Key-bored to Tears: The Usability Cost of Character Authentication on Mobile Devices

Ann-Marie Horcher

Nova Southeastern University
horcher@nova.edu

ABSTRACT

Walking into traffic, off the beaten path, or colliding with people – distracted walking is on the rise as people struggle with touchscreen interactions designed for workstation instead of mobile devices. The keyboard is a well-known mental model for soliciting input for authentication. Mental models familiar to the user reduce the cognitive effort required to understand the desired interaction with the security interface. Though the cognitive effort to understand the interface may be conserved, there is also cognitive effort expended to use the keyboard-style interface. The reality of the actual cognitive effort required is documented by the rise in pedestrian accidents involving smartphone usage.

Measures of the effort required for smartphone authentication using human performance modelling show how security design choices can significantly impact usability on the mobile platform, and calls into question current common practices. Strong passwords on a mobile device demand more cognitive effort than is safe at any speed.

1. INTRODUCTION

Increasingly, mobile devices have moved from being companion devices of a computer workstation [38] to being the primary or stand-alone device for digital information access [59]. As the use of mobile devices as the primary increased, so has the amount of sensitive data stored on the devices [14].

In spite of receiving security advice suggesting the need to protect data, users still choose not to protect the data. For instance, Herley observed that security advice is getting increasingly complex without a clear positive cost-benefit trade-off for the additional effort expended by the user [21]. In the absence of an independent measure of the effort, it is still possible that many users are correctly perceive basic authentication as an unreasonable security hurdle to an application. As an example, Harbach et al. empirically showed that in 27 days, the participants in their study spent an average of over an hour each day just unlocking their devices [19].

When listening to music or talking, individuals are more likely to look at their device [49]. The danger of cognitive distraction from mobile phone use reduces situation awareness and , increases unsafe behavior [39]. Pedestrians are at greater risk for accidents, and crime victimization. Every eyes-on interaction decreases ability to ambulate due to the need to divide attention between the screen and the surrounding environment [29].

The dropped head posture adopted by the user to see the screen affects not only visibility of surroundings but also balance and gait [27]. Dancers and figure skaters have long known the weight shift caused by a head dropped forward by looking at the ground is detrimental to balance [57], even though the weight of the average human skull is only 10-11 pounds. Eyes-on security input, such as basic authentication, requires both looking away from the environment to ensure authentication success, and a dropped head. Disengagement from the environment while the user in motion even as a pedestrian decreases usability and safety.

2. BACKGROUND

Distractions caused by mobile phone use while driving have clearly shown the connection between texting and traffic accidents [34]. In the United States, hands-on use of a mobile phone has been regulated in fourteen states and has resulted in a reduction of traffic accidents particularly for less-experienced drivers [62]. There is conflicting evidence on the impact of conversation as a distraction. Drivers taking calls related to work experienced a higher level of distraction [15], but those who were conversing had decreased levels of driver fatigue in a monotonous driving situation [48].

The damage done while driving is exacerbated by the distances travelled during the distraction, roughly 100 yards at 55 mph in 4 seconds [36]. A typical pedestrian walks at 3 feet per second [27] amounting to a distance travelled of 12 feet. In an urban setting with no barriers between pedestrians and traffic, plus other obstacles, 4 seconds is more than sufficient to move from safety to danger [37].

Security input for basic authentication differs from input for a text message because of the rules for strong passwords [24]. To prevent a dictionary attack to guess a password, users are encouraged to choose character sequences that are not typically typed [55] Passwords that are easily typed by going across a row in in a keyboard (QWERTY) are also discouraged [16]

More complex typing tasks and higher cognitive induce dual-task interference while walking [33]. The higher the cognitive load required by input, the less cognition is available for safely navigating the surroundings. Research to improve typing usability on the mobile device keyboard has focused on predictive text to reduce interaction time [47, 56]. Since strong passwords should fail predictive text criteria, these algorithms do not improve the accuracy of security input. Touchscreens also produce higher error rates during movement, and user familiarity does not improve accuracy [42].

Symposium on Usable Privacy and Security (SOUPS) 2017, July 12 -- 14, 2017, Santa Clara, California..

3. RESEARCH QUESTIONS

The current designs used for mobile security input for basic authentication rely heavily on characters entered through a keyboard interface. The usability of using security designed on a workstation and then transferred to a mobile platform has been questioned [40]. If cognitive load and touchscreen manipulation are the factors that determine the safety/usability of a security interface on the mobile platform, it is important to understand how those resources are being expended.

RQ1 – How does a keyboard usability for security input on a workstation compare to mobile?

RQ2 - How do the constrained resources of power, cognitive effort and form factor impact usability of basic authentication on mobile?

4. THE STUDY

The study uses Cogtool, 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 [26]. The current version of Cogtool predicts how much time an expert user will take to execute typical tasks with a UI [61]. The predictions are based on a database of human performance on a series of micro-tasks such as eye movement, hand movement, screen taps, keystrokes, and mouse movements.

Amendment of the KLM is necessary to adjust for the reality of mobile [13], particularly for security. KLM assessment of user interactions commonly combines a mental effort operator with physical operator (s) to describe an operation block [4]. However for the novice or less technology literate, the mental effort may varies within that sequence of mental and physical actions [18]. This research separates mental from physical effort.

The following hypotheses were evaluated to address the research questions.

H0 –Non-workstation inputs and cognitive effort have no significant impact on the Cogtool score for basic authentication

H1 - Conserving mobile form factor manipulations will improve predicted usability of basic authentication from Cogtool

This hypothesis explores the concept that the manipulation of the form factors is the root of the lack of usability for many applications on the mobile platform [31, 50, 51], and even more so for security [10].

H2 – Conserving user effort will improve predicted usability from Cogtool

The second hypothesis focuses on the role of cognitive effort in authentication. Less obvious than the physical challenges explored in the first hypothesis, but the importance of conserving cognitive effort is recognized as needed in authentication [22, 54].

4.1 Methodology

The study uses Design Science Research (DSR) methodology has illustrated in Figure 1. In DSR an artifact is built or created to validate the proposed model [23]. Several alternatives for the security interface design were created as series of wireframes. The wireframes were analyzed in Cogtool to identify the least complex interface.

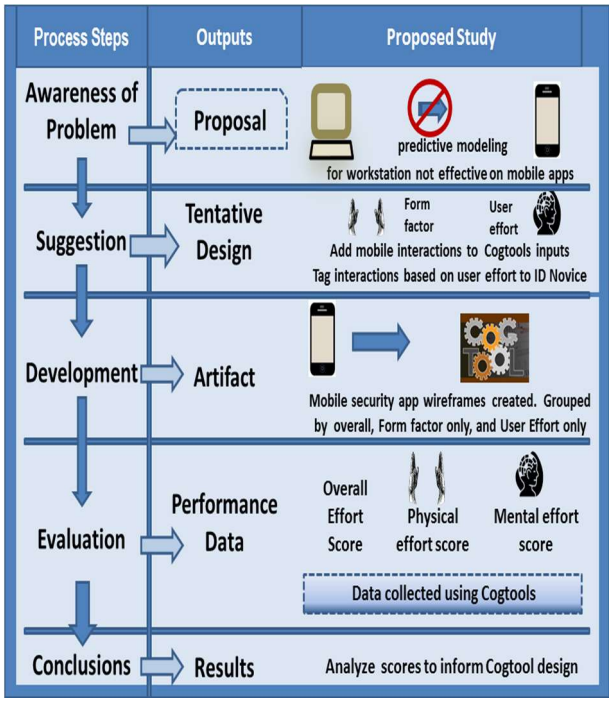

Figure 1: DSR used in Cogtool study

The analysis focused on actions that consume the constrained resources, as such as cognitive effort and mobile form factors. The actions, described in Table 1, were chosen based on the literature on mobile security interfaces and novice users.

Table 1: Actions consuming constrained resources

Resource	Action consuming constrained resource
Form Factor	On-screen Keystrokes [32] Screen Tap/Swipe [4] Button pushes [13]
User effort	Free recall of a piece of information [53] Cued recall of information [18]

Though Cogtool was developed initially to evaluate desktop design with keyboard and mouse, the accuracy of the Cogtool measure on the mid-range touchscreens (7-17") has been verified as acceptable [1]. Later work by Ocak compared Cogtool measures to actual end-user performance data on mobile [41]. For specific operations that involved less decision and more confirmation, such as tapping an "OK" button, or a swipe, Ocak found an up to 20% overestimation for Cogtool. When the user is familiar with the interface, they proceed to the next step with less "Think" time then estimated by Cogtool.

However, the tasks showing an overestimation by Cogtool also had screen targets the width of the mobile screen, or the size of a fingertip or greater. The typical screen keyboard has targets much smaller than a fingertip. In the case of interaction with an on-screen keyboard, the end-user performance times from Ocak were slightly higher than the Cogtool prediction. In this study the "Think" time associated with each screen-tap that represents a keystroke is due to need for eyes-on interaction. Acquiring a

target smaller than a fingertip and separated from the next target by less than a fingertip requires greater dexterity and more visual direction by the user.

The artifact was then created as a web application using basic authentication. The web application stores hints to help users log on to infrequently used websites. The hints are delivered based on the concept of progressive authentication, which seeks to reduce the authentication overhead on mobile devices [46]. During Riva's evaluation of a prototype of progressive authentication the users were allowed to trade off convenience against stronger protection based on an assignment of risk. When using content at lower risk, less frequent authentication was required from the user.

In the web application used in this study risk was determined by location. In a high risk location the user does not receive hints to assist in authentication. In a medium or low risk location the user receives hints to cue recall of UID and/or passwords. The user also has a reduced requirement to authenticate based on lowered risk.

A pilot study showed the need for defining successful logon as a criteria determining usability [25]. These results were fed back into the artifact design and re-analyzed with Cogtool. Using a micro-release technique recommended for software development in a rapidly changing technology [11], the artifact was updated and re-evaluated as is directed by DSR methodology.

4.2 Procedure

Four security-related tasks were analyzed for usability in each design (Table 2). Three versions of the security interface to a mobile web application were created with varying amounts of user cognitive effort and screen interactions. Because the artifact was a web application, the same interfaces were also evaluated on the traditional workstation.

Table 2: Security-related Tasks for Basic Authentication

Task	Knows UID	Knows Password
Logon Attempt	Yes	Yes
UID recovery	No	Yes
Password Reset	Yes	No
Password Recovery (Cued recall)	No	No

The UID password used to "demonstrate" or walk through a Cogtool simulation was chosen to emulate the most typical values used for user accounts. Before emails became common-place, users chose random usernames as an account identifier [45]. Email addresses became a popular option with account suppliers because they:

1. Are already unique
2. Provide a communication channel for both marketing and password recovery.

The majority of email address ranges between 16-28 characters [7]. On the other hand, email addresses generated from legacy systems such as Unix are typically 8 characters plus "@"plus a domain name for the email server [6]. Users typically prefer a shorter email particularly if typing on a mobile phone. Therefore the UID chosen for the simulation is: abcdefgh@abcd.com.

The password for the demonstration was chosen to follow rules for a strong password which are shown in Table 3.

Table 3: Strong Password Rules [24]

Rule	Derivation from Literature
8 characters or more	Morris & Thompson ,1979 [35]
At least one number and at least one uppercase	Vu et al., 2007 [58]
Misspell words	Keith, Shao & Steinbart, 2007[28]
Use Passphrase	Pinkas & Sander, 2002 [44]
No seasons, days of the week, months, or names	Morris & Thompson ,1979[35]

The rule for misspelled words and passphrase is used to avoid a dictionary lookup which checks for words, so the password chosen is not a word. The password is also not based on a row of keys on the QWERTY keyboard. A special character is also a frequent requirement for passwords generated by banks and other institutions providing access to sensitive information. Therefore the password chosen for the simulation was: Abcdefgh2`

4.2.1 Login Attempt

The login attempt task is mapped to the subject providing the typical basic authentication input of a UID and password. This path leads to success as shown in Table 2 when the user knows both the UID and the password.

4.2.2 UID Recovery

The UID recovery task is performed when the subject forgets the UID. The artifact verifies if the UID provided by the user is valid. If it is not valid, the appropriate message is displayed. Since the UID is typically relatively public [21], as described earlier, the recovery by an email confirmation to account establishment email. UID recovery is only needed in a high risk location. UID is pre-filled in low and medium risk locations.

4.2.3 Password Reset

Password reset occurs when the subject cannot recall the password. The user requests a reset and receives a temporary password sent to the email account used as the UID for this authentication. The user copies the temporary password and provides a new strong password. The user is also prompted to create a password hint to allow password recovery in locations which are low risk.

4.2.4 Password Recovery (Get hint)

The password recovery task is only available if the user is in a low risk location. It provides an avenue to successful authentication that is an alternative to the password reset process. The user sees a recall cue if one was set when prompted during password change.

4.2.5 Mapping the sub-tasks

The current version of Cogtool provides a visualization of how the measures of user interaction is generated. In the tool only two visualizations can be compared at a time (Figure 2). The measures on the visualization graph are broken down into eye movements, left hand movements, cognition, etc. In the same amount of time one keystroke is completed on mobile (green box), three keystrokes are completed on the desktop (yellow box).

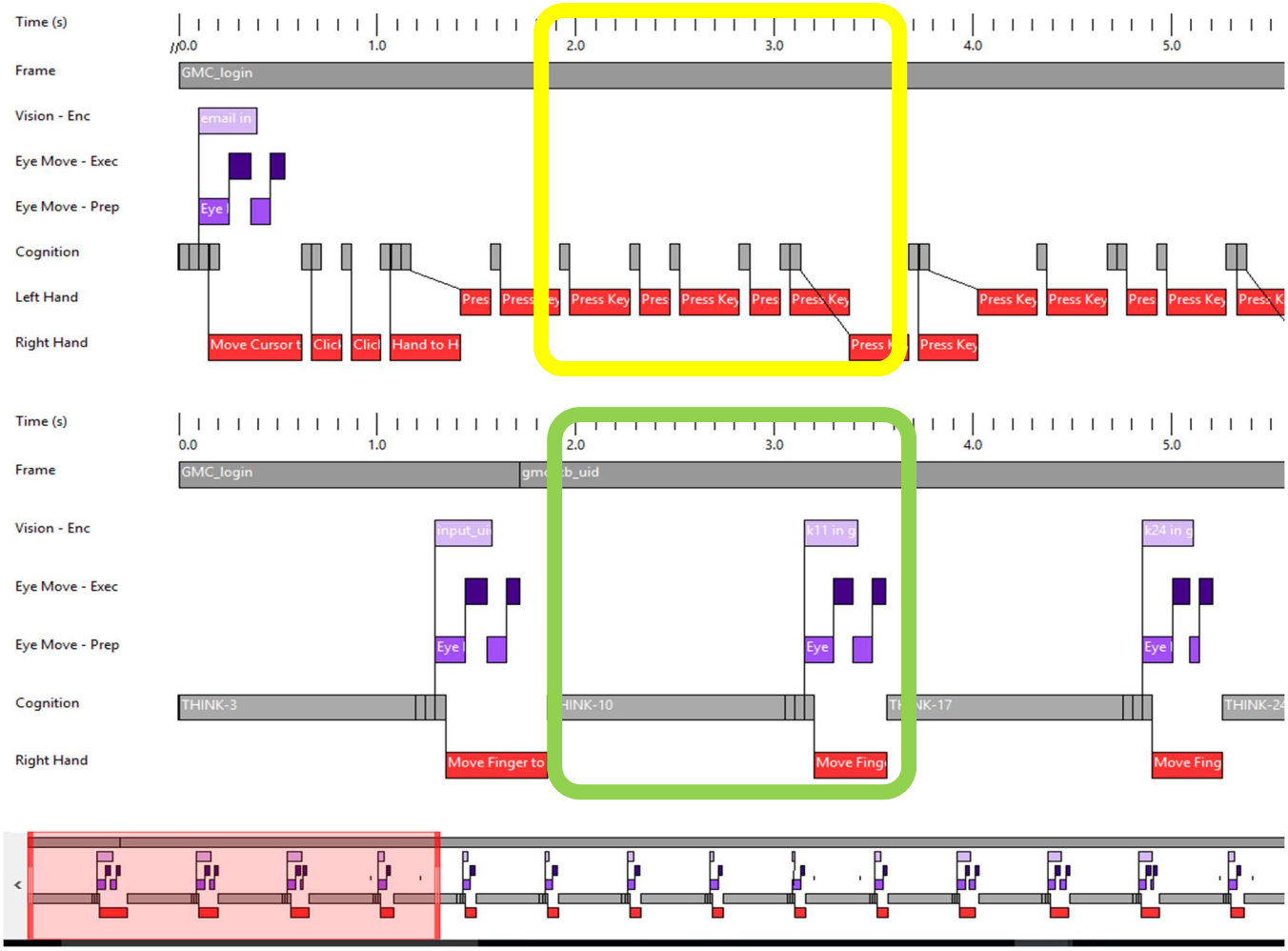

Figure 2 – Excerpt of Cogtool Visualization Comparing Desktop (Yellow) to Mobile (Green) for Logon Attempt

On the desktop, there is an eye movement at the beginning of the sequence of keystrokes to position the hands. On mobile, there is an eye movement, cognition, and positioning on every keystroke in the sequence.

Unfortunately the level of granularity shown in the visualization is not in the reports available to the designer using the tool. Cogtool does provide the ability to export the demonstration as a series of steps to a comma-limited values (CSV) file, but without the difficulty score attached.

To get the difficulty scores separated by the constrained resource being deployed, the Cogtool actions as described in the CSV file were mapped to power, user effort, and form factors. Then the individual actions were demonstrated, and a difficulty score computed for each separate action (Table 4).

Power and User Effort each only related to one Cogtool action. When assigning a difficulty for tasks involving cognitive effort, the complexity of the mental task being performed was considered. The most complex task, computing a new password, has the greatest complexity and consequently the greatest difficulty.

To get the difficulty for form factors, the individual actions were demonstrated on both desktop and mobile. The effort for a lower case character is less than for upper case, or special characters.

Table 4: Difficulty scores for Constraints in seconds

Action to measure	Con-straint	Cogtool equivalent	Difficulty (seconds)
Display screen	power	Look at	0.5 sec
Recognition	user effort	Think	1.2 sec
Decide	user effort	Think + Think +Think Decision require evaluation of option 1 and 2 and a choice.	3.6 sec
Compute input	user effort	Think + Think + Think + Think A multiple step mental process with recall of requirements, and creation of an entry	4.8 sec

There are also actions that only occur on one environment or other, such as swipe (mobile-only) and mouse (desktop-only).

Table 5: Difficulty compared for Desktop vs. Mobile

Action to measure	CogTool equivalent	Difficulty	
		Desktop	Mobile
Input character	Input lower case character	0.4 sec	1.8 sec
Input UC	Input upper case character	0.6 sec	3.4 sec
Input Special	Input special character	0.7 sec	5.1 sec
Input UClc	Input upper case followed by lower case	1.0 sec	5.1 sec
Move and Tap	Move finger to target and Tap touchscreen	NA	0.6 sec
Move Mouse	Move Mouse to target and Left Click	2.0 sec	NA
Move-no-think	Move Mouse from muscle memory	0.9 sec	NA

4.3 Results

Each security task was demonstrated for each version of the design. Some actions are also auto-generated by Cogtool based on the database of human performance modelling data. Wherever Cogtool determined a new screen had appeared, a "Look At" action was added to the script. Every keypress automatically creates a hand movement action with the correct hand that would be used by a touch typist trained in the QWERTY keyboard. For a touchscreen interaction, a cognitive action to identify hand position is auto-generated based on the need for the user to look at the keyboard and identify the spot to touch [26].

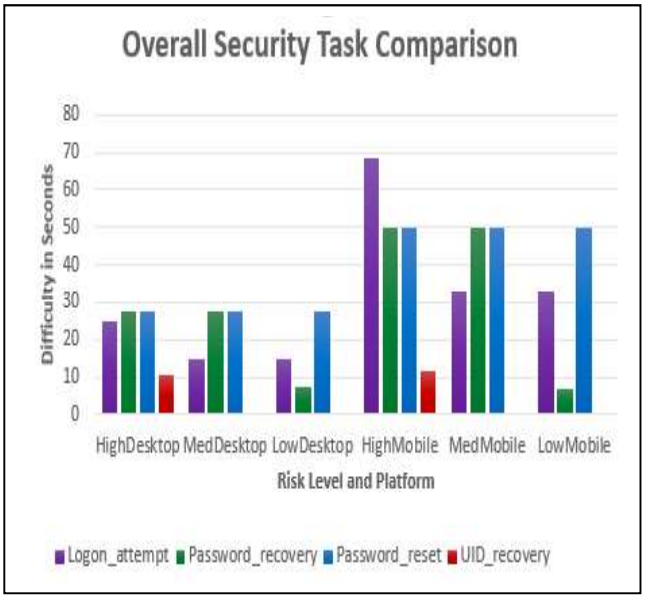

Figure 3: Security Task Difficulty Comparison

An overall score for security task demonstration appears in Figure 3. As suggested by the greater form factor difficulty for individual actions on mobile in Table 4, mobile has a higher difficulty in seconds for the current norm, which is labelled "High." The design changes to conserve constrained resources on mobile in the "Medium" and "Low" versions show some improvement on scores were generated for desktop. For some tasks the conservation of resources in design eliminates the task (UID_recovery) and benefits both platforms. The Logon_attempt and Password_reset security tasks are the most difficult and have the most interaction with a keyboard.

4.3.1 Logon Attempt Difficulty

The Logon_attempt typically occurs on every usage of an application. Making this task more usable would have high impact. The Cogtool score for the logon attempt task on mobile is more than double the desktop platform score (Figure 4).

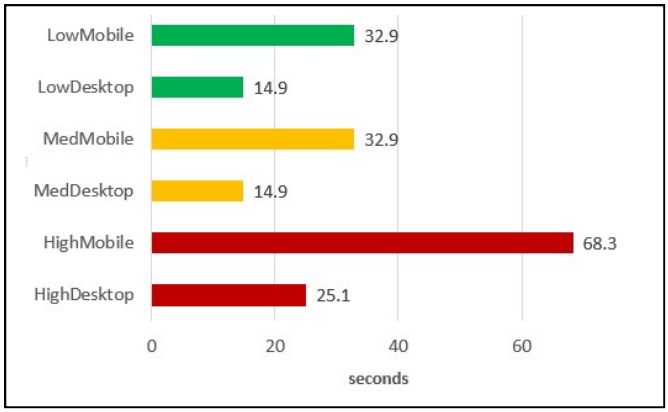

Figure 4: Difficulty in Seconds of Logon Attempt Comparison

When the logon attempt is broken into subtasks, as shown in Table 5, it is clear the subtasks of inputting both UID and password are responsible for most of the difficulty.

Table 5: Detailed Difficulty scores for subtasks of Logon

Task	High DT	Med DT	Low DT	High Mobile	Med Mobile	Low Mobile
Logon	25.1	14.9	14.9	68.3	32.9	32.9
Subtasks						
Display GPS	2.6	0.6	0.6	1.7	0	0
Recall UID	2.5	0	0	3.2	0	0
Input UID	6.9	0	0	31.2	0	0
Recall pw	2.5	2.5	2.5	3.2	3.1	3.1
Input pw	9.8	9.7	9.7	27.8	27.8	27.8
Display Home	0.8	2	2	1.3	1.8	1.9

As seen in the Cogtool visualization (Figure 2), the security interface on Desktop is drawing upon different resources than the Mobile platform for the input of both the UID and the password. Though mental model of "typing" on a keyboard is identical, the reality of performing the tasks is not the same difficulty.

On a workstation an expert user inputs a UID and a password using a physical keyboard. The script generating from modelling this activity is shown in Figure 5. In terms of user effort and form factor manipulation, the physical keyboard demands less movement of the eyes and hands. The string of characters that makes up the input is processed as whole.

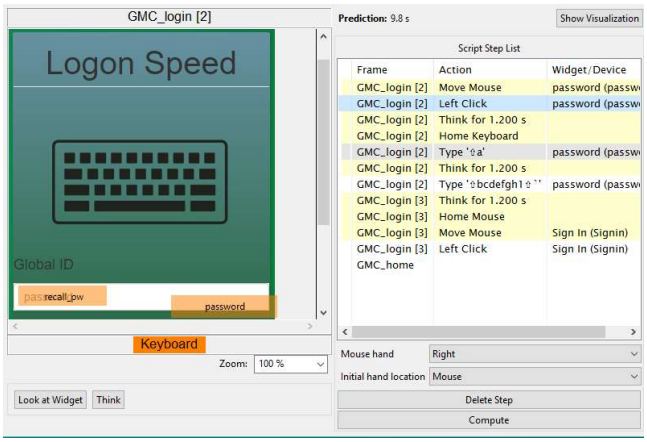

Figure 5: Cogtool Script modelling password input on Desktop

In comparison the script generated from modelling this activity on a mobile device shows a repetitive but more challenging series of actions to achieve the input (Figure 6). The user does not typically use both hands or even both thumbs [43] to input security strings such as UID and password. Each letter or character requires an eye movement (user effort), a movement to position a finger over the key (user effort), and the actual key tap (form factors). A portion of each keypress form factor action on mobile is cognitive effort.

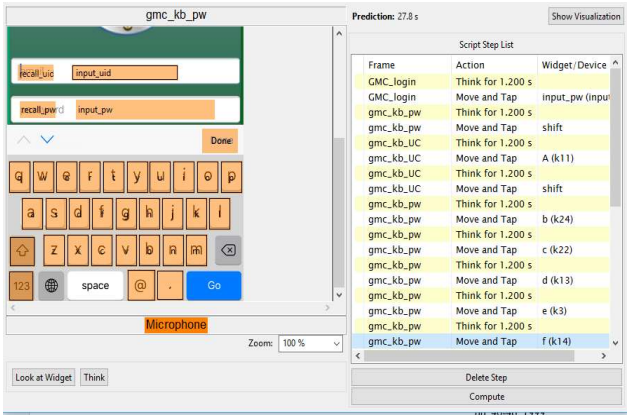

Figure 6: Cogtool Script modelling password input on Mobile

5. Discussion

Though the ineffectiveness of wholesale transport of workstation security design to the mobile platform has been called into question by previous research [40], the security model of basic authentication retains a significant foothold on mobile [10]. The lack of usability of basic authentication has generated considerable research on alternatives such as pass-faces [12], graphical passwords[5, 8, 10, 17, 53], pass-chords[3, 30], and gestures [50, 52], but basic authentication is still the most common security model.

The results show interaction with basic authentication on a non-workstation platform differs from the workstation resulting in decreased usability. There is hidden cognitive load in eyes-on input that increases the difficulty of the security interface.

The universal availability of a keyboard-like input and the widespread understanding of the concept of basic authentication make the low implementation cost almost irresistible to the less innovative security designer. In the absence of a measure-predicted usability like this study, the impact of poor choices on input can be disregarded. Similar to the "Don't Text and Drive" campaign, eyes-on security like keyboard-based character authentication with taking over 3 seconds should be blacklisted on mobile as the primary interface.

The usability lessons have been so poorly learned that the paradigm of using a touchscreen for keyboard has spread to even smaller screens with a similar lack of success [60]. Password meters have been successful in leading users towards stronger passwords [9]. Security usability meters that calculate the difficulty of input on various platforms that could guide security designers toward understanding the cost of their security choices. For a mobile platform the length of time the user must be "eyes-on" could a trigger a usability warning.

Common practices supplant best practices when ease of adoption is too high and the detrimental effects are not clearly understood. At one time changing passwords every 60 days was best practice for security – now research has clearly shown this not to be the case.

This research calls into question the common practice of using an email address as the UID. The mental ease of recall has trumped the difficulty of typing a lengthy sequence with special characters on a touchscreen. The difficulty of typing the UID is frequently as high as or higher than the actual password. Furthermore, the added difficulty does not result in added security.

The lack of usability for security inputs on a touchscreen also points to a need for a better design of the touchscreen keyboard construct. A security-input optimized keyboard may alleviate the issues that hamper the usability of touchscreen input. The use of a security-optimized keyboard could be limited to security inputs in the design of an interface so as to not impact other uses of the keyboard. Alternate versions of keyboards are already triggered to ease entry of email addresses and URLs. A similar technique could be used.

Voice and haptic interfaces have improved to become a viable "eyes=off" option [2]. The cognitive load on the mobile user can be reduced by collecting information about the user from the environment and processing with artificial intelligence to create conversational interaction [20]. Instead of turning a slab of glass into a bad keyboard, the design principles for usable security must conserve the constrained resources and exploiting the extended possibilities.

6. REFERENCES

[1] Abdulin, E., "Using the keystroke-level model for designing user interface on middle-sized touch screens," *CHI '11 Extended Abstracts on Human Factors in Computing Systems*, pp. 673-686, 2011.

[2] Arif, A., Pahud, M., Hinckley, K., and Buxton, W., "A tap and gesture hybrid method for authenticating smartphone users," *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, pp. 486-491, 2013.

[3] Azenkot, S., Rector, K., Ladner, R., and Wobbrock, J., "PassChords: secure multi-touch authentication for blind people," *Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility*, pp. 159-166, 2012.

[4] Bernal, J. F. M., Ardito, L., Morisio, M., and Falcarin, P., "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.

[5] Biddle, R., Chiasson, S., and Oorschot, P. C. V., "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surv.,* vol. 44, no. 4, pp. 1-41, 2012.

[6] Blezard, D. J., and Marceau, J., "One user, one password: integrating unix accounts and active directory," *Proceedings of the 30th annual ACM SIGUCCS conference on User services*, pp. 5-8, 2002.

[7] Bliss, A. "How Long Is The Average Email Address?," March 6, 2017; http://www.freshaddress.com/fresh-perspectives-blog/long-email-addresses/

[8] Bulling, A., Alt, F., and Schmidt, A., "Increasing the security of gaze-based cued-recall graphical passwords using saliency masks," *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, pp. 3011-3020, 2012.

[9] Carn, X. D., #233, Carnavalet, D., and Mannan, M., "A Large-Scale Evaluation of High-Impact Password Strength Meters," *ACM Trans. Inf. Syst. Secur.,* vol. 18, no. 1, pp. 1-32, 2015.

[10] Chiang, H.-Y., and Chiasson, S., "Improving user authentication on mobile devices: a touchscreen graphical password," *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, pp. 251-260, 2013.

[11] Clarke, P. M., Elger, P., and O'Connor, R. V., "Technology enabled continuous software development," *Proceedings of the International Workshop on Continuous Software Evolution and Delivery*, pp. 48-48, 2016.

[12] Dunphy, P., Nicholson, J., and Olivier, P., "Securing passfaces for description," in Proceedings of the 4th symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 2008, pp. 24-35.

[13] Dunphy, P., and Olivier, P., "On automated image choice for secure and usable graphical passwords," *Proceedings of the 28th Annual Computer Security Applications Conference* pp. 99-108, 2012.

[14] Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., and Wagner, D., "Are You Ready to Lock?," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, Arizona, USA, 2014, pp. 750-761.

[15] Engelberg, J. K., Hill, L. L., Rybar, J., and Styer, T., "Distracted driving behaviors related to cell phone use among middle-aged adults," *Journal of Transport & Health,* vol. 2, no. 3, pp. 434-440, 9//, 2015.

[16] Furnell, S., "Assessing password guidance and enforcement on leading websites," *Computer Fraud & Security,* vol. 2011, no. 12, pp. 10-18, 2011.

[17] Gao, H., Ma, L., Jia, W., and Ye, F., "Multiple password interference in graphical passwords," *Int. J. Inf. Comput. Secur.,* vol. 5, no. 1, pp. 11-27, 2012.

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

[19] Harbach, M., Von Zezschwitz, E., Fichtner, A., De Luca, A., and Smith, M., "It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception," *Symposium on usable privacy and security (SOUPS)*, pp. 213-230, 2014.

[20] Harris, R. A., "Chapter 8 - Crafting Voice Interfaces," *Voice Interaction Design*, pp. 203-222, San Francisco: Morgan Kaufmann, 2005.

[21] Herley, C., "So long, and no thanks for the externalities: the rational rejection of security advice by users," *Proceedings of the 2009 workshop on New security paradigms workshop*, pp. 133-144, 2009.

[22] Herzberg, A., and Margulies, R., "Training Johnny to Authenticate (Safely)," *Security & Privacy, IEEE,* vol. 10, no. 1, pp. 37-45, 2012.

[23] Hevner, A. R., March, S. T., Park, J., and Ram, S., "Design Science in Information Systems Research," *Management Information Systems Quarterly,* vol. 28, no. 1, 2004.

[24] Horcher, A.-M., and Tejay, G. P., "Building a better password: the role of cognitive load in information security training," *Proceedings of the 2009 IEEE international conference on Intelligence and security informatics* pp. 113-118, 2009.

[25] Horcher, A.-M., Tejay, G., and Cohen, M., "Poster: Mobile Security for Dummies: Designing Mobile Security Interfaces for the Non-Expert," *Computer,* vol. 12, pp. 16, 2014.

[26] John, B. E., "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.

[27] Kao, P.-C., Higginson, C. I., Seymour, K., Kamerdze, M., and Higginson, J. S., "Walking stability during cell phone use in healthy adults," *Gait & Posture,* vol. 41, no. 4, pp. 947-953, 2015.

[28] Keith, M., Shao, B., and Steinbart, P. J., "The usability of passphrases for authentication: An empirical field study," *International Journal of Human-Computer Studies,* vol. 65, no. 1, pp. 17-28, 2007.

[29] Laatar, R., Kachouri, H., Borji, R., Rebai, H., and Sahli, S., "The effect of cell phone use on postural balance and mobility in older compared to young adults," *Physiology & Behavior,* vol. 173, pp. 293-297, 2017.

[30] Leftheriotis, I., "User authentication in a multi-touch surface: a chord password system," *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, pp. 1725-1730, 2013.

[31] Li, F. C. Y., Guy, R. T., Yatani, K., and Truong, K. N., "The 1line keyboard: a QWERTY layout in a single line," *Proceedings of the 24th annual ACM symposium on User interface software and technology*, pp. 461-470, 2011.

[32] Li, H., Liu, Y., Liu, J., Wang, X., Li, Y., and Rau, P.-L. P., "Extended KLM for mobile phone interaction: a user

study result," *CHI '10 Extended Abstracts on Human Factors in Computing Systems* pp. 3517-3522, 2010.
[33] Lim, J., Amado, A., Sheehan, L., and Van Emmerik, R. E. A., "Dual task interference during walking: The effects of texting on situational awareness and gait stability," *Gait & Posture,* vol. 42, no. 4, pp. 466-471, 10//, 2015.
[34] Lipovac, K., Đerić, M., Tešić, M., Andrić, Z., and Marić, B., "Mobile phone use while driving-literary review," *Transportation Research Part F: Traffic Psychology and Behaviour,* vol. 47, pp. 132-142, 5//, 2017.
[35] Morris, R., and Thompson, K., "Password security: A case history," *Communications of the ACM,* vol. 22, no. 11, pp. 594-597, 1979.
[36] Muttart, J. W., Fisher, D. L., Knodler, M., and Pollatsek, A. "Driving Without a Clue: Evaluation of Driver Simulator Performance During Hands-Free Cell Phone Operation in a Work Zone."
[37] Mwakalonge, J., Siuhi, S., and White, J., "Distracted walking: Examining the extent to pedestrian safety problems," *Journal of Traffic and Transportation Engineering (English Edition),* vol. 2, no. 5, pp. 327-337, 2015.
[38] Myers, B. A., "Using handhelds for wireless remote control of PCs and appliances," *Interacting with Computers,* vol. 17, no. 3, pp. 251-264, 2005.
[39] Nasar, J., Hecht, P., and Wener, R., "Mobile telephones, distracted attention, and pedestrian safety," *Accident Analysis & Prevention,* vol. 40, no. 1, pp. 69-75, 1//, 2008.
[40] Oberheide, J., and Jahanian, F., "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.
[41] Ocak, N., and Cagiltay, K., "Comparison of Cognitive Modeling and User Performance Analysis for Touch Screen Mobile Interface Design," *International Journal of Human–Computer Interaction*, pp. 1-9, 2016.
[42] Orphanides, A. K., and Nam, C. S., "Touchscreen interfaces in context: A systematic review of research into touchscreens across settings, populations, and implementations," *Applied Ergonomics,* vol. 61, pp. 116-143, 5//, 2017.
[43] Oulasvirta, A., Reichel, A., Li, W., Zhang, Y., Bachynskyi, M., Vertanen, K., and Kristensson, P. O., "Improving two-thumb text entry on touchscreen devices," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2765-2774, 2013.
[44] Pinkas, B., and Sander, T., "Securing passwords against dictionary attacks," in Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, 2002.
[45] Poremba, S. M. "How a Single Username Puts Your Security at Risk."
[46] Riva, O., Qin, C., Strauss, K., and Lymberopoulos, D., "Progressive Authentication: Deciding When to Authenticate on Mobile Phones," pp. 301–316, 2012, 2012.
[47] Sandnes, F. E., "Reflective Text Entry: A Simple Low Effort Predictive Input Method Based on Flexible Abbreviations," *Procedia Computer Science,* vol. 67, pp. 105-112, 2015/01/01, 2015.
[48] Saxby, D. J., Matthews, G., and Neubauer, C., "The relationship between cell phone use and management of driver fatigue: It's complicated," *Journal of Safety Research,* vol. 61, pp. 129-140, 6//, 2017.
[49] Schwebel, D. C., Stavrinos, D., Byington, K. W., Davis, T., O'Neal, E. E., and de Jong, D., "Distraction and pedestrian safety: How talking on the phone, texting, and listening to music impact crossing the street," *Accident Analysis & Prevention,* vol. 45, pp. 266-271, 3//, 2012.
[50] Serrano, M., Lecolinet, E., and Guiard, Y., "Bezel-Tap gestures: quick activation of commands from sleep mode on tablets," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 3027-3036, 2013.
[51] Shirazi, A. S., Henze, N., Dingler, T., Kunze, K., and Schmidt, A., "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.
[52] Singha, J., Misra, S., and Laskar, R. H., "Effect of variation in gesticulation pattern in dynamic hand gesture recognition system," *Neurocomputing,* vol. 208, pp. 269-280, 10/5/, 2016.
[53] Stobert, E., and Biddle, R., "Memory retrieval and graphical passwords," *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pp. 1-14, 2013.
[54] Theofanos, M. F., and Pfleeger, S. L., "Shouldn't All Security Be Usable?," *IEEE Security & Privacy,* vol. 9, no. 2, pp. 12-17, 2011.
[55] Topkara, U., Atallah, M. J., and Topkara, M., "Passwords decay, words endure: secure and re-usable multiple password mnemonics," *Proceedings of the 2007 ACM symposium on Applied computing*, pp. 292-299, 2007.
[56] Trinh, H., Waller, A., Vertanen, K., Kristensson, P. O., and Hanson, V. L., "Phoneme-based predictive text entry interface," *Proceedings of the 16th international ACM SIGACCESS conference on Computers & accessibility*, pp. 351-352, 2014.
[57] United States Figure Skating Association, *The official book of figure skating*: Simon & Schuster, 1998.
[58] Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., and Eugene Schultz, E., "Improving password security and memorability to protect personal and organizational information," *International Journal of Human-Computer Studies,* vol. 65, no. 8, pp. 744-757, 2007.
[59] West, J., and Mace, M., "Browsing as the killer app: Explaining the rapid success of Apple's iPhone," *Telecommunications Policy,* vol. 34, no. 5-6, pp. 270-286, 2009.
[60] Withana, A., Peiris, R., Samarasekara, N., and Nanayakkara, S., "zSense: Enabling Shallow Depth Gesture Recognition for Greater Input Expressivity on Smart Wearables," *Proceedings of the 33rd Annual*

ACM Conference on Human Factors in Computing Systems, pp. 3661-3670, 2015.

[61] Zezschwitz, E. v., Dunphy, P., and Luca, A. D., "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.

[62] Zhu, M., Rudisill, T. M., Heeringa, S., Swedler, D., and Redelmeier, D. A., "The association between handheld phone bans and the prevalence of handheld phone conversations among young drivers in the United States," *Annals of Epidemiology,* vol. 26, no. 12, pp. 833-837.e1, 2016.