunphy, and A. D. Luca, "Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices," presented at the Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services Munich, Germany, 2013.

[18] J. F. M. Bernal, L. Ardito, M. Morisio, and P. Falcarin, "Towards an Efficient Context-Aware System: Problems and Suggestions to Reduce Energy Consumption in Mobile Devices," *Proceedings of the 2010 Ninth International Conference on Mobile Business / 2010 Ninth Global Mobility Roundtable,* pp. 510-514, 2010.

[19] H. Li, Y. Liu, J. Liu, X. Wang, Y. Li, and P.-L. P. Rau, "Extended KLM for mobile phone interaction: a user study result," *CHI '10 Extended Abstracts on Human Factors in Computing Systems* pp. 3517-3522, 2010.

[20] P. Holleis, M. Scherr, and G. Broll, "A revised mobile KLM for interaction with multiple NFC-tags," *Proceedings of the 13th IFIP TC 13 international conference on Human-computer interaction - Volume Part IV* pp. 204-221, 2011.

[21] J. Gebauer, D. M. Kline, and L. He, "Password Security Risk versus Effort: An Exploratory Study on User-Perceived Risk and the Intention to Use Online Applications " *Journal of Information Systems Applied Research,* vol. 4, pp. 52-62, 2011.

[22] M. F. Theofanos and S. L. Pfleeger, "Shouldn't All Security Be Usable?," *IEEE Security & Privacy,* vol. 9, pp. 12-17, 2011.

[23] S. Furnell. (2008). *End-user security culture: A lesson that will never be learnt?* . Available: http://www.sciencedirect.com/science/article/B6VNT-4S807WG-F/2/0c9e7de7efb8df6814a63948a149cb5a

[24] E. v. Zezschwitz, P. Dunphy, and A. D. Luca, "Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices," *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services,* pp. 261-270, 2013.

[25] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *Management Information Systems Quarterly,* vol. 28, 2004.

[26] S. Chiasson, A. Forget, E. Stobert, P. C. v. Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords," *Proceedings of the 16th ACM conference on Computer and communications security* pp. 500-511, 2009.