2018

Conservation of Limited Resources: Design Principles for Security and Usability on Mobile Devices

Ann-Marie Horcher
Nova Southeastern University, horcheram@gmail.com

NSUWorks Citation

Ann-Marie Horcher. 2018. *Conservation of Limited Resources: Design Principles for Security and Usability on Mobile Devices.* Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1028) https://nsuworks.nova.edu/gscis_etd/1028.

Conservation of Limited Resources: Design Principles for Security and Usability on Mobile Devices

by

Ann-Marie Horcher

A dissertation submitted in partial fulfillment of the requirements
For the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

March 1, 2018

We hereby certify that this dissertation, submitted by Ann-Marie Horcher, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Gurvirender Tejay, Ph.D.
Chairperson of Dissertation Committee

03/01/18
Date

Ling Wang, Ph.D.
Dissertation Committee Member

03/01/18
Date

Maxine S. Cohen, Ph.D.
Dissertation Committee Member

3/1/2018
Date

Approved:

Yong X. Tao, Ph.D., P.E., FASME
Dean, College of Engineering and Computing

3/1/2018
Date

College of Engineering and Computing
Nova Southeastern University

2018

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Conservation of Limited Resources: Design Principles for Security and Usability on Mobile Devices

by

Ann-Marie Horcher

Abstract

Mobile devices have evolved from an accessory to the primary computing device for an increasing portion of the general population. Not only is mobile the primary device, consumers on average have multiple Internet-connected devices. The trend towards mobile has resulted in a shift to “mobile-first” strategies for delivering information and services in business organizations, universities, and government agencies. Though principles for good security design exist, those principles were formulated based upon the traditional workstation configuration instead of the mobile platform. Security design needs to follow the shift to a “mobile-first” emphasis to ensure the usability of the security interface.

The mobile platform has constraints on resources that can adversely impact the usability of security. This research sought to identify design principles for usable security for mobile devices that address the constraints of the mobile platform. Security and usability have been seen as mutually exclusive. To accurately identify design principles, the relationship between principles for good security design and usability design must be understood. The constraints for the mobile environment must also be identified, and then evaluated for their impact on the interaction of a consumer with a security interface.

To understand how the application of the proposed mobile security design principles is perceived by users, an artifact was built to instantiate the principles. Through a series of guided interactions, the importance of proposed design principles was measured in a simulation, in human-computer interaction, and in user perception. The measures showed a resounding difference between the usability of the same security design delivered on mobile vs. workstation platform. It also reveals that acknowledging the constraints of an environment and compensating for the constraints yields mobile security that is both usable and secure. Finally, the hidden cost of security design choices that distract the user from the surrounding environment were examined from both the security perspective and public safety perspective.

Acknowledgements

When I started my first class at Nova Southeastern University, my first professor said, "When you do research you stand on the shoulders of giants." My second professor said, "Research is fun." They were both right. In my journey towards my degree I have done my share of standing tall and having fun. There were people who walked beside me and guided my way

My thanks goes first to my advisor Dr. Gurvirender Tejay. His grasp of theory and method challenged me to create my best work. Even when I was most frustrated by feedback, I knew that he was pushing me past what I would have done on my own. My committee members, Dr. Maxine Cohen and Dr. Ling Wang each provided expertise in their areas. Dr. Cohen introduced me to the intersection between HCI and security. When I heard the concept "usable security" I knew I had found my research niche. Dr. Wang provided input on data gathering and analysis. She acknowledged all the interesting and distracting tangents my research uncovered, while still keeping me focused on the target. I thank her as much for what she took out of the analysis as for what she put in.

I would also like to thank my peer mentor, Dr. Laura Downey and my family, particularly my sister, Fran Horcher, and my daughters, Kate-Alice and Mona Martin. Seeing myself through their encouraging eyes kept me going. They, and the "MG" kept things going when I couldn't do it on my own.

The SOUPS community has been a research home for me, providing encouragement and inspiration. In particular I thank Dr. Lorrie Faith Cranor, Dr. Simson Garfinkel, Dr. Rick Wash, and Mary Ellen Zurko.

The late Dr. Aimee Tabor, and the attendees of the WISE seminar provided me with early feedback on my research ideas, and participated in my pilot studies. Every summer I spent with them took me a giant step forward toward my goal.

Last I would like to thank my colleagues at Central Michigan University who supported me in the final part of my journey.

Table of Contents

Chapters

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

1.1 Introduction and Problem Statement

Access to digital information is no longer reserved to an elite minority of scholars and businesses—the Internet has put access in hands of the general public (Yang & Zhiyong, 2010). From environmental information to e-government services to phone directories, information delivery and interaction has shifted from print to exclusively electronic (Kirk, Chiagouris, & Gopalakrishna, 2011). The accelerated movement of service to e-only delivery makes technology a necessity for all instead of a non-essential luxury item (Kim, Lee, & Menon, 2009).

Increasingly, mobile devices have moved from being companion devices of a computer workstation (Myers, 2005) to being the primary or stand-alone device for digital information access (West & Mace, 2009). Computer crime, already a problem on the traditional workstation (Brenner, 2007; Lawton, 2007), has followed computer users to the mobile platform (Salerno, Sanzgiri, & Upadhyaya, 2011). A mobile computing platform provides challenges in security that differ from the traditional computing workstation (Oberheide & Jahanian, 2010), and the structured work environment (Green, 2007). The challenges include designing sufficiently usable security to match the needs and capabilities of the users of these devices.

1.2 Problem Statement and Argument

The research objective is to identify effective principles to design usable security for mobile devices. Principles exist for achieving a good security design for information systems (Saltzer & Schroeder, 1975), as well as for usability design of information systems (Shneiderman et al., 2016). These principles do not exist in a consolidated framework, making the application of either one (Boivie, Gulliksen, & Göransson, 2006) or both in a coordinated effort uncommon (Rehman & Mustafa, 2009). Furthermore, these principles were developed for information systems in the context of a stationary workstation instead of the mobile devices (Botha, Furnell, & Clarke, 2008). The two environments are significantly different in application design capabilities as well as hardware (Burigat, Chittaro, & Gabrielli, 2008). The design of security on the mobile device is equally impacted by the platform and hardware of mobile devices as are other applications (Oberheide & Jahanian, 2010). Usable security is demanded by the typical user community of mobile devices for e-banking and other financial applications (Weir, Douglas, Richardson, & Jack, 2010).

To effectively design these principles, attention must be paid to the effort required of the user to follow security (Yuan, Archer, Connelly, & Zheng, 2010), appropriate security for the value of the information (Grawemeyer & Johnson, 2011) , and the resource constraints of the devices in terms of physical form factors (Mittal & Sengupta, 2009) and device capabilities (Shih & Wang, 2011).

The key to satisfying these needs is design that unifies both security and usability principles (Cranor & Garfinkel, 2005). Systems designed with security and usability principles remain more secure, because the users do not circumvent security for functionality (Albrechtsen & Hovden, 2009).

Security is frequently an add-on (Baskerville, 1993). Usability is similarly an add-on (Garfinkel, 2005). In both cases, the lack of integration of security and usability into the bedrock of the design makes both less effective.

Beyond this similar disrespect, there is a deeper relationship between security and usability. Lack is of usability is a form of security (Sasse, Brostoff, & Weirich, 2001). The most secure system is one that never breached, but not necessarily used. The reverse can also be true: the removal of complicated security protocols can make a system extremely usable. System design can turn into a tug-of-war between the two extremes, with many systems designers choosing to trade off usability for security and vice versa (Faily & Flechais, 2010).

Closer examination of secure design principles, such as those proposed by Saltzer and Schroeder (1975), and usability principles documented by Shneiderman et al. (2016), may reveal a relationship between security and usability principles. For example, a streamlined design with an efficient interface can offer both good security and high usability, if it is possible to follow a combined set of design principles.

Security that is designed with usability does not trigger users' natural aversion to systems that make them trade off functionality for security (Stanton, Stam, Mastrangelo, & Jolton, 2005). One of the ways used to address the aversion to confusing security measures is security awareness training (Horcher & Tejay, 2009; Shaw, Chen, Harris, & Huang, 2009). For the non-organizational user of mobile devices, there is no formal oversight or compensating training (Poole, Chetty, Morgan, Grinter, & Edwards, 2009). The user depends upon an informal network of resources of varying quality and security knowledge.

1.3 Contribution to the Body of Knowledge – Dissertation Goal

While security and usability have been addressed, both separately and together, the previous focus has been on conventional workstations (Oberheide & Jahanian, 2010) or specific instances of mobile security (Weir, et al., 2010). Instead of a case by case basis, this study proposes a series of design principles that apply across mobile devices as a group.

Garfinkel (2005) most clearly documented the gap in the literature on secure and usable design. Garfinkel proposed the use of design patterns for secure operations. These patterns, such as “least surprise” and “disable by default” are almost too simple to be respected. The common sense of using good defaults is most obvious in hindsight. The dissertation also calls for new defaults to address the burgeoning need for combined security and usability on mobile platforms. Patterns are a step towards understanding security as a dimension of usability and vice versa.

1.4 The Importance of the Research Problem

Usability in information system security design reduces the effort needed to follow secure practices, similar to how usability reduces the effort to use websites and even items of a user’s normal environment (Norman, 2004). Users typically choose functionality over security when security becomes a barrier to getting the job done (Albrechtsen & Hovden, 2009); therefore, adding usability to a security design should reduce the need to choose functionality over security (Furnell, 2008). A combined security-usability design framework reduces the effort needed to add security, and security designer does not choose security functionality over system usability (Whitten & Tygar, 1999).

1.4.1 The Challenge of Usability

Computer systems have moved outside the context of business and research organizations to become an essential part of the home (Mazurek et al., 2010). In the home the traditional support structure, with a dedicated Information Technology expert, is not the norm (Poole et al., 2009). For the home user, there are no organization resources to compensate for difficult security. Too much security and the users run the risk of not having access to their own devices. The home user seeks informal support through a personal network, or systems that provide a highly positive user experience with usability, such as the Apple iPhone (Arruda-Filho, Cabusas, & Dholakia, 2010), and need less support.

1.4.2 Dealing with More Devices per User

Mobile devices have increased the convenience of computing, and also the variety of an individual user's computing experience (Oulasvirta & Sumari, 2007). A typical information worker may manipulate a laptop, a cell phone, several hard drives, and a portable music player in the course of the work day (gAshbrook & Lyons, 2010). Each device adds a degree of complexity with its own security mechanism and information management structure.

The interoperability of multiple mobile devices through a network can improve the sharing of information (Walker, Stanton, Jenkins, & Salmon, 2009). Ebook readers such as the Amazon Kindle and the Barnes & Noble Nook have used this interoperability to move content seamlessly between platforms and increase user acceptance through usability (Horcher & Cohen, 2011). Though ebooks and ebook readers had been available for over a decade, surmounting the content acquisition barrier with a common repository in the cloud, and a non-intrusive authentication mechanism made the media and devices accessible to a wider community. Applying consistent usability-security could induce the same user satisfaction and acceptance of security on the multiple mobile devices.

1.4.3 More Sensitive Information on Mobile

Mobile devices have become so multi-functional that access controls are needed to protect the users' information on the device, and provide secure authentication to the systems interfaced to by the device (Pasquinucci, 2009). To provide the ease of use needed for user adoption, these controls must take into account the in-motion environment where the device will be used (Barnard, Yi, Jacko, & Sears, 2005, 2007; Chang, 2010) and the form factors of the mobile device (Chang, 2010). Instead of simply transferring methods designed for the form factors of a standard-sized keyboard and screen, the security methods need to optimize and exploit the capabilities of the device (Botha et al., 2008).

The current authentication mechanisms such as the PIN or complex passwords, which are exponentially more difficult to input on the mobile keyboard, generate increased user pushback and induce the typical trade-off between functionality and security (Furnell, Clarke, & Karatzouni, 2008). Since the portability of the device makes loss more probable, plus the increasing value of the information stored on mobile devices and the increasing dependence of users on their mobile devices, the loss or compromise of mobile devices has financial, reputation, and emotional repercussions (Chen & Katz, 2009).

The mismatch of traditional security procedures with mobile capabilities is typical of design that is not centered on the human element. Understanding how humans interact with the device in an anthropometric context, which includes hand size, dexterity, and gender (Bylund & Burström, 2006), and situational context (e.g., in-motion, while performing other device activities) is key to determining which current authentication methods are optimal for mobile devices and what human-centered design elements affect securing mechanisms (Hwang, Cho, & Park, 2008).

In addition to the proliferation of computing devices, the resource-constraints of mobile devices have further complicated the design of both security and usability. Unlike desktop workstations, every micrometer of internal space, every inch of screen real estate, and every amp of power is at a premium (Rahmati & Zhong, 2009).

1.5 Scope and Definitions of Terms

The following terms are used for this study.

- *Information Security:* A well-informed sense of assurance that information risks and controls are in balance (Anderson, 2003). Risks are based on the context of the information. What is secure in a small organization may not be in a large organization. Keeping the controls in balance speaks to the trade-off between security and accessibility. The “well-informed sense” requires the implementation of controls using a deep understanding of the goals of the organization or situation being protected.
- *Information System:* All information handling activities at the technical, formal and informal levels of an organization (Liebenau & Backhouse, 1990). Formal levels of an organization are marked by regulation and explicit consequences.

Information handling done by imitation or unconscious observation is at an informal level. Explicit transfer of information from teacher to student is typical of technical information handling.

- *Mobile Devices:* mobile devices refers to hand-held cellular communication devices. These devices primarily consist of smart phones and tablets. Mobile devices not included are laptop computers, portable hard drives, USB thumb drives, and portable music players (Hosmer et al., 2011).
- *Usability:* the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use (Jokela, Iivari, Matero, & Karukka, 2003).
- *Security-usability (or usable security):* usability that relates specifically to the security interface (Cranor and Garfinkel, 2005).

1.6 Research Questions

This study has two specific research questions that seek to address how to better design usable security for mobile devices. The first research question is:

Research Question 1 – How does the overlap or conflict between security and usability impact the design of effective usable security on mobile devices?

Design principles for usability are well-known within the HCI community. Security design principles are lesser known both within the HCI community and the security community. Even less acknowledged is the difference between usability of the security component of a system or device, and the usability of primary components of the system or device.

Another concern is whether it is possible to apply a new set of design principles in an effective way; therefore, the second research question is:

Research Question 2 – Will a set of design principles structured to conserve constrained resource attain security usability?

Approaching this question creates a need to define meaningful measures of usability and security.

1.7 Structure of the Dissertation

This dissertation is organized into five main chapters: introduction, literature review, research methodology, results and discussion. The introduction is the first chapter of this dissertation and provides an introduction to the proposed study. Topics addressed in the introduction include why usability and security should be researched as a combination and why the mobile platform is of significance. Next, the research problem is presented along with the underlying argument, its relevancy and its significance for research. The research questions are then presented and discussed along with how the research questions support the research problem. A brief set of definitions follows. Finally a review of the overall structure of this dissertation is presented.

The next chapter of the dissertation reviews the research literature that is relevant to usability and security. First previous work in security design is reviewed. Then usability research related to form factors is discussed. The difference between mobile vs. fixed computing environments in terms of security design is discussed, followed a summary of user behavior research related to security and functionality.

The review of literature chapter then discusses what is known about human computer interfaces on mobile devices, security and mobile devices, and the gaps in the extant literature. Once the gaps are clearly identified then the significant contributions this research makes to the existing body of knowledge is presented. This chapter concludes with a brief summary.

The next chapter of the dissertation presents the research methodology and theoretical basis for the study. The research methodology begins with an overview of design science research as it was originally conceived (Hevner, March, Park, & Ram, 2004) and how design science research has been applied in recent studies (Venable, 2010). A high level view of the research method is outlined with the steps required to accomplish the research study.

The fourth chapter of the dissertation presents the results of the study. The demographic information about participants is covered. The results section is divided into the three phases that were described in the methodology, with the hypotheses that were evaluated in each individual phase linked to their results.

The final chapter discusses the meaning of the results, the importance of the results, and the contribution to the literature. Future research suggested by the results is also discussed.

Chapter 2

Review of the Literature

The review of literature is comprised of four sections that provides the theoretical basis for this study. The first section reviews the current state of security design and best practices. The next section reviews the current research in human computer interfaces (HCI). The third section reviews the differences and challenges in developing for the mobile platform, particularly in the area of resource conservation. Finally, the fourth identifies the gap in the literature that this study attempts to address.

2.1 Security Design

The need for new security techniques to address the brave new reality of mobile and pervasive computing has several root causes (Oberheide & Jahanian, 2010). In some cases the lessons learned from desktop security are just as valid for the mobile platforms. In others the new platform has challenges due to resource constraints that make a classic technique inappropriate.

After a series of studies in the early nineties Baskerville (1993) proclaimed human error was the greatest problem in security. These studies also show the reluctance of companies and individual users to reveal mistakes that caused security breaches. The evidence continues to suggest that humans are not getting smarter about computers and security (Flechais & Sasse, 2009). Designing for this weakest link in the security structure yields a better result than training the human to exhibit less usable behavior (Ng, Kankanhalli, & Xu, 2009; Sasse et al., 2001). Using a checklist can predict vulnerabilities in systems (Farahmand, Navathe, Enslow, & Sharp, 2003), but usability can pre-dispose a system to have less incidents.

Modeling languages to represent security requirements have been proposed to streamline the design process (Hatebur, Heisel, Jorjens, & Schmidt, 2011). Giving designers a language to express security design concepts improves communication in the design process. Another approach is to create security monitoring devices that are more usable (Davies & Tryfonas, 2009). Instead of requiring the security practitioner to engineer the scan through a series of command line prompts, the interface presents in a web browser with full-screen output.

2.2 Human Computer Interface (HCI) for Mobile Devices

Waves of new technology bring an accompanying amnesia of human-centered design principles. Human-centered design, instead of technology-centered design, will produce devices that will be accepted, effective, and even loved by the owner, because they satisfy a functional need and elicit an emotional response (Norman, 2004). Mobile and wearable devices have become a part of everyday life to the point where an individual is emotionally dependent on the device (Chen & Katz, 2009), and financially dependent on the security of the device (Hwang et al., 2008).

Acceptance and usability of mobile/wearable devices depends on design based on user requirements accurately reflecting human interaction with the device, even where the population is not homogeneous. Gender, age, and capability differences drive how humans interact with devices, including mobile and wearable devices (Schwanen, Kwan, & Ren, 2008). “One size fits all” is particularly ineffectual in biometric-based applications (Hunter, 2004). Similarly, requirements for mobile and wearable need to reflect physical and particularly biometric differences where those differences affect key design components.

2.2.1 HCI and mobile device usage

Current research on mobile device design is centered on the functionality of the internals of the mobile device, as opposed to the form factors of the external device. College students are a mobile population with high dependency on their mobile devices (Chen & Katz, 2009). Mobile devices provide direct and private communication that is easily available because the device is carried on their person. Similarly, the features that college students prize in their mobile devices extend past communication to auxiliary activities like email, music players, organization and reminder activities, and even style (Economides & Grousopoulou, 2009). The trend continues to evolve toward combining individual electronic devices into one multi-functional device that retains a compact footprint.

College students show some gender differences on mobile device usage. In particular, the female respondents were less concerned about price (Economides & Grousopoulou, 2009). The buying power of women is a significant factor in the economy, as women have become the largest growing market of consumers. Designing products that appeal to women’s need to simplify, or reclaim time, is an economic advantage (Silverstein, Sayre, & Butman, 2009).

Similarly, the functionality requirements of the mobile professional have been assessed (Gebauer, 2008). The functionality of mobile devices, even with usability issues, was preferred over the non-mobile counterpart. Using the task technology fit (TTF) theory, Gebauer (2008) mapped the task to its non-mobile equivalent to measure how well the device performed. The results actually showed a mutation of the task when in the mobile environment, with the users performing the tasks for different reasons, and in a different manner. The form factors of weight and size, which are not the focus of the TTF theory, play a prominent role in the success and user acceptance of the device.

The need for specialized versions of tools in the mobile environment also creates a disparity with the non-mobile equivalent (Economou, Gavalas, Kenteris, & Tsekouras, 2008). The authoring tools of the non-mobile platform need special versions to be able to create applications at all, and in particular ones that suit the smaller keyboard, lower processing speed and limited storage of the mobile device. In some ways it is the equivalent of returning to the early days of computing when every byte of storage was rationed, and every computing cycle was optimized to use the least amount of processing.

Tourist information, mapping, and global positioning satellite (GPS) applications (Kenteris, Gavalas, & Economou, 2009) are capabilities most needed by uses who uses the mobile device to navigate in real time, while acquiring new information about the surrounding environment. The concept of the mobile web browser was originally proposed for the Apple Newton PDA in 1995 (Gessler & Kotulla, 1995). Looking at the design objectives, or requirements for the future device based on that more primitive device, shows the value of abstracting the design objectives for future re-use.

Besides navigational information, the mobile professional also has an evolving need to be able to tap into personal information repositories when on the move (Karypidis & Lalis, 2007), without acquiring the overhead of synchronization and file management. The Omnistore software is one of the solutions proposed to handle this challenge, as mobile professionals continue to create a personal area network with information moving between laptops, desktops, and small form factor mobile devices (Karypidis & Lalis, 2007). Research on mobile devices also has included the head-mounted devices (HMD), as well as laptop and PDA combinations (Serif & Ghinea, 2008). The research had participants performing real-life tasks in "realistic scenarios," but not actually as part of daily life. The environment was pre-configured to have Wi-Fi blankets readily available as opposed to the current norm of isolated Wi-Fi hotspots.

Beyond the actual applications, the mobile device presents challenges for readability, which is linked both to physical screen size, and processing power deliverable in a the compact format (Dennler et al., 2007). Larger screen sizes and more processing create a greater drain on battery power, particularly conventional lithium-ion battery power (Min, Cha, & Ha, 2009). The development of solar fuel cells have the twin advantages of reducing the weight of the device because they are thinner, and improving the battery life by the recharging in the mobile environment from a widely available energy source (Dennler, et al., 2007). Oquist and Goldstein (2003) used readability formula rapid serial visual presentation (RSVP) to propose an alternate presentation of text on the screen to improve readability. Instead of the eye moving across the screen, the text appears in discernible chunks anticipating the readers' consumption rate. Movement of the eye is a factor in balance, which is particularly relevant to mobile devices being used while in motion (Barnard, et al., 2005).

2.1.2. HCI and Gender Differences

In the human-computer interaction studies of mobile devices, the focus has been specific functionalities such as hand positions (Wobbrock, Myers, & Aung, 2008). However, gender differences are frequently noted in the studies, as in preferences of older women for haptic and older men for tactile interface (Kurniawan, 2008). With the current devices so heavily based on manual interaction, the gender differences in physicality become significant.

Gender differences in hand shape and strength affect the performance of manual tasks (Bylund & Burström, 2006; Clerke, Clerke, & Adams, 2005; Crosby & Wehbé, 1994; Talsania & Kozin, 1998). Even in a pre-pubertal population, handgrip strength was predictable along gender lines (Jürimäe, Hurbo, & Jürimäe, 2009), showing boys and girls of similar ages and height still differed significantly in forearm strength. In addition to hand strength and shape, the predilection to carpal tunnel, osteoarthritis and other medically handicapping conditions also shows a gender difference (Boz, Ozmenoglu, Altunayoglu, Velioglu, & Alioglu, 2004; Xu et al., 1998), where the hand strength anthropometric norm of females became a risk factor for developing carpal tunnel syndrome (CTS) and osteoarthritis.

Beyond gender differences in body parts, there are also differences in how men and women interact with mobile devices due to gender norms in processing visual information (Kimchi, Amishav, & Sulitzeanu-Kenan, 2009). As information is presented on a small screen in a compact format, optimizing the perception of the mobile user either by device physical design, or software design pays off in user satisfaction.

The pattern of Internet-connected activities also shows gender differences (Ren & Kwan, 2009), with women performing a much higher percentage of maintenance-related tasks, over leisure tasks as compared to men. In addition, the locale of everyday activities varies between the genders (Schwanen et al., 2008). Women traditionally have a higher responsibility for household and care giving, and their time available for

Internet-connected tasks is fragmented. Not being tied to a primary location, such as the home, provides both freedom and risk. The maintenance tasks can be performed while in transit, or waiting for another activity to commence. In addition, mobile devices must have sufficient security, as in the firewall protection typical of the home network when the devices are being used to transmit and manipulate highly private information of household finance manipulation.

The mounting evidence of gender differences points to a need for flexible interfaces that can be tailored to specific physicality of the user (Rode, 2011). The "one size fits all" design that lacks the ability for adjustment leads to HCI with one size that fits none well.

2.3 Mobile Platforms and Security

Mobile devices are becoming the technology platform of choice for most people to interact with throughout their day (Saha & Mukherjee, 2003). More than just a phone, a mobile device can be an emotional and medical lifeline (Chen & Katz, 2009; Osmani, Balasubramaniam, & Botvich, 2008). With more and more information moving to the cloud, the connectivity of the device is as important as the on-board capabilities (Buyya, Yeo, Venugopal, Broberg, & Brandic, 2009). Along with connectivity, the security capabilities of the device must protect the information being transmitted to guard an individual's privacy (Price, Adam, & Nuseibeh, 2005) and to guard against misuse by cyber-criminals (Oberheide & Jahanian, 2010).

The nature of the mobile device provides new technology challenges for providing security, and new constraints (Mancini et al., 2009). The physical form factor of mobile devices that makes them lightweight and convenient to carry also limits the size of the screen, and the size of the processor that can be put into the device. The need for portability constrains the size of the battery to power the device, and requires the battery last as long as possible (Rahmati & Zhong, 2009). Therefore, the processes on mobile devices must be designed to use the lesser computing power of a smaller processor and conserve the power used.

Along with the constraints, mobile devices typically come with additional capabilities such as global positioning systems (GPS), motion detectors (accelerometers), and voice input. This new norm of technology provides new possibilities for interacting with the devices (Bayir, Demirbas, & Eagle, 2010).

2.4 Addressing the Gap in Current Research

Though usability design principles have been extensively discusses for the workstation platform, these principles focus on the workstation platform (Shneiderman et al., 2016). The differences in workstation and mobile platforms impacts the effectiveness of workstation-based design principles when transferred to the mobile platform (Oberheide & Jahanian, 2010), particularly in area of security because security is not the primary objective of the user (Gebauer, Kline, & He, 2011), and resources are constrained on the mobile platform. Design principles that reflect the reality of mobile devices are needed for effective usable security for mobile devices.

2.5 Summary of Literature Survey

Looking across at the literature domains of security design reveals an emphasis on complexity for security strength even while the literature on user behavior indicates complexity alone fails. Human error is documented as the consistent weakest link in any security system, yet eliminating human error by design is still not the greatest emphasis in security. The difficulty of studying human behavior related is compounded by reluctance of companies and individuals to participate in security studies for fear of revealing too much truth about their behavior and creating a security vulnerability.

The HCI literature reveals that the size of screen and the manipulation of mobile interfaces create challenges in design. Differences in ability to manipulate the device based on gender and age are magnified by the smaller margin of error caused by the device size. Finally because mobile devices are not fixed in position, mobile security presents additional design challenges to achieve usable security.

Chapter 3

Research Methodology

Typically, application designers for information systems are domain experts in the primary functionality of the application, rather than security or usability (Pfleeger & Pfleeger, 2009). Design principles that guide the domain expert designer to best practices for usability and security enhance the integration of security and usability into information systems (Garfinkel, 2005). In this section, the principles for good security design and high usability, as defined in the literature, are examined for overlap and conflict. A combined framework of security-usability principles is presented as a result of mapping security and usability design principles together. Next, resources available on mobile devices are examined for possible impact on security-usability. Constrained resources specific to the mobile platform are identified, as well as the combined security-usability design principles that address conservation of those resources.

The resulting combined security-usability design principles are evaluated using a design science research (DSR) approach. An artifact consisting of a mobile application with a security interface is created by applying the new security-usability design principles. To determine how well the design of the artifact refutes or supports the hypotheses, three phases of evaluation were done. The first set of measures scores the complexity of the security interface a predictive modeling tool. The second set of measures uses an experiment where the usage of the artifact is tracked as it conserves resources on the mobile platform. The third set of measures uses a standardized usability survey to measure user satisfaction with the artifact.

Design science research solves problems in a more effective and efficient manner by creating an artifact to represent the proposed solution (Hevner, March, Park, & Ram, 2004). Because of the nature of many design-research problems, an optimal solution may not always be possible (Simon, 1996). A designer instead searches through available alternatives until an acceptable alternative, or satisficing is found. Choosing the design science approach is also supported by the security-usability design principles developed for the desktop by Garfinkel (2005). Garfinkel advocated “Good Security Now,” which requires designers to search through the available solutions for the best fit at a particular point in time.

3.1 Security and Usability Design Principles Frameworks

Usability in design reduces the effort needed to use the system properly from both a physical and cognitive perspective (Shneiderman et al., 2016). When security becomes a barrier to getting the job done, users typically choose functionality over security (Albrechtsen & Hovden, 2009). Adding usability to a security design should alleviate the need to choose functionality over security (Furnell, 2008). A combined security-usability design framework reduces the effort needed to add security, which means the security designer feels less pressure to choose security functionality over system usability (Whitten & Tygar, 1999).

When designing computer security, it is important to understand what security means. Most secure design focuses on confidentiality and integrity at the expense of availability (Aiello & Ruffo, 2012). Availability makes a security asset available to the appropriate people at the appropriate times. Another way to say this is to make a security asset “usable.”

To articulate the concept of secure design Saltzer and Schroeder (1975) created nine principles. These principles, seen in Table 1, further specify what makes a system secure. At least half of the secure design principles relate directly to the interface with the user as shown in the table. As a result, "good" security design created according to these principles already includes recommendations about the interface. The "protection" and "restriction" categories contain principles that describe the functionality that should be present to ensure a secure design.

Table 1. Security Design Principles by Functionality (Saltzer & Kaashoek, 2009)

Functionality	Principle and Description
Interface	**Psychological Acceptability** Whether the user is favorably disposed
	Complete Mediation Handle all interaction to completion
	Least Common Mechanism Avoid combining multiple security objectives into the same interface. (Similar to modular code.)
	Economy of Mechanism Simple but elegant design
	Failing Secure Security error does not create a security breach
Protection	**Reluctance to Trust** Access to information, like power, corrupts.
	Never Assume that Your Secrets are Safe Even the best security can fail
Restriction	**Principle of Least Privilege** Give the user only the right access
	Separation of Privilege/duty Checks and balances to avoid too much power for one user

Similar to the security principles created by Saltzer and Schroeder (1975), the usability practitioners have the two seminal sets of heuristics or principles for design. The Golden Eight from Shneiderman et al. (2016) and ten more from Nielsen (1990) form the core of usability design. These two sets of principles have very similar statements on how to design with usability, as shown in Table 2.

Table 2. Usability Principles

Usability Principles I Shneiderman's Eight (Shneiderman, et al., 2016)	**Usability Principles II Nielsen's Ten Usability Heuristics (Nielsen & Tahir, 2001)**
Internal locus of control	User control and freedom
Shortcuts for experience	Flexibility and efficiency of use
Easy reversal of actions	Match between system and the real world
Dialog to Closure	Visibility of system status
Informative Feedback	Error prevention
	Help and documentation
Consistency	Consistency and standards
Reduce short-term memory load	Recognition rather than recall
	Aesthetic and minimalist design
Simple Error Handling	Help users recognize, diagnose, and recover from errors

These two sets of usability principles have been the cornerstone of usability research for over two decades. In addition to these usability principles, Shneiderman co-invented the Nassi-Shneiderman chart technique to represent structured programming

(Dykstra-Erickson, 2000; Nassi & Shneiderman, 1973). Similar to the usability research, the Nassi-Shneiderman structure charting techniques make the drawing of the flow of a structured program more usable than previous techniques.

Table 3. Comparing Security Design Principles to Usability Design Principles

Security Principles (Saltzer & Schroeder, 1975)	**Eight Usability Principles (Shneiderman, et al., 2016)**	**Ten Heuristics for Usability Design (Nielsen, 1990)**
Psychological Acceptability	Internal locus of control Shortcuts for experience Easy reversal of actions	User control and freedom Flexibility and efficiency of use Match between system and the real world
Complete Mediation	Dialog to Closure Informative Feedback	Visibility of system status Error prevention Help and documentation
Least Common Mechanism	Consistency	Consistency and standards
Economy of Mechanism	Reduce short-term memory load	Recognition rather than recall Aesthetic and minimalist design
Failing Secure	Simple Error Handling	Help users recognize, diagnose, and recover from errors

Nielsen’s seminal usability principles are still used as the basis of usability testing for the latest technology including mobile devices such as the Amazon Fire tablet (Nielsen, 2011). Resolution of the perceived conflict between security and usability requirements in software design has led to the development of frameworks that weigh either one or the other concept as a priority (Mairiza & Zowghi, 2010). The existence of this security-usability conflict is an ongoing theme in software design (Ben-Asher, Meyer, Moller, & Englert, 2009; Ka-Ping, 2004; Turpe, 2008).

Mapping Shneiderman et al.’s (2016) eight usability principles and Nielsen’s (1990) ten heuristics for user interface design to Saltzer and Schroeder’s (1975) security design principles as shown in Table 3, yields an interesting result. Usability principles are not in conflict with secure design principles. The chart shows each principle in the category “interface” for security parallels a usability principle or principles stated for the same concept in both Shneiderman’s usability principles and Nielsen’s ten heuristics for user interface design.

Psychological acceptability can be improved by designing a system according to user’s mental map of how the system should work, and their capabilities (Bishop, 2005). Security and usability are often labeled non-functional requirement (NFR) and, therefore, a less critical part of the software design due to security-usability illiteracy of the designer. A combined design framework reduces the effort needed by a non-expert to add security-usability.

3.1.1 Combining Security and Usability

In spite of scarcity of usability in security designs (Cranor & Garfinkel, 2005), the mapping shows that usability design principles are essentially a subset of good security design principles (Table 4). Garfinkel (2005) also included usability issues caused by

Table 4. Consolidated Principles of Security and Usability Design

Security Principles (Saltzer & Schroeder, 1975)	**Usability Principles I (Shneiderman, et al., 2016)**	**Usability Principles II (Nielsen, 1990)**	**Usability & Security (Garfinkel, 2005)**
Psychological Acceptability	Internal locus of control Shortcuts for experience Easy reversal of actions	User control and freedom Flexibility and efficiency of use Match system to the real world	Least Surprise
Complete Mediation	Dialog to Closure Informative Feedback	Visibility of system status Error prevention Help documentation	Consistent Meaningful Vocabulary
Least Common Mechanism	Consistency	Consistency and standards	Consistent Controls
Economy of Mechanism	Reduce short-term memory load	Recognition over recall Aesthetic and minimalist design	No External Burden
Failing Secure	Simple Error Handling	Help users recognize, diagnose, and recover from errors	Provide Standard Security Policies
Reluctance to Trust*, Promote Privacy* , Never Assume Secrets are Safe* Least Privilege* Separation of Privilege/duty*	Not mentioned	Not mentioned	Good Security Now*

Note. *security principles not related to usability non-users of the system (Table 4). In particular the principle “no external burden” advocates designs that do not force the user to inconvenience non-users to achieve security. Burdening a non-user who does not use the system directly, and who derives no benefit creates a high level of push-back.

In articulating these design principles, Garfinkel (2005) made a more usable framework by reducing the number from ten (Nielsen, 1990) and eight (Shneiderman et al., 2016) to six. To further reduce the analysis effort of the novice designer, Garfinkel suggested the use of design patterns to exploit the natural affinity humans have for patterns (Schmidt, Fayad, & Johnson, 1996). Creating usability and security solutions from a good model saves time and improves quality (Howarth, Smith-Jackson, & Hartson, 2009).

Garfinkel (2005) proposed usability-security design patterns for resolving suggested the use of design patterns to exploit the natural affinity humans have for patterns (Schmidt, Fayad, & Johnson, 1996). Creating usability and security solutions from a good model saves time and improves quality (Howarth, Smith-Jackson, & Hartson, 2009) and resolves common issues related to authentication, deletion of files, and management of encryption keys. Howarth, Smith-Jackson, and Hartson (2009) used a similar approach to improve the results of novice usability researchers by creating tools to resolve the typical data collection and management issues. Design patterns are also being advocated for mobile device interface (Nielsen, 1990) to address the limitations of the small screen form factor (Churchill & Hedberg, 2008).

3.1.2 *Transitioning to Mobile*

Translating security-usability principles to mobile security design patterns goes beyond ticking off items on a checklist. The current security-usability framework does not address the resource constraints upon mobile devices. Addressing the constraints yields principles more relevant to the mobile device platform. Certain principles may have more impact than others based on the user effort required to use the system if the principle is violated. Quantifying the impact of each principle on usability makes it possible to measure system usability. It also provides designers with a means of prioritizing which principles have the most impact.

Simply transferring security practices from desktop to mobile has not yielded satisfactory usability and user acceptance (Oberheide & Jahanian, 2010). In spite of this, Oberheide and Jahanian (2010) cautioned against throwing out all proven security practices. Instead they advocate an open-minded approach that keeps what works.

Ignoring certain security-usability principles in the traditional workstation environment of a business or research organization has minor consequences (Botha, Furnell, & Clarke, 2008). In risk management assessment of an information system, the vulnerabilities are weighed against the probability of the occurrence, and the loss potentially incurred from the occurrence (Azer, El-Kassas, & El-Soudani, 2009). Ignoring the resource constraints of the mobile device increases the probability of vulnerability because the practical functionality of device is compromised.

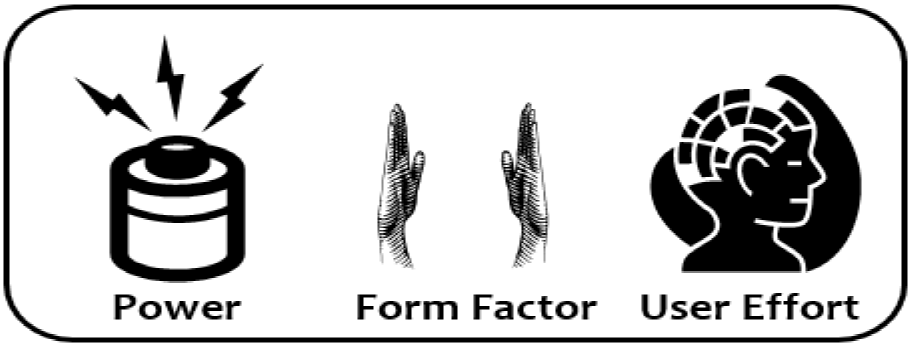


Figure 1. Resource Constraints on Mobile Devices

3.1.3 Design to Alleviate Resource Constraints

The three major resource constraints of the mobile device platform are power, form factors, and user expertise (Figure 1). To be mobile, the devices must run from a portable and renewable power source, such as a battery (Economides & Grousopoulou, 2009). The battery life is an important measure of user satisfaction. Security design that accelerates the drain of battery life reduces the usability of the device.

To be mobile the devices must be small enough and light enough to carry easily (Haverila, 2011). The screens must be big enough to use but small enough to fit in pocket or purse (Churchill & Hedberg, 2008). In addition the devices are manipulated for information gathering in a variety of settings, often while away from a formal workstation (McGibbon, Hosmer, Jeffcoat, & Davis, 2011).

In the absence of a formal organization to compensate for individual user deficiencies, the applications themselves must have reduced complexity (Churchill & Hedberg, 2008). This paper proposes a security-usability framework that prioritizes conserving the resources limited by the physical nature of the device and the expertise of the user. Usable security on the mobile device requires this resource conservation perspective over the organizational bias of previous design principles.

Revisiting the security-usability framework, seen in Figure 2, reveals five of the consolidated principles specifically address conservation of resources, which is clearly indicated by the words “Least” and “Economy.” Principles that relate to organizational objectives such as separation of power and reluctance to trust are not as relevant to the single-user mobile device, or the non-organization-based mobile device, such as a tablet shared by a family. As shown in Figure 2, certain principles align to the critical resource constraints of mobile devices**.**

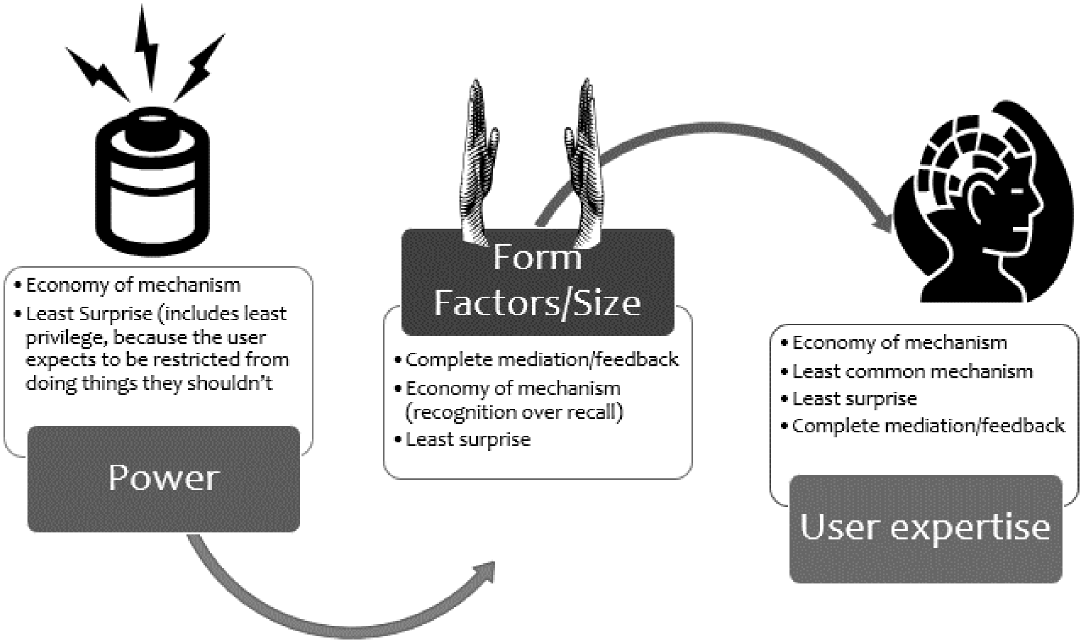

• Economy of mechanism
• Least Surprise (includes least privilege, because the user expects to be restricted from doing things they shouldn't
Power
Form Factors/Size
• Complete mediation/feedback
• Economy of mechanism (recognition over recall)
• Least surprise
• Economy of mechanism
• Least common mechanism
• Least surprise
• Complete mediation/feedback
User expertise

Figure 2**.** Design Principles Related to Resources

"Economy of Mechanism" relates to all three areas of resource constraint. The result of mapping resource constraints to the design principles is a framework that prioritizes conservation of resources, as seen in Table 5. This framework can be used as a starting point to create measures that quantify the energy and effort expended by the user, and by the system.

The concept of simplification for good security design is also supported by the most recent work from security pioneer Jerome Saltzer. The difficulty of maintaining security on a complex group of systems with competing security protocols led to the proposal of "Minimize secrets" as an additional security principle (Saltzer & Kaashoek, 2009; Smith, 2012). Every secret increases a system's administrative burden. In the case of self-managed security like a mobile device, the burden falls upon the user. Consequently, user effort has already been confirmed as a constrained resource.

Table 5. Proposed Security-Usability Principles for Resource-Constrained Devices

Security Principle	Usability Principle Manifestation
Least Surprise	User in control (flexibility and reversibility) Shortcuts for experience Match between system and real world
Complete Mediation	Visibility of system status Dialog to closure Informative Consistent Feedback Error prevention and Help
Least Common Mechanism	Consistency and standards in security policy Consistency and standards in placement of information (look-and-feel)
Economy of Mechanism	Reduce cognitive load Recognition rather than recall Aesthetic and minimalist design
Principle of Least Privilege	Good Security Now Limit Functionality/Access to Reduce Complexity

3.2 Design Science Research Methodology

To validate the combined security-usability principles for mobile devices proposed in the previous section, this study uses design science research (DSR) methodology. Design research (DR) is research into or about design. DSR is research using design as a research method or technique (Hevner et al., 2004). DSR methodology has a series of steps that result in specific outputs (Figure 3). It can be an iterative process, as information from an evaluation influences the design of another element (Vaishnavi & Kuechler, 2004).

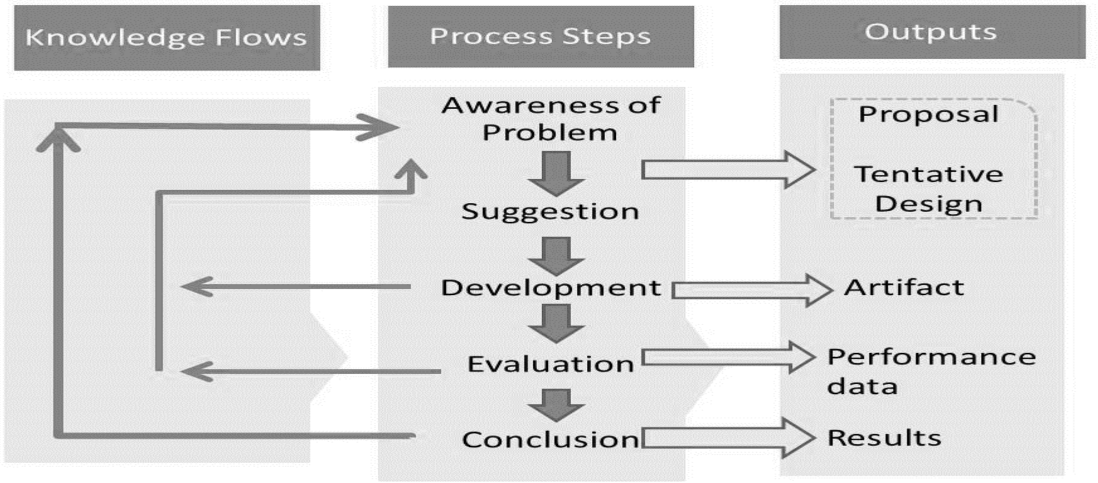


Figure 3. Steps in DSR Methodology (Hevner et al., 2004)

3.2.1 Awareness of Problem: Design Principles Needed for Mobile Devices

As discussed in 3.1.2, Transitioning to Mobile, the design principles for security-usability have not effectively transferred from workstation to mobile. The proposed security-usability principles address the issues that are at the heart of the incompatibility. An artifact that is designed with these principles should demonstrate a higher level of security-usability.

In applying the design principles to increase the security-usability, the artifact should mitigate the normal resistance behavior of users to security (Virginia Tech, 2011). Security is not the main goal of the user, and security challenge is seen as an interruption of progress toward the desired task (Pfleeger & Caputo, 2012). For example, a mobile user does not unlock a phone because they want to use the unlocking mechanism; they unlock the phone to answer it. The interruption of a task makes the primary task take longer to complete and lowers the quality of the result (Lenox, Pilarski, Leathers, & 2012). Unusable security can prove so repulsive to a user that the user may make the choice to stop using the device to avoid the experience (Theofanos & Pfleeger, 2011).

In the mobile environment where users primarily manage their devices outside the confines of an organization, the effect of resistance to security is not mitigated by formal policies, or security awareness training (Barkhuus & Polichar, 2011). Neither is there an information technology department to support the user in resolving security interface issues. As discussed in Chapter 2, this puts a greater burden on the user to gain the expertise to navigate less usable security interfaces.

The most common security interface for Internet sites uses password and user identifier authentication, also known as basic authentication (Chiasson, Forget, Stobert, Oorschot, & Biddle, 2009). The manner in which basic authentication is currently encountered by mobile device users creates a situation where failure is not only common, but inevitable. The average user has 25 or more user identifier (userid) and password combinations to manage (Gao, Ma, Jia, & Ye, 2012). In most cases the user is expected to recall the passwords and userids from memory. Though users are encouraged to use unique passwords for each account (Florencio & Herley, 2007), four to five is the number of unrelated, regularly used passwords that users can be expected to successfully manipulate (Adams & Sasse, 1999).

Because most people find it difficult to remember alphanumeric passwords (Florencio & Herley, 2007), they adopt various strategies, usually unsafe, to manage them (Everitt, Bragin, Fogarty, & Kohno, 2009). The gap between passwords to manage, and the number that can be remembered dooms the effort to failure if the user relies upon the normal capabilities of human memory recall (Horcher & Tejay, 2009). As a result, the accumulation of more accounts normally means the reuse of more passwords, not the creation of new ones (Gaw & Felten, 2006).

Using graphical passwords to enhance memorability does not negate the difficulty of multiple password recall (Biddle, Chiasson, & Oorschot, 2012). Furthermore, the user may have difficulty in recalling the user identifier (UID), which is relatively public (Florencio, Herley, & Coskun, 2007), as well as the password. The quantity of passwords hampers recall regardless of the format. On the other hand, passwords cannot be abandoned until an alternate method of authentication which is usable and secure is developed (Stajano, 2011). As stated previously, Garfinkel's security-usability design principle of "Good Security Now," advises system designers to design the best security possible with the current capabilities instead of waiting for some future discovery to solve all the issues (Garfinkel, 2005). Password safe software to store groups of passwords securely behind a single key (Lee & Ewe, 2007) or external password storage in a hardware token such as Pico (Stajano, 2011) are options for managing multiple passwords. Using a paper notebook to organize the insecure practice of writing (Roberts, 2010) can be better from the user perspective than being denied access to accounts.

3.2.2 Suggested Solution: Cued-recall Location-based User Entry (CLUE)

The artifact used to instantiate the proposed security-usability principles, a security navigation interface, provides an alternative to current navigation of basic authentication. Rather than the pure recall required by typical UID-password authentication, the user is assisted with cued-recall, also known as hints. The hints are delivered based on the concept of progressive authentication, which seeks to reduce the authentication overhead on mobile devices (Riva, Qin, Strauss, & Lymberopoulos, 2012). 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 this case the amount of assistance, or cued-recall location-based user entry (CLUE), is higher in safe locations and lower in less safe locations. The design uses the capabilities and intrinsic qualities of mobile, such as GPS, to implement progressive security based on location.

Risk assessment of the use of technology shows locations are not equal in security risk. Internet Protocol (IP) addresses of a device are used as a means to identify risk (H. Park & Redford, 2007). By definition a mobile device is one that can change location (Barkhuus & Polichar, 2011), so the GPS address is a better indicator of the location and the potential risk of the location. When in the locations that have reduced risk, less risk should require less security. Less security, in turn, should require less consumption of resources. Varying the security based on location should appropriately conserve constrained resources.

Authentication schemes are based on what a user knows, what a user has, and/or what a user is (Almuairfi, Veeraraghavan, & Chilamkurti, 2012). The artifact stores password hints and user identifiers instead of the passwords. When the actual password is not stored, the user must still bring something they know to authenticate. The user must decode the hint into a password. Using cued recall to perform the memory task of password retrieval allows previously inaccessible information in a pure recall situation to be retrieved with a retrieval clue (Stobert & Biddle, 2013). The effort of cued-recall is lower than pure recall (Biddle, Chiasson, & Oorschot, 2012). Therefore the appropriate use of cued-recall conserves one of the constrained resources identified for mobile devices, user expertise/effort, and applies the proposed security-usability principles.

3.2.3 Adjust Security Based on Risk to Conserve Constrained Resources

The Microsoft security threat model is one of the most simple, and applicable to characteristics of software (Steer & Popli, 2008). As seen in Figure 4, the assessment begins with an examination of the objectives of the software. The objectives of CLUE are to conserve the constrained resources on mobile devices. If the risk varies based on location, then the expenditure of resources to compensate for that risk could also vary. For example, within the home, a user may not need to have a frequent phone lockout because the risk of compromise in that location is lower.

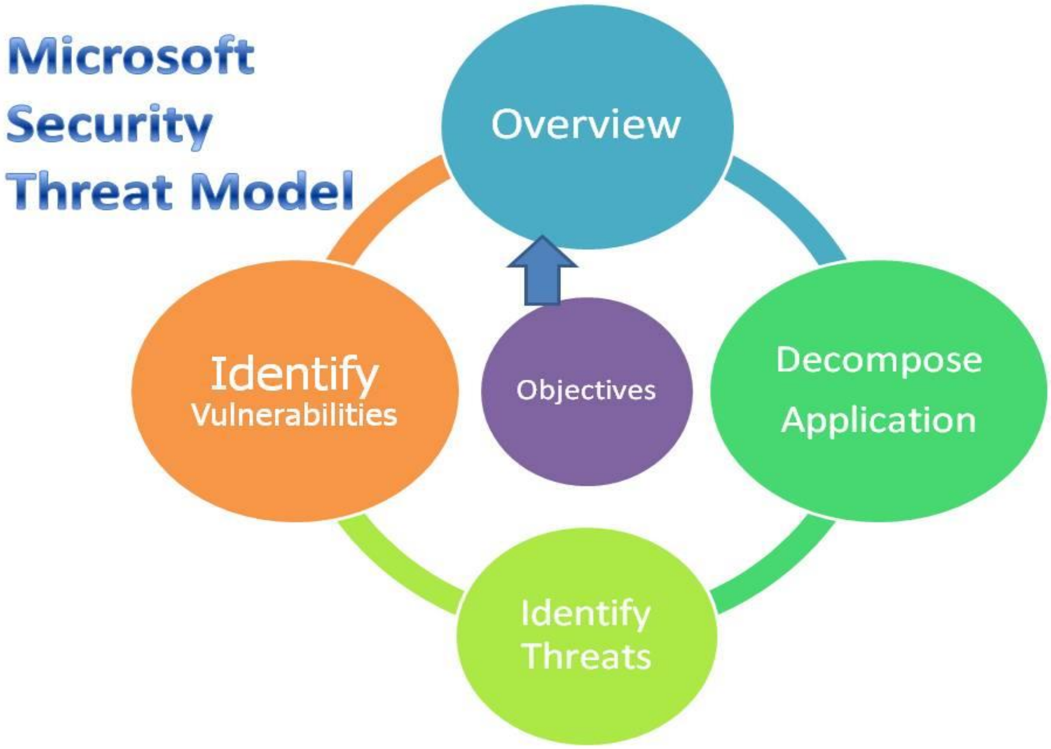
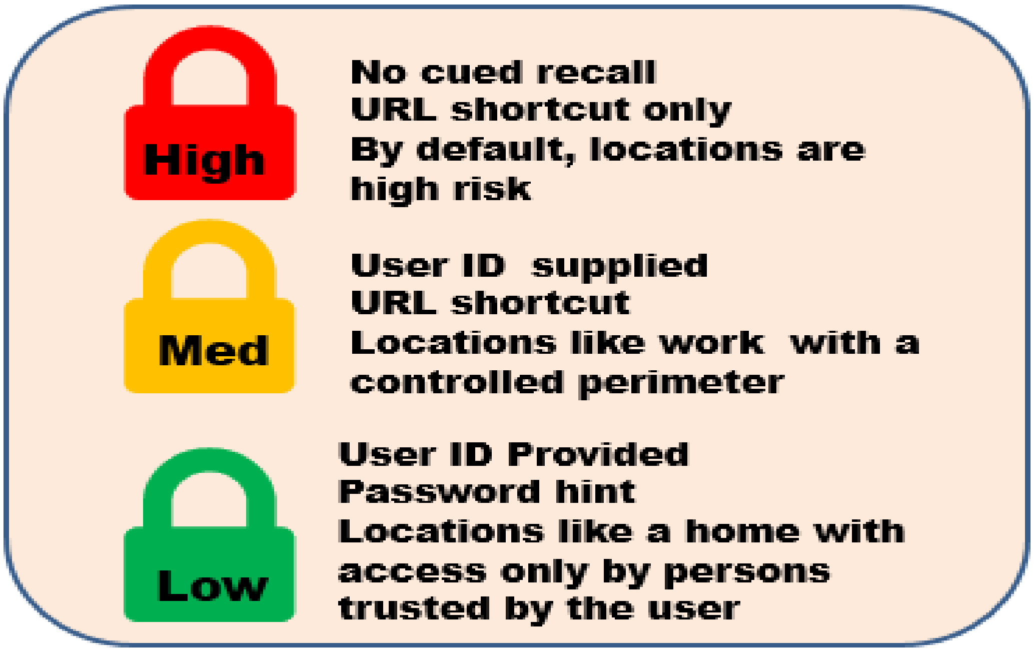


Figure 4. Microsoft Security Threat Model.

Each location where a mobile device uses the CLUE interface is put in category that represents the probable risk at that location. The categories are described in Figure 5, and the resulting security behavior from the CLUE interfaces.



High

No cued recall
URL shortcut only
By default, locations are high risk

Med

User ID supplied
URL shortcut
Locations like work with a controlled perimeter

Low

User ID Provided
Password hint
Locations like a home with access only by persons trusted by the user

Figure 5. Location Security Categories and Behaviors

The high risk setting of CLUE behaves like conventional security available on mobile devices and desktop workstations. The user receives no assistance from the CLUE interface, other than a shortcut to the URL of the Internet site being visited. The functionality resembles bookmarks functionality present in most browsers, and has the same risk. Locations by default are public and considered high risk.

The medium risk setting of the CLUE interface provides a link to the desired Internet site, and the user identifier (UID) for that site. A work location is typically medium risk because physical access is frequently controlled.

The low risk setting of the CLUE interface provides a link to the desired Internet site, the UID, and a password hint. The hint is not displayed until the user requests it. The user's home location is typically low risk, because there is very limited access to the location, and the access is by persons trusted by the user.

As a result of providing variable security for variable risk (Figure 5), the CLUE interface conserves the constrained resources of power, form factors, and user effort in a mobile security interface. Use of the CLUE interface in situations where more of these resources are conserved demonstrates a higher level of usability if the proposed principles are valid.

3.2.4 Development

For the purposes of the study, mobile devices with GPS capability were needed. The mobile device can be used in many contexts, and in very personal ways (Barkhuus & Polichar, 2011). The operating systems on the platform are increasingly diverse, as are the capabilities of each platform (Tilson, Sorensen, & Lyytinen, 2012). To create the greatest accessibility across mobile devices, web applications that are accessed using a mobile browser have become more popular than creating the application in each native operating system (Qing & Clark, 2013). Web applications that run in Internet browsers are compatible with all current mobile platform and allow a comparison to desktop.

The web application used as the artifact was created using the Bootstrap web design framework which uses pre-defined Cascading Style Sheet (CSS) classes more easily create responsive screens which adapt to various device sizes (Lerner, 2012). The scripting backend was the Angularjs JavaScript framework which uses the Model-View-Whatever (MVW) structure for separating the presentation layer from the database layer (Ramos, Valente, Terra, & Santos, 2016). These structures allow web application development that can use modular programming similar to traditional programming languages (Ramos et al., 2016).

The backend uses Google’s Firebase platform for authentication (Google, 2017a). Firebase provides basic authentication with email as the UID. There are also options to use federated identity providers like Facebook, Twitter, and GitHub. Using Firebase authentication ensures a secure and stable authentication protocol with minimal code for integration. The Firebase platform also provides a no-SQL database for data collection in the cloud (Google, 2017b). The data is synchronized in real-time, and remains available even when the application is off-line. A data console allows a developer to interact with the data directly, as well as through Application Programming Interface (API).

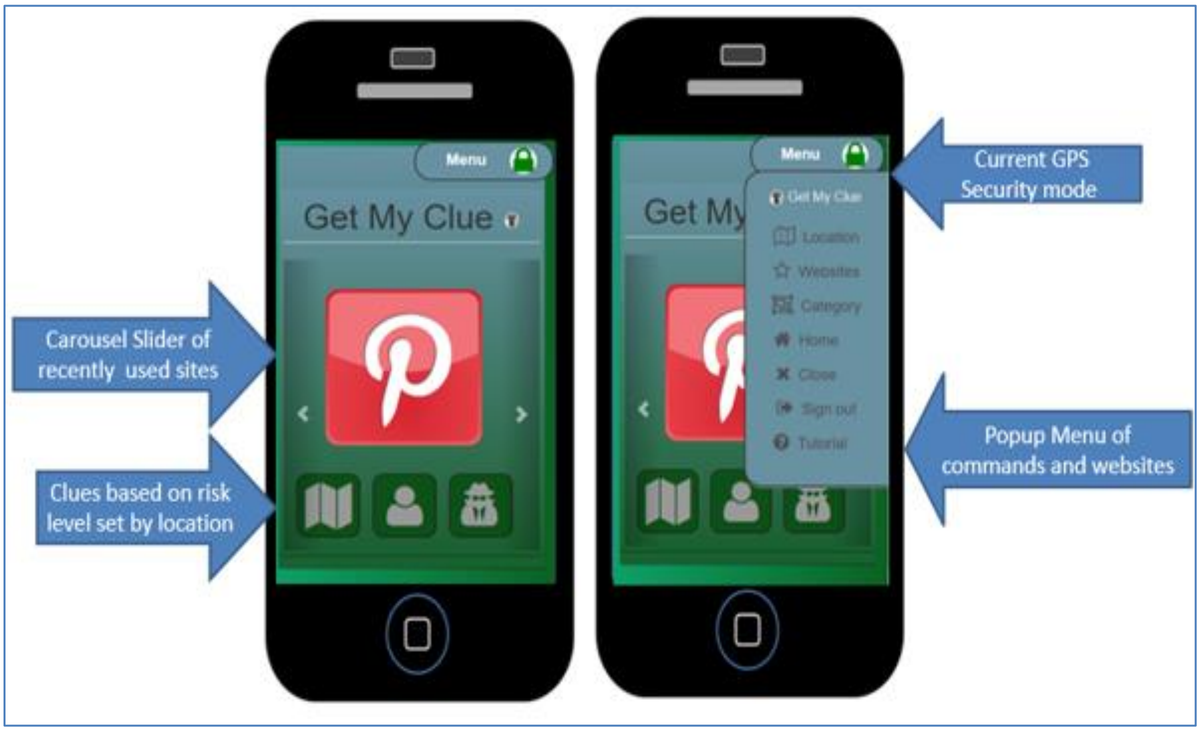

Menu
Get My Clue
Carousel Slider of recently used sites
Clues based on risk level set by location
Menu
Get My
Get My Clue
Location
Websites
Category
Home
Close
Sign out
Tutorial
Current GPS Security mode
Popup Menu of commands and websites

Figure 6**.** Two Views of CLUE Home Screen with Functionality Labeled

A screenshot of the CLUE interface home screen is shown in Figure 6 with labels describing the functionality on the screen. Key functionalities of the interface that apply the proposed security-usability principles are labeled by the large blue arrows. The functionality may relate to more than one of the design principles**.** Only the functionalities in the interface directly related to user interaction with authentication are labelled.

Table 6. Application of Security Principles to CLUE Design (Subset)

CLUE element	Principle	Usability Equivalent	Discussion
Menu of websites	Least Surprise	User in control	User chooses websites
		Match system to real world	Menu like restaurant
	Complete Mediation	Error prevention and Help	Help option on menu
	Least Common Mechanism	Consistency in placement	Upper right corner
	Economy of Mechanism	Reduce cognitive load Recognition rather than recall	Select instead of type
		Aesthetic and minimalist design	Hide/display on click
GPS mode	Least Surprise	Shortcuts for experience	User can change mode
		Match system and real world	Icons use traffic light color (red/yellow/green)
	Complete Mediation	Visibility of system status	Risk level on screen
		Informative Consistent Feedback	Pictures instead of words
	Economy of mechanism	Aesthetic and minimalist design	Pictures instead of words
	Principle of Least Privilege	Limit Functionality/Access to Reduce Complexity	Auto-set risk level
Favorites Carousel	Economy of mechanism	Reduce cognitive load Aesthetic and minimalist design	Select from screen Large icons as default

In Table 6 the security-usability principles derived in 3.1.3 are mapped to the corresponding functionality in the CLUE interface. Each user interaction with the CLUE interface was designed to conserve the number of keystrokes/clicks, the cognitive load on the user, the complexity of the layout on a smaller screen, the number of processes that run, and apply the maximum security-usability principles possible. Simply following a checklist has not produced high quality usable interfaces (Zezschwitz, Dunphy, & Luca, 2013). At an IBM research facility, examining software designs and getting predictive feedback on user interactions even at the wireframe stage was critical to a successful software design (Bellamy, John, & Kogan, 2011). This technique, which produced the user interface design instrument Cogtool, was used to measure the efficiency of CLUE.

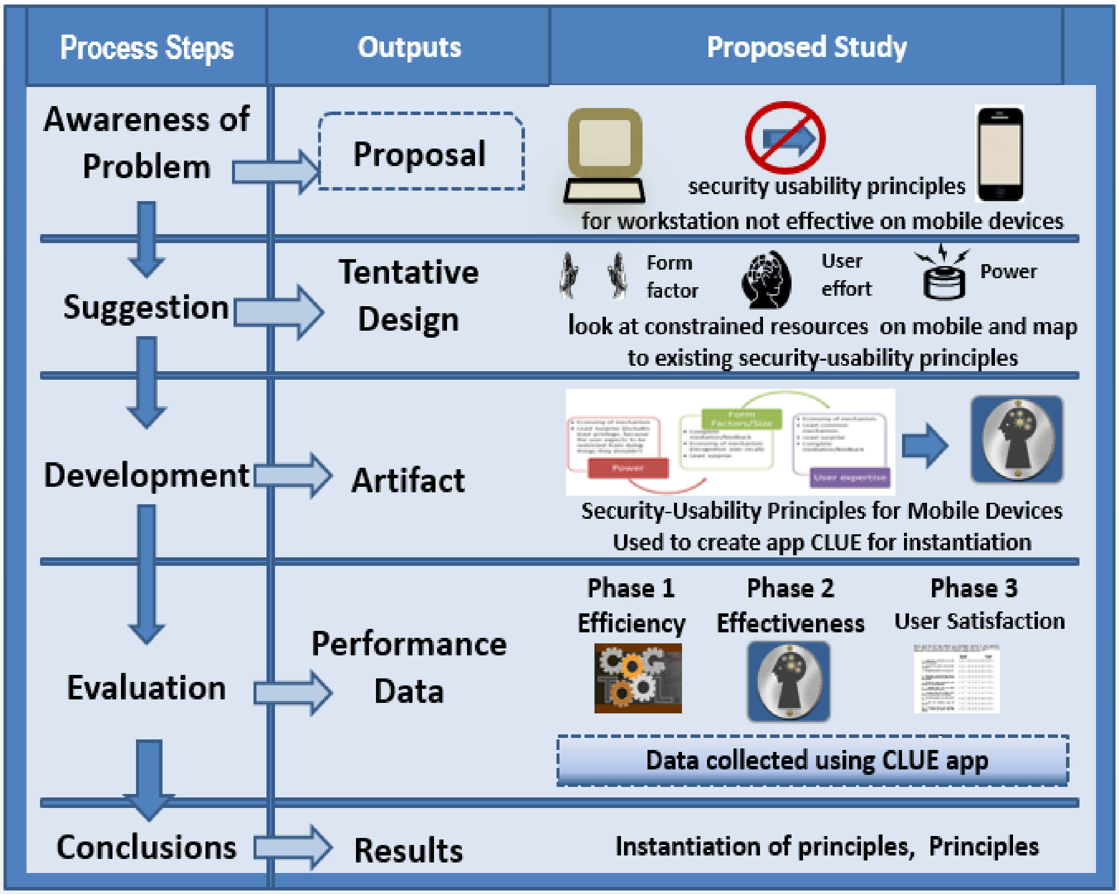

Process Steps
Outputs
Proposed Study
Awareness of Problem
Proposal
security usability principles
for workstation not effective on mobile devices
Suggestion
Tentative Design
Form factor
User effort
Power
look at constrained resources on mobile and map
to existing security-usability principles
Development
Artifact
Security-Usability Principles for Mobile Devices
Used to create app CLUE for instantiation
Evaluation
Performance Data
Phase 1
Efficiency
Phase 2
Effectiveness
Phase 3
User Satisfaction
Data collected using CLUE app
Conclusions
Results
Instantiation of principles, Principles

Figure 7. Design Science Research Applied to Proposed Research.

3.3 Evaluation

The CLUE interface embodies the combined security-usability principles for mobile devices described above. In Figure 7, the steps followed are summarized and mapped to DSR. In the evaluation phase, the CLUE interface is assessed using the web application created as an artifact to instantiate the mobile security design principles. The artifact was evaluated based on the following hypotheses to prove security usability for mobile devices requires conservation instead of complication.

- H0: CLUE will have no impact on the usability of basic authentication
- H1: CLUE will increase the user success navigating basic authentication
- H2: CLUE will improve the user experience of using basic authentication

The first two hypotheses looks at whether the user achieved entry into the application and did not have to retrieve either the UID or password, or need to reset password. Lack of success has typically led to circumventing security or insecure practices like writing passwords down (Nelson & Vu, 2010). Avoiding those time-consuming actions leads to both success and improved experience.

- H3: CLUE will improve usability by reducing the power consumed by reducing the frequency of issuing the security challenge
- H4: CLUE will improve usability by minimizing manipulation of the device during authentication in ways such as keystrokes and screen swipes

Measuring power from a hardware perspective is a complicated procedure and typically prohibitively expensive for the software designer with the usual skill set (Hudert, Niemann, & Eymann, 2010). Instead, application developers are encouraged to conserve power by reducing displays, calls to networks, and screen refreshes (John, Swart, Bellamy, Blackmon, & Brown, 2013). The third hypothesis uses this convention of avoiding power usage to measure the conservation of power.

The fourth 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 (Li, Guy, Yatani, & Truong, 2011; Serrano, Lecolinet, & Guiard, 2013; Shirazi, Henze, Dingler, Kunze, & Schmidt, 2013), and even more so for security (Chiang & Chiasson, 2013).

- H5: CLUE will improve usability by conserving user effort such as memory recall, and task identification
- H6: Non-workstation (mobile) use of basic authentication with design principles of CLUE will show less difficulty than workstation use of basic authentication.

The fifth hypothesis focuses on the role of cognitive effort in the actions involved in basic authentication. This effort is less obvious than the physical challenges explored in the first hypothesis, but the importance of conserving cognitive effort is recognized as needed in authentication (Herzberg & Margulies, 2012; Theofanos & Pfleeger, 2011). Finally, the sixth hypothesis looks at the higher level of difficulty experienced by users of security interfaces on mobile versus desktop (Oberheide & Jahanian, 2010).

As mentioned in the literature review, usability is characterized by efficiency, effectiveness, and satisfaction (Jokela, Iivari, Matero, & Karukka, 2003). To validate that applying the security-usability design principles for mobile device to security interfaces increases usability, three phases of validation were done, each aligned with a characteristic of usability.

The current preferred norm for basic authentication provides no assistance for retrieving the UID or the password (Capek, Hub, Myskova, & Roudny, 2010). Within the CLUE interface the High-risk location is the option/pathway/mode that equates to that norm. Consequently, measures taken for High-risk mode represents the pre-experimental conditions. The basic authentication, in spite of its weaknesses, is still the ISO standard for entity authentication (Basin, Cremers, & Meier, 2012).

In Table 7 the various phases of the evaluation that correspond to the ISO 9241-11 characteristics of usability (Jokela et al., 2003) are summarized and mapped to the hypotheses. In each case the hypotheses are supported or/ refuted by applying the principles to the design as a whole, not as individual principles. Details of each phase are

Table 7**.** Summary of Evaluation Phases and Hypotheses Measured

Phase	**Research Method**	**Principle(s) tested**	**Hypotheses**
1-Efficiency	Simulation with known instrument Cogtool	Economy of mechanism, Complete mediation	H0 – no impact H1 – success in navigation H3 – power conserved H4 – Form factor conserved H5 – User effort conserved H6 - Mobile vs Desktop
2-Effectiveness	Experiment	Least Surprise, Economy of Mechanism, Least Privilege, Complete Mediation, Least common mechanism	H0 – no impact H1 – success in navigation H2 – user satisfaction H3 – power conserved H4 – Form factor conserved H5 – User effort conserved H6 - Mobile vs Desktop
3-Satisfaction	Survey	Least Surprise, Economy of Mechanism, Complete Mediation	H0 – no impact H1 – success rate H2 – user satisfaction H5 – User effort conserved H6 - Mobile vs Desktop

in the sections following the table. Combining cognitive modelling like Phase 1 with a user study like Phase 2 gives more evidence and better perspectives (Bhensook & Senivongse, 2012).

3.3.1 Use Cases

In phase 1 and 2 of evaluation, the following use cases are to generate the data for measurement. Each use case describes a sequence of events related to a user's interaction with the CLUE security interface. There are four possible use cases in the CLUE interface for a user's interaction with an interface with password-UID authentication (Table 8). Depending on the security mode as set by GPS location, described in 3.2.3, the user gets varying amounts of assistance to navigate the user interface. Detailed diagrams of use cases appear in Appendix A.

Table 8. Use Cases for Testing Security Set by Location

Use Case	**Got UID?**	**Got Password ?**	**Assistance given (applying principles0**	**Comments**
1	Yes	Yes	All modes need no assistance	All modes lead to success
2	Yes	No	High- none Medium - UID Low – UID & password hint	High fails, other modes may succeed
3	No	Yes	High- none Medium - UID Low – UID & password hint	High fails, other modes may succeed with assistance
4	No	No	High- none Medium - UID Low - UID & password hint	High fails, other modes have more success

3.3.2 Measuring the Constrained Resources

Within the evaluation phase, the consumption of constrained resources was measured both in the design phase, and during actual user interaction. Previous research in HCI and security interfaces on the mobile platform provides guidance on which indicators to measure (Table 9). Cognitive activity as a critical component of usability frameworks is also supported by constructs employed by usability professionals to evaluate system use (Hertzum & Clemmensen, 2012).

Table 9**.** Actions to Measure for Constrained Resources

Constrained Resource	**Action to Measure**	**Reference**
Power	Screen display 30 sec elapsed display CPU call by command button	Knight, Pyrzak, & Green, 2007 Hudert et al., 2010 Anand et al., 2011
Form Factor	# of Keystrokes (desktop) # of Screen Touch/Swipe (mobile) # of Button pushes	Holleis, Scherr, & Broll, 2011 Bernal, Ardito, Morisio, & Falcarin, 2010 Dunphy & Olivier, 2012
User effort	# of pure Mental recalls # of cued mental recalls	Holleis et al., 2011 Holleis et al., 2011

These three manifestations of display, CPU, and network consume 45-50% of the total system power on the typical smart phone (Knight et al., 2007). Therefore, to measure power consumption from the context of the CLUE interface, three manifestations of expending power are recorded as seen in Figure 8.

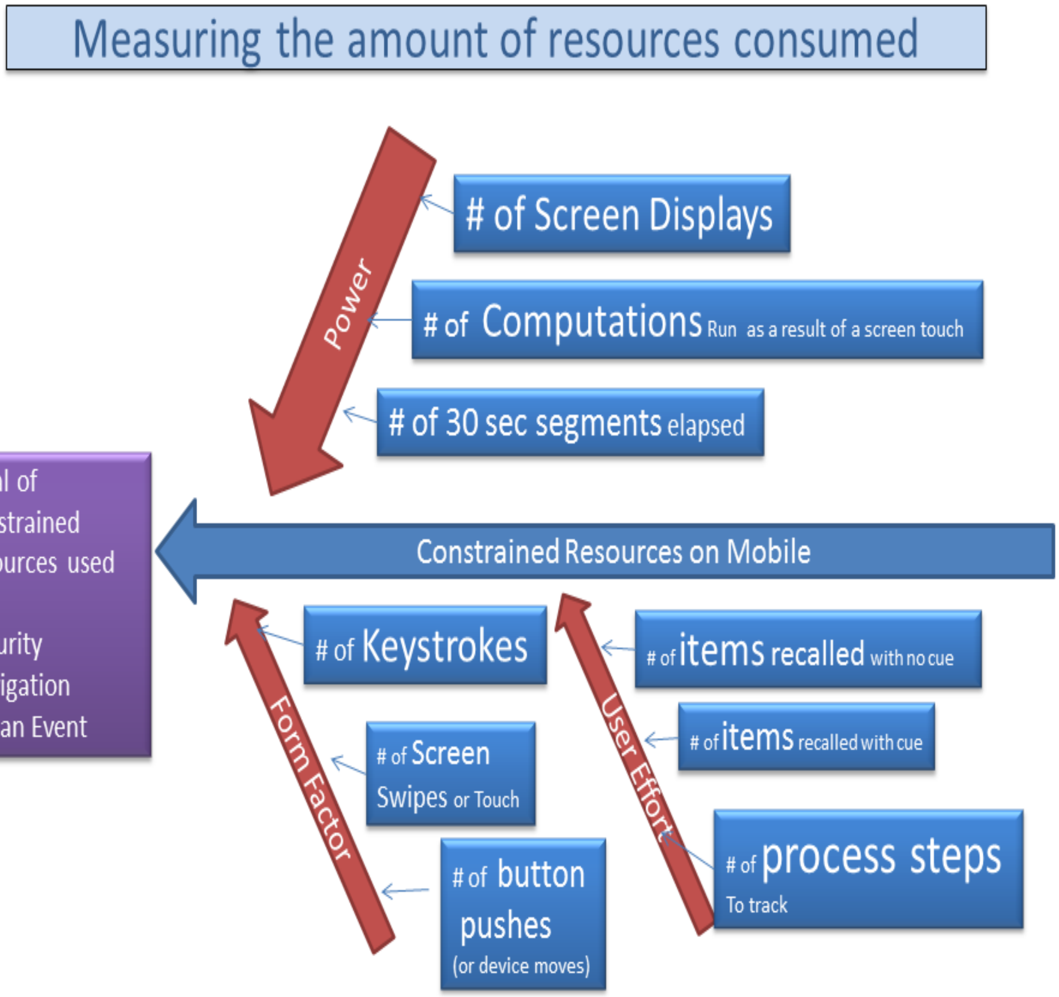

Measuring the amount of resources consumed
Power
# of Screen Displays
# of Computations Run as a result of a screen touch
# of 30 sec segments elapsed
Total of constrained resources used for Security Navigation For an Event
Constrained Resources on Mobile
Form Factor
# of Keystrokes
# of Screen Swipes or Touch
# of button pushes (or device moves)
User Effort
# of items recalled with no cue
# of items recalled with cue
# of process steps To track

Figure 8. Measuring Constrained Resources

To measure how much manipulation of the form factors is required, the number of keystrokes plus the number of screen swipes/touches and the number of physical buttons pushes (other than keyboard) is recorded. Though Li, Liu, Liu, Wang, Li, and Rau (2010) proposed nine new operators to describe a user’s physical interaction with mobile devices, not all these operators are valid in the context of a security interface. Since this research looks at reducing the number of keystrokes and screen interactions, the different motivations for the physical interactions that motivate the delineation described by Li et al. (2010) are not of interest. This summarization of the physical operators is supported by Holleis et al. (2011) in their expansion of KLM to study NFC tags on the mobile platform.

Both Holleis et al. (2011) and Li et al. (2011) combined a mental effort operator with physical operator (s) to describe an operation block. In the expert user community that Holleis et al. (2011) and Li et al. (2011) study this sequencing may be valid. However for the novice or less technology literate, the mental effort may vary within that sequence of mental and physical actions. This research focuses on the novice user, so the mental effort is separated from physical effort. Studies of literate and non-literate mobile phone users in India support this separation of physical form factor effort from mental effort (Holleis, Luther, Broll, & Souville, 2013). The results of rural mobile phone usage indicate little variance in the physical effort, but a great variance in the usability of the mental effort tasks between the literate and non-literate users. Cognitive activity as a critical component of usability frameworks is also supported by constructs employed by usability professionals to evaluate system use (Hertzum & Clemmensen, 2012).

User effort to recall is measured by recording the number of times a user is asked to recall information with and without a cue, and how many steps are in a process sequence executed by a user. Each process step equates to a recall “unit” of measure. Each recall with a cue is equated to one effort unit. Each recall without a cue is measured as two units, because of the higher level of difficulty and cognitive load. This consideration of the user cognitive activity, and weighting of increased difficulty as a component of usability, is supported by the usability professionals common research constructs analyzed by Hertzum et al (2012).

Previous studies have looked at keystrokes as a measure of the usability of a system, such as the total-effort metrics approach (Kim et al., 2010). As usability designers continue to examine the difference between desktop keystrokes and mobile device keystrokes, amendment of the Keystroke-Level-Modeling protocols (Card et al. 1980), particularly in the area of security interfaces, have been necessary to accommodate the reality of mobile (Dunphy & Olivier, 2012; Zezschwitz et al., 2013). This research looks for the impact in more than one area of resource consumption.

3.3.3 Phase 1 – Efficiency with CogTool

A CogTool score of application complexity is used to measure the efficiency of the CLUE security interface, As discussed in 3.2.4CogTool was developed by usability researchers to model the complexity of an application interface based on wireframes of the planned screens, and a mapping of the flow between these screens (John, 2011). The CogTool score is based on a database of human performers using computer interfaces. A lower CogTool score indicates a less complex interface which is more desirable.

CogTool can create a usability measure at the design stage, instead at the production stage. This allows fine-tuning of a design without the expense of programming (Zezschwitz et al., 2013). In this study the measures were done at the end of development to provide a measure of usability of the final version.

Other functionalities available for adding categories, websites, and new locations to the various security modes are not part of an authentication sequence and thereby excluded from the measures in this study.

Hypotheses Tested

In Phase 1 evaluation of the efficiency of security-usability, the following hypotheses are addressed as described in Table 10.

Table 10. Phase 1 Hypotheses Validation

Hypothesis	Measurement	Measuring success
H0 - no impact	Overall CogTool score for all security tasks	High is the current norm High risk score would be less than or equal to score for the Medium and Low risk meaning the principles don't apply
H1 - impact on usability	Overall CogTool score for all security tasks	High is the current norm. High risk score would be greater than score for the Medium and Low risk meaning principles apply
H2 - improve the user experience	CogTool score of each security task for each platform and each security mode	Score for Low and Medium risk are lower than High risk for using for each task
H3 - conserving power	CogTool score for power subtasks that make up the security tasks	Score for Low and Medium risk are lower than High risk
H4 - reducing manipulation	CogTool score for form factor subtasks that make up the security tasks	Score for Low and Medium risk are lower than High risk
H5 - conserving user effort	CogTool score for user effort subtasks that make up the security tasks	Score for Low and Medium risk are lower than High risk
H6- Mobile vs desktop	Overall CogTool score for each security task on each platform	Score for security task on mobile is lower than score on desktop once principles applied for Med and Low modes

Data Collection for Phase 1 Efficiency

To compute a CogTool score the designer creates a wireframe of the interactions that to be measured. The transitions that occur between the various screens are drawn out and described based on how they are accomplished. For example, typing in a textbox transition using a workstation or desktop involves a keyboard and a string of characters that are entered. In the illustration below the wireframes of the CLUE artifact are linked with arrows that have data attached that describe the actions that take place when transitioning between the screens. In Figure 9 the wireframe for the interface on desktop for low risk can be seen. Wireframes for the other designs are in Appendix B.

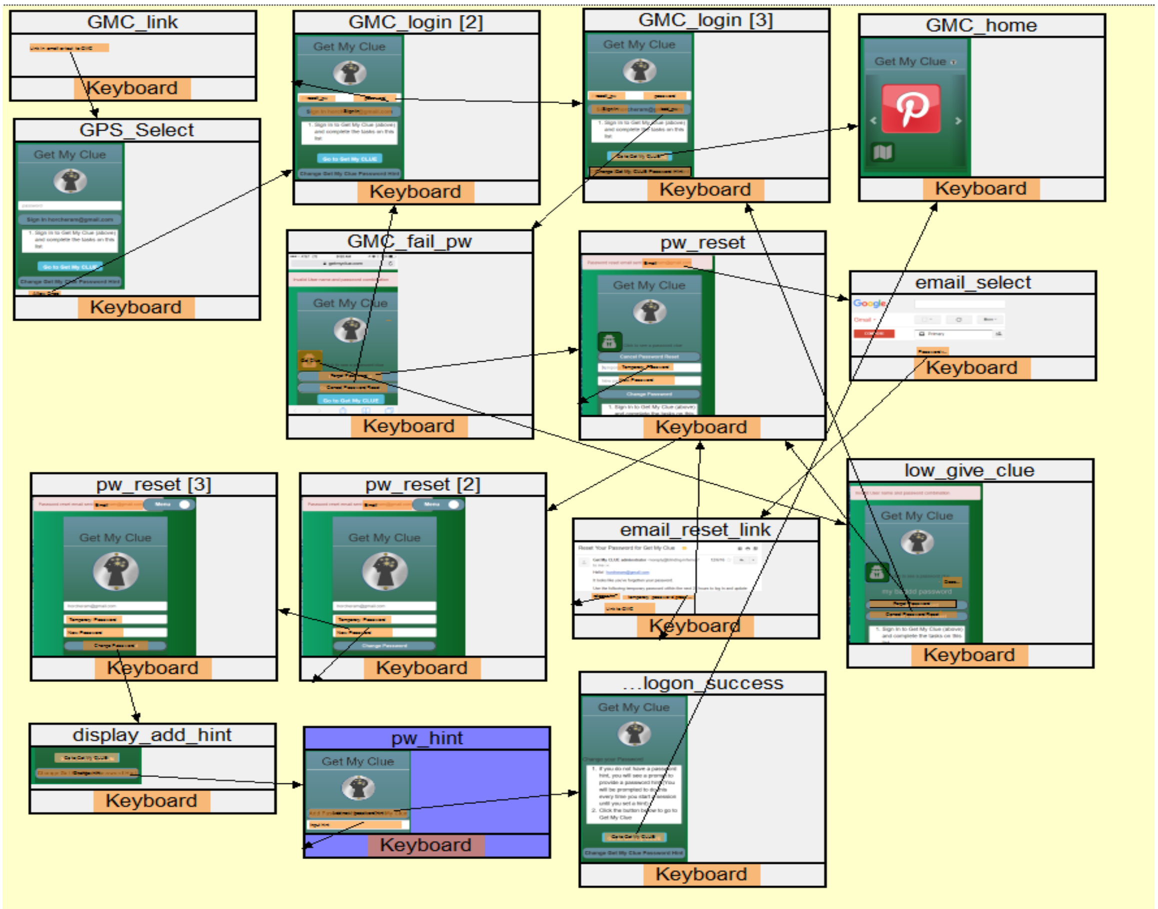


Figure 9. CogTool Wireframe of Desktop Design for Low Risk

Once the wireframes are linked with transitions, the designer goes into the CogTool demonstrate mode to walk through the tasks. Four security-related tasks were analyzed for usability in each design (Table 11). Three versions of the security interface to a 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 evaluated on the traditional workstation and on mobile devices. The study examines the difference between a security-interfaces constrained on the mobile platform. Therefore when the designer demonstrates the task, it is done on a design that reflects the form factor, user effort, and power that is available on a workstation, as well as a design that shows the capabilities of a mobile device.

Table 11. 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

These same four security tasks are used to describe the path taken by a user through the security interface. There are four possible paths through the interface based what security information the user possesses. Depending on the design of the interface, the designer demonstrated more or less of the tasks. For example, as part of the design for medium and low risk the UID is provided as part of the assistance offered to the user. Therefore in medium or low mode the UID recovery task is never performed. The password recovery task is only available in low mode. On the other hand Logon Attempt and password reset tasks are used in all risk modes. Use Case 4, where the user does not know UID or password is diagrammed in Figure 10. The diagrams for all four use cases appear in Appendix A.

In the diagram (Figure 10) the red arrows represent the current norm, which is High risk. The yellow arrows represent Medium risk, and the green arrows the Low risk mode. Using the diagrams for the four use cases, the security tasks that must be performed to achieve successful authentication in each instance are clear. The CogTool score for successful authentication becomes the sum of the security-related tasks that are on the path for a particular design (Zezschwitz et al., 2013).

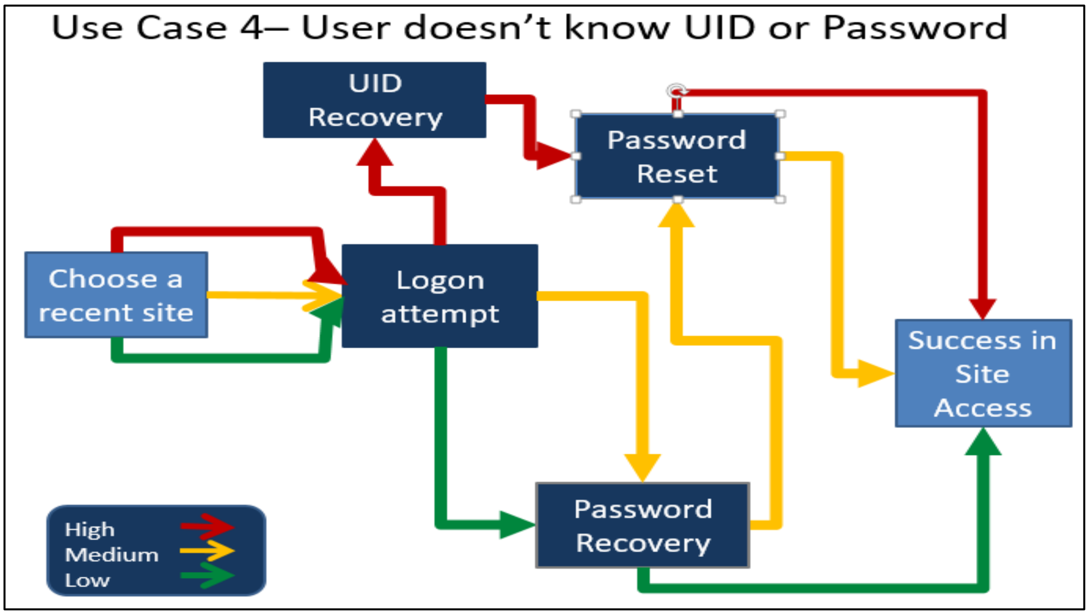


Figure 10. Use Case 4 - User Does Not Know UID or Password

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 (Poremba, 2014). Email addresses became a popular option with account suppliers because they are already unique and provide a communication channel for both marketing and password recovery.

The majority of email address ranges between 16-28 characters (Bliss, 2015). 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 (Blezard & Marceau, 2002). 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 12. 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` After the simulation of the path through the security interface is complete, CogTool computes a score which indicates the difficulty in seconds.

Table 12. Rules for a Strong Password (Horcher & Tejay, 2009)

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

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 11). The measures on the visualization graph are broken down into eye movements, left-hand movements, and cognition. Looking at the visualization example of email input on desktop and mobile, it is clear that the same keystroke on desktop uses different resources on each platform and different amounts of that resource. In particular, more of the constrained resources of user effort (aka cognition) and form factor (Eye-move, Right-hand, Left-hand) are consumed on mobile.

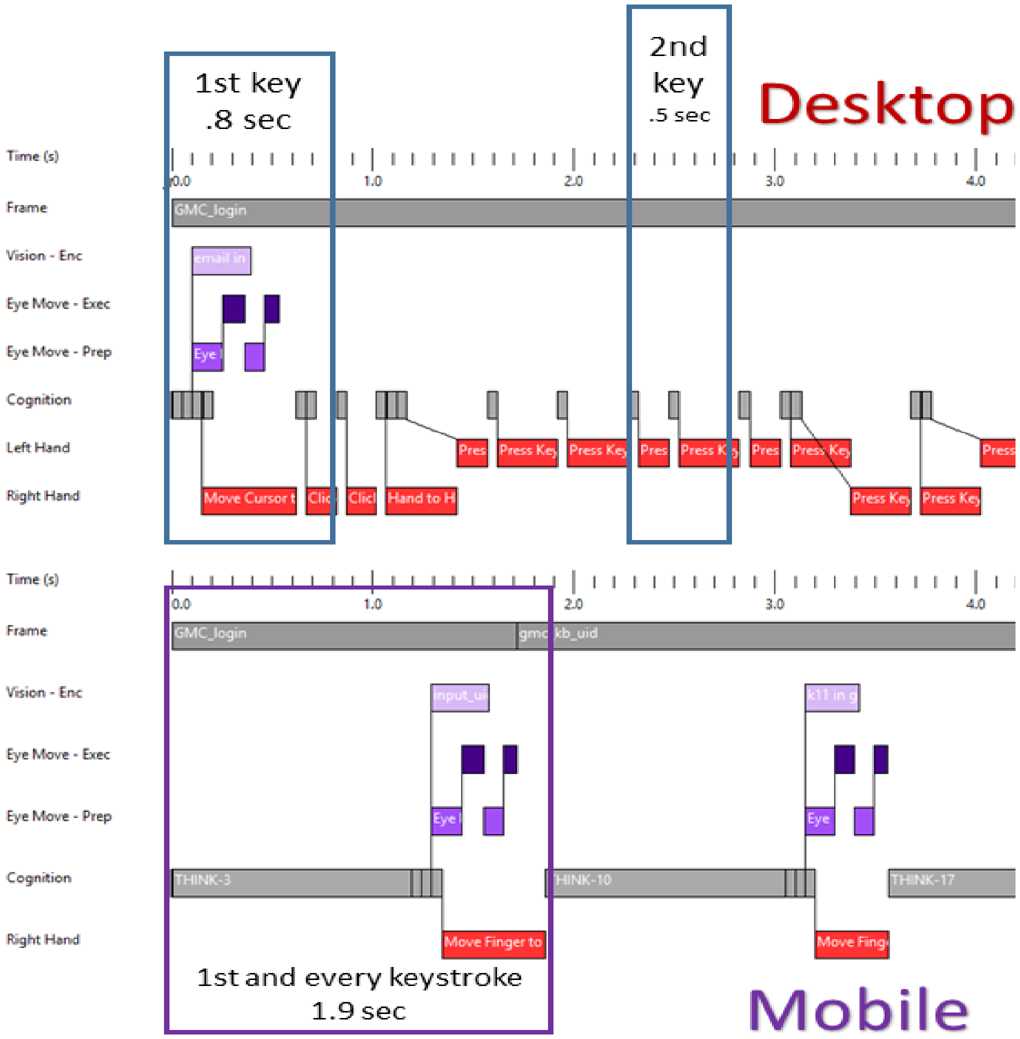
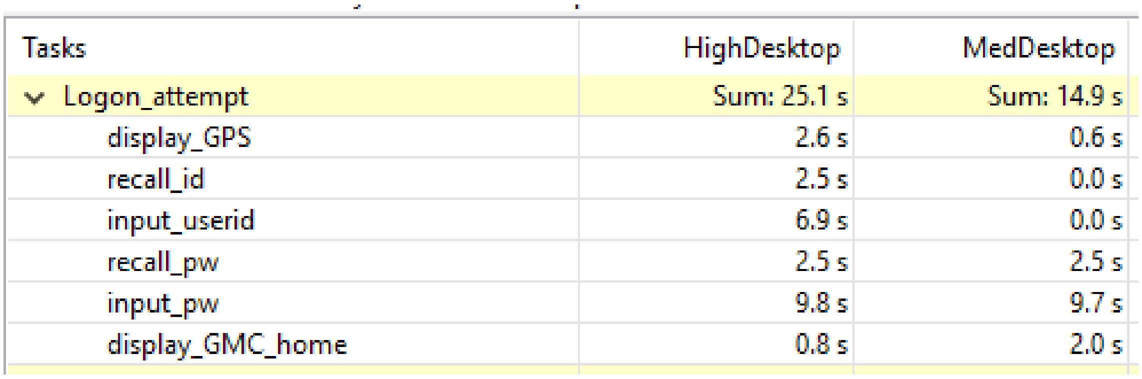


Figure 11. Cogtool Visualization of Input on Desktop (above) and Mobile (below)

Unfortunately this level of granularity is not in the reports available to the designer using the tool. To make the data for the CogTool score more granular for analysis, each security task was divided into subtasks for demonstration. Each subtask corresponds roughly to one of the three constrained resources. The subtasks typically represent a self-contained sequence that can possibly be avoided by re-design and subsequently conserve a resource. Breaking the predicted resource consumption down by the constrained resources allows individual confirmation/refutation of hypotheses related to these resources.



Tasks	HighDesktop	MedDesktop
⌄ Logon_attempt	Sum: 25.1 s	Sum: 14.9 s
display_GPS	2.6 s	0.6 s
recall_id	2.5 s	0.0 s
input_userid	6.9 s	0.0 s
recall_pw	2.5 s	2.5 s
input_pw	9.8 s	9.7 s
display_GMC_home	0.8 s	2.0 s

Figure 12**.** Sample Values from CogTool

Data Analysis

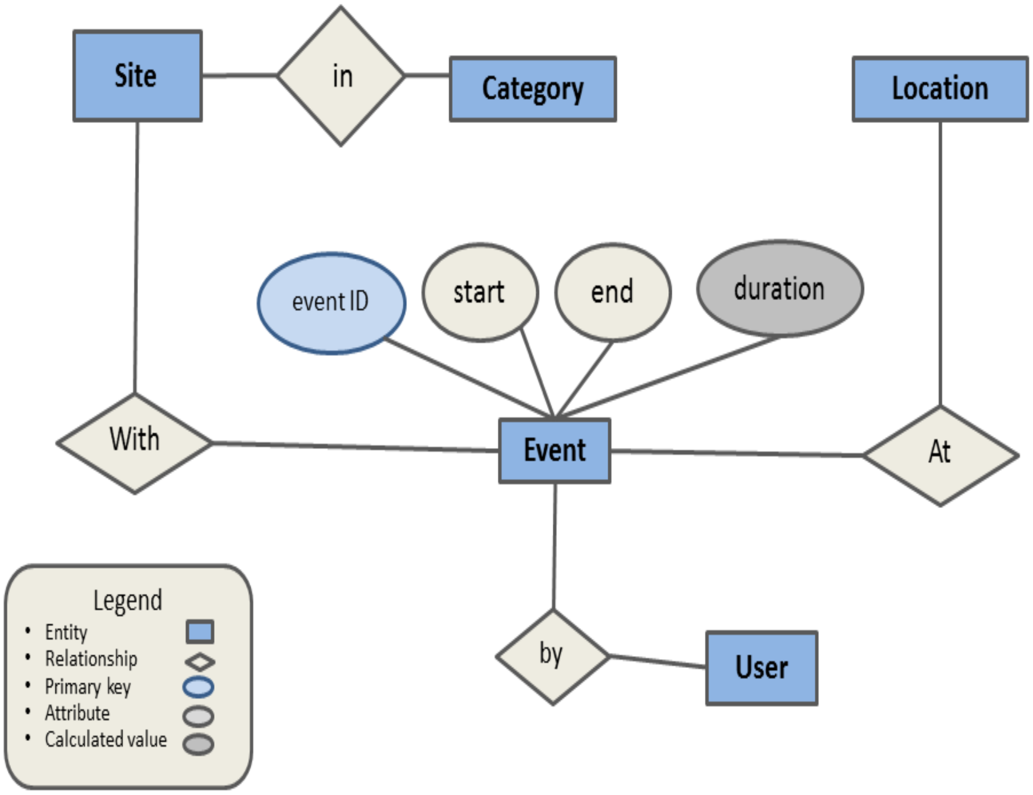
CogTool was used to create a score for each mode of security access, according to the use cases described in 3.3.1. The CogTool scores were also created for the constrained resources for each design. A comparative analysis of the resulting scores is how the data is typically analyzed to determine the best alternative. During the introduction of CogTool at the IBM research laboratories software designs were scored with CogTool, and the resulting scores and graphs of functionality implementation compared. John et al. (2011) also found the process of visualization required for the CogTool analysis provided clarity to the designers. The CogTool scores were also used to identify which tasks are consuming the greatest amount of constrained resources.

3.3.4 Phase 2 –Effectiveness

In this phase the impact of the CLUE interface design on user navigation of basic (password-UID) authentication on website was assessed. The actual usage data collected reveals how often the assistance offered by CLUE is invoked as part of daily usage.

Experimental research method was chosen because evaluating a design artifact using an experiment empirically demonstrates the qualities of the artifact and provides an avenue for generalizing the findings to a larger context (D'Aubeterre, Singh, & Iyer, 2008). An experiment frequently compares a previous norm with a changed set of conditions. As described in 3.2.3, the previous norm is the “High-risk” mode which provides no additional assistance. The degree to which data collected for “Medium-risk,” and “Low-risk” deviate from the data collected for “High-risk” clearly illustrates the impact of the applying the security-usability principles.

The CLUE interface automatically collects data about which sites were used, the security mode used, how long the user spent in the interface, and whether the usage was successful. The data collected about usage is appears the data model shown in Figure 13.



.

Figure 13. Data Model of Phase 2 Data

Experimental Design

To evaluate the web application created as an artifact to illustrate the security-usability design principles for mobile devices; this phase study used a quasi-experiment with repeated measures and counter-balanced design. The decision process for design type is shown in Figure 14.

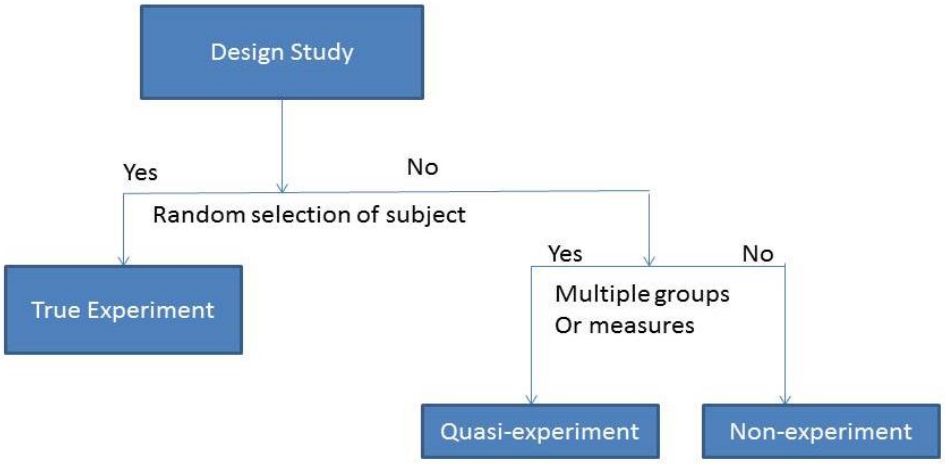


Figure 14. Experiment Design Decision Process (Lazar, Feng, & Hochheiser, 2010)

This phase used a repeated measures design, in which subjects act as their own control as they are exposed to all versions or variations of the changed conditions (D'Aubeterre et al., 2008). In this study, the control was represented by the "High" mode. The repeated measures design provides powerful statistics even with a limited subject group.

After initial training and the first set of measures, the subjects used the various modes based on their location. The number of tasks possible within the interface is minimized as described in Appendix A. A smaller number of tasks improves the ability of the users to identify usability problems (Bruun & Stage, 2012). The frequency of how often the subjects invoke each mode determined the success rate of the improved modes of “Medium,” and “Low” versus the current norm represented by “High.”

Subjects

The subjects for this study were recruited from an organization of small business owners and professionals, a group of technical women, and university students. These subjects were a convenience sample, recruited from organizations to which the principal investigator had access. The technical women, ranging from 22-75, belonged to a national group and represent both academic and business leaders with a high level of computer literacy. The business owners and professionals, on the other hand, ranged in age from 22-75, split almost 50-50 in gender, and range in technology ability from neophyte to skilled computer support. The university students included both graduates and undergraduates ranging in age from 18-28. The subject population consisted of 15-20 subjects as is typical for usability studies (Hwang & Salvendy, 2010), particularly of non-medical systems (Schmettow, Vos, & Schraagen, 2013)

Participation in the study was voluntary. An incentive of a gift card was provided to every subject who completed the tasks in this phase, Phase 2, as listed in Appendix C, plus Phase 3 of the CLUE evaluation. Incentives such as cash and gift cards are typical techniques for recruiting research study participants (T. Park et al., 2011) and have been shown to improve the quality of the participants’ interaction (H. Li et al., 2010).

Procedure

There are three stages to the experimental procedure: configuration, initial usage, ongoing usage (Appendix D). The configuration stage was designed to absorb all the user effort present only at setup, and remove it from the experiment evaluation. This reflects a batteries-included approach (Dubois, 2007) to technology interaction. A questionnaire administered by Surveygizmo provided default values for the websites configured in the CLUE interface. The data from Surveygizmo similar to other Internet survey tools like Survey Monkey.

The survey data was analyzed using frequency tables to see which websites and categories are the appropriate values to be presented as the default set. The questions asked during the survey were used to determine the most commonly used Internet sites that require password authentication, typical categories that users used to describe the sites in terms of security risk, and what security risk level the users felt relevant to particular sites. Research conducted on the security needs of the at-home user versus the business user indicates that there is a growing perception that security needs vary by application (Hayashi, Riva, Strauss, Brush, & Schechter, 2012).

Because Internet website landscape is a rapidly evolving environment, the most common sites were updated over the course of the study (Androutsos, 2011). The questionnaire provided a consistent data feed for that information not biased by the perspective of an individual blogger, and more current for an Internet user population possessing varying levels of technology competency of the CLUE interface.
The questionnaire used for Surveygizmo appears in Appendix E.

The initial usage stage introduced the subject to the interface using a tutorial. . The subject then signed up for an account so their usage of CLUE could be authenticated. The ongoing usage stage tracked usage of the CLUE interface in a natural setting, with a daily reminder via text message and email with a suggested task. This type of data is more revealing of day-to-day usage patterns and is a preferred measure of usability, particularly on mobile platform (Zezschwitz et al., 2013). Studies involving mobile device interactions with web browsers (Shirazi et al., 2013) similar to the CLUE interface have illustrated the value of field data, particularly when validating and deriving design guidelines.

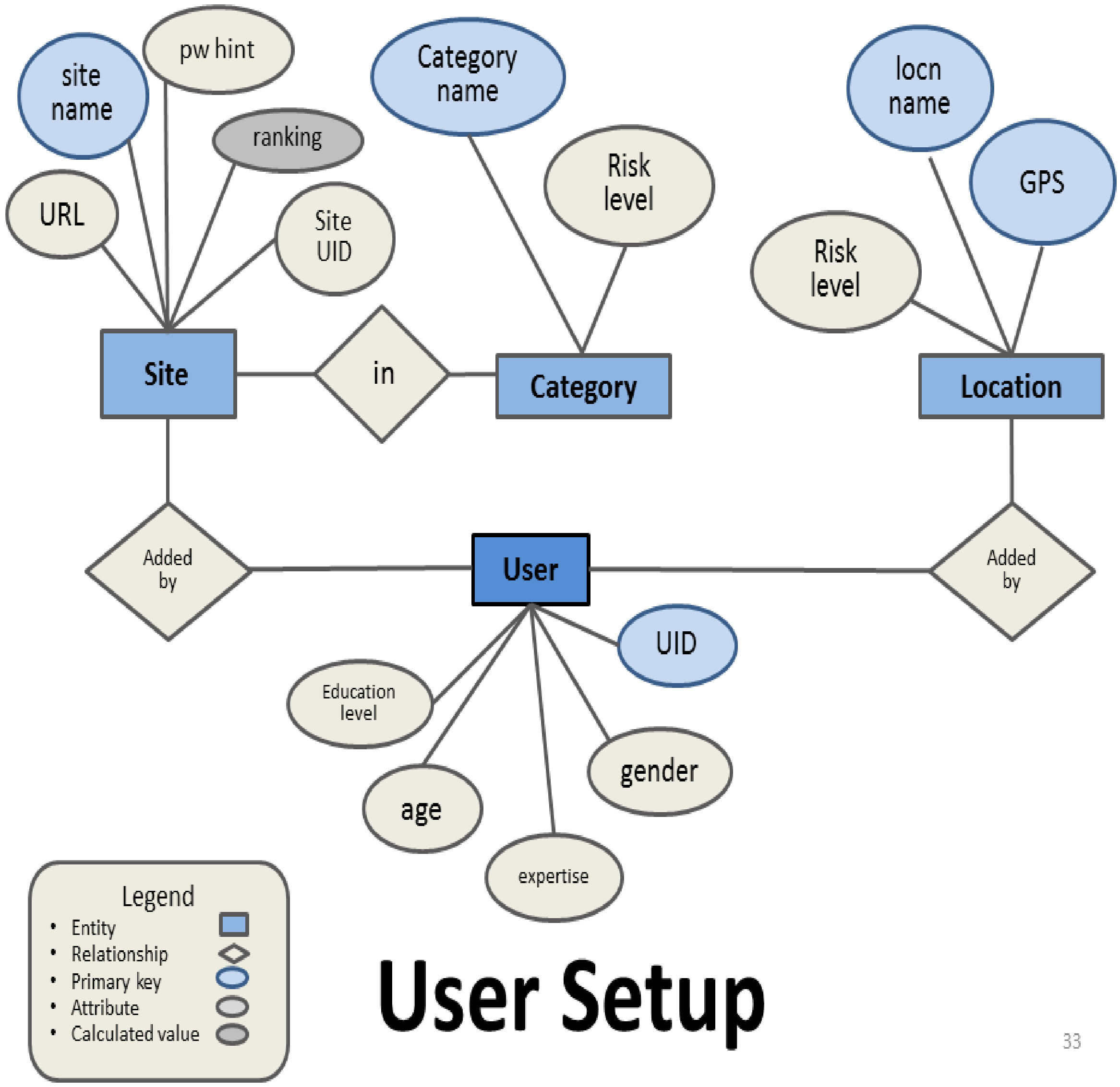


Figure 15. Data Model of User Setup Done in Configuration.

The subjects interact with the CLUE interface for two weeks. A minimum amount of usage was required to receive the incentive. A data model of the configuration and data collection appears in Figure 15. At the end of two weeks, the subject was invited to take the satisfaction survey described in Phase 3 of evaluation. The following hypotheses are tested during this phase of the evaluation, as seen in Table 13.

Table 13. Phase 2 Hypotheses Tested

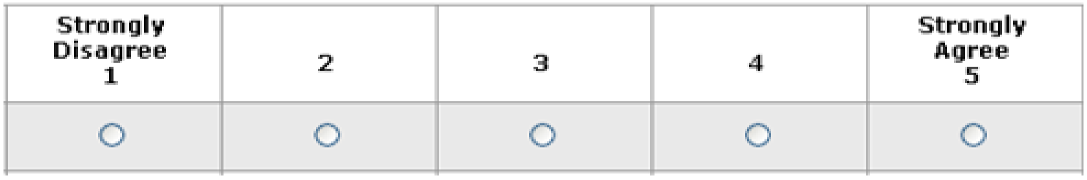
Hypothesis	**Variables**	**Indicators**
H0 - no impact	Security mode Success/Fail	There is no difference in the rate of successful usage Resource consumption will be the same across all modes Medium and low security modes will lower to no frequency of usage
H1- will increase the success	Success/Fail per usage and Security mode	Security modes with medium and low security will have a higher success rate
H3 – conserving power	#screen displays #processes # elapsed	Medium and low security modes will have lower power consumption recorded
H4 – reducing manipulation	#keystrokes #swipes/taps #Physical button push	Medium and low security modes will have less form factors recorded
H5 – reduce user effort	# pure recall # cued recall # multi-step sequences	Medium and low security modes will have less user effort requested

Data Analysis

The datasets with the usage data described in Figure 13**,** plus the demographic and configuration data described in Figure 15, were loaded into SPSS and Excel. The impact of applying the security principles was examined by looking at the rate of successful usage of the medium and low security modes. The frequency of how often the low and medium security modes are invoked shows how often the resources are conserved. The duration of usage was analyzed to determine the typical amount of time spent navigating authentication in both desktop and mobile environments in the original and new designs.

3.3.5 Phase 3 – User Satisfaction

The third study assesses user satisfaction using the survey method. Surveys are a widely accepted method for gathering this measure within both the security and usability communities (Bowen, Reeves, & Schweer, 2013). One of the most popular, and well-validated, is the Standardized Usability Scale (SUS), a standardized questionnaire created by Brooke (1996) at Digital Equipment Corporation (DEC) as a quick and dirty assessment of usability. Over 500 additional research studies applying SUS have proven that the scale is quick, but not so dirty assessment (Sauro, 2011). This questionnaire is considered the best of open-source norm available (Heeringa, West, & Berglund, 2010).



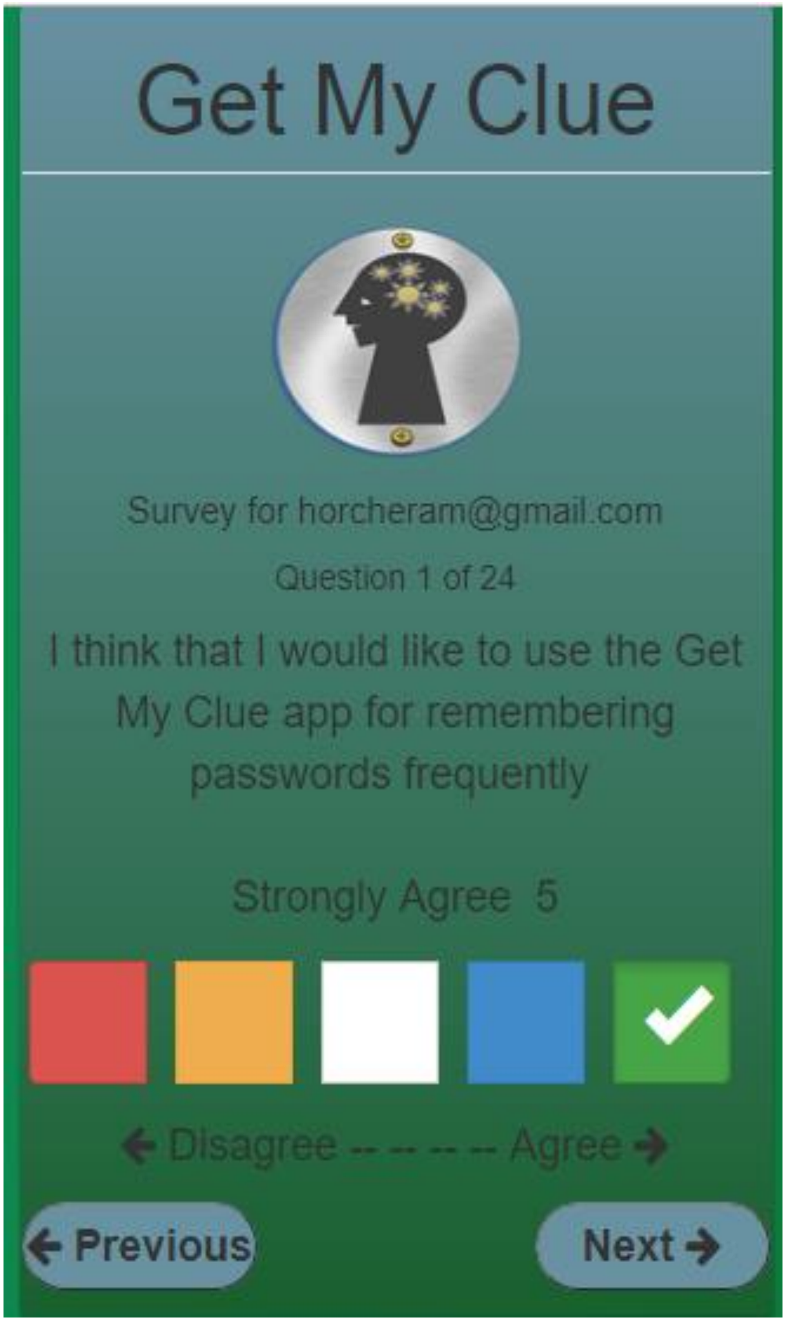
Strongly Disagree 1	2	3	4	Strongly Agree 5
○	○	○	○	○

Figure 16. Standard SUS Reported Likert Scale

The SUS uses the following response format shown in Figure 16. It uses a 5 point scale to assess user attitudes (Likert, 1932). The results of raw SUS scores when converted to percentiles yield a letter grade for the application which can be compared to other studies.

The goal of the survey was to evaluate the security interface within the CLUE artifact. Exposing subjects to another security interface to authenticate to collect survey data could influence the user perception of the target interface. To avoid this the presentation of the survey was designed according to the same usability principles as used for the CLUE interface, and matched to the look and feel of CLUE. The use of color with green to indicate positive and red to indicate negative, with white as neutral conserves user effort by indicating meaning without requiring the user to read the screen

(Figure 17). This follows the Finstad study that uses images to solicit responses to eliminate the need to read the scale (Finstad, 2010). The on-screen targets for responses are the recommended size of 9.2 mm to allow easy acquisition from a touchscreen (Parhi, Karlson, & Bederson, 2006).



Get My Clue

Survey for horcheram@gmail.com

Question 1 of 24

I think that I would like to use the Get My Clue app for remembering passwords frequently

Strongly Agree 5

Figure 17. Mobile-optimized Response Format with Color Coding

Survey Design

The SUS contains 10 items with those five response options, as seen in Table 14. The questions were all expressed as positives, instead of flipping between positive and negative. Recent research from Sauro and Lewis (2011) shows that reversing the direction of the usability evaluation can result in inconsistent answers if the subject responding does not notice the re-calibration in scale. The reverse a**lso** requires the researcher recode the responses to keep the scale consistent. The responses with a consistent scale direction (all positive) were demonstrated to have similar accuracy to the traditional reversing scale.

Table 14. Standardized Usability Survey – Positive response (Sauro & Lewis, 2011)

Item #	**Question**
1	I think that I would like to use this system frequently
2	I found the system to be simple.
3	I thought the system was easy to use.
4	I think that I could use this app without the support of a technical person.
5	I found the various functions in this system were well integrated.
6	I thought there was a lot of consistency in this system
7	I would imagine that most people would learn to use this system very quickly.
8	I found the system very intuitive.
9	I felt very confident using the system.
10	I could use the system without having to learn anything new.

As recommended Sauro and Lewis (2011), the specific description of “CLUE” was inserted in place of the more generic term, “system.” The addition of actual system name instead of a generic does not affect validity of responses. Data analysis was done using the techniques described below on the standard subgroups within the questionnaire.

Subjects and Procedure

The subjects for the survey are the same participants used for Phase 2 study used to evaluate effectiveness. After two weeks of using the CLUE artifact, the subjects are prompted via email, and in the app, to fill out the exit survey. In each case the link to survey is specific to each user to allow correlation of survey data with demographic and usage information collected in Phase 2. The subjects receive an incentive for completing the survey. Subjects who do not complete the survey, do not receive the incentive.

Hypotheses Tested

The survey data will be evaluated to support or refute the hypotheses. Specific questions are mapped to specific hypotheses as shown in Table 15.

Table 15. Phase 3 Hypotheses Tested

Hypothesis	**Measurement**	**Measuring success**
H1- Applying principles will increase the success of the user in completing authentication	Examine questions about success (#1,#2,#3,#5,#6,#7,#8,#9 on SUS)	Favorable rating received as answers on usability questions
H4 – reducing manipulation	Examine questions about manipulating the system (#2, #6, #8)	Positive rating received as answers on these questions
H5 – conserving user effort	Examine questions that address user cognitive effort (#4, #5, #7, #10)	Positive rating received as answers on these questions

Data Analysis

The data analysis for the SUS response will use the accepted techniques for generating a grade from the raw score as described by Sauro (2011), and shown in Table 16. In addition analyzing the subscales for learnability and usability (Lewis and Sauro 2009) will provide measures to support or refute the hypotheses related to conserving user effort and manipulation of form factors as described in Evaluation above. The techniques provided in Table 16 provide a letter grade that indicates a favorable or unfavorable rating. That is the advantage to SUS – the letter grade is a standard output of the data analysis.

Table 16**.** Statistics Analysis for SUS Data *(Sauro, 2011)*

Stat	**Description**
Percent Agree	summarize the percent of respondents who agreed to the item
Top-Box	For 5-point scales the top box is strongly agree
Net Top Box	The number of respondents that select the top choice (strongly agree) minus the number that select the bottom choice (strongly Disagree choice
Z-Score to Percentile Rank	This is a Six-Sigma technique. It converts the raw score into a normal score—because rating scale means often follow a normal or close to normal distribution.
Coefficient of Variation	Used instead of standard deviation because there is a mix of scale points in data. The CV divides the standard deviation by the mean. (1 Higher values indicate higher variability)

3.4 Summary

This chapter provided an introduction to security usability and design science research methodology. The mapping of security design principles to usability principles yielded a combined set of principles. According to this mapping, usability is a subset of good security. The limited resources on the mobile platform are described. The combined security-usability principles will be focused according to the limitations of the mobile platform. This will produce a set of security-usability principles focused on the mobile platform.

Once the theoretical background was explained, the research design was presented. The research design reviewed the research methodology, with a high level breakdown of the data collection and analysis. The data collection and analysis section provided the necessary research steps required. The instantiation of the principles was done in three phases, with data collected that related to efficiency, effectiveness, and user satisfaction. Each phase evaluated one or more of the hypotheses, with some of the hypotheses evaluated in all three phases. The measures used for determining the support or non-support of the hypotheses were identified for each phase. Materials and resources were then identified for completing the study.

.

Chapter 4

Results

This chapter reports the results from the data collection described in Chapter 3. Each phase is reported separately. The data collected for the phase is summarized in a table and displayed in a graph, where appropriate. After the results for each phase the hypotheses that were tested in that phase are refuted or confirmed.

4.1 Phase 1 – CogTool Analysis of Efficiency

As described in the methodology, the current state of basic authentication is represented by the risk mode labelled "High." Six different designs were mapped in CogTool, representing High, Medium, and Low risk modes on both a desktop and mobile platforms. Four primary security-related tasks were modelled including logon attempts, recovering user identifiers and password, and getting a clue to recall a password.

CogTool provides the ability to export the demonstration as a series of steps to a comma-limited values (CSV) file, but the difficulty score is not 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 by CogTool (Table 17). Power and user effort both only related to one Cogtool action. Assigning a difficulty for cognitive effort tasks requires consideration of the mental task being performed (Shankar, Lin, Brown, & Rice, 2015). Within the Cogtool predictions there needs to be an adjustment for mental effort for more complex tasks. The most complex task, computing a new password, has the most analysis and consequently the greatest difficulty.

Table 17. Difficulty Scores in Seconds for Constrained Resources by Action

Action to Measure	**Constrained Resource**	**CogTool Equivalent**	**Difficulty Desktop**	**Difficulty Mobile**
Display a screen	Power	Look at	0.5 sec	0.5 sec
Recognition	user effort	Think	1.2 sec	1.2 sec
Decide	user effort	Think + Think +Think Decision require evaluation of option 1, evaluation of option 2, and choice.	3.6 sec	3.6 sec
Compute input	user effort	Think + Think + Think + Think A multiple step mental process with a recall of requirements like password, and composing an entry that meets the rules.	4.8 sec	4.8 sec
Input character	form factor	Input lower case character	0.4 sec	1.8 sec
Input UC	form factor	Input upper case character	0.6 sec	3.4 sec
Input Special	form factor	Input special character	0.7 sec	5.1 sec
Input UClc	form factor	Input upper case followed by lower case	1.0 sec	5.1 sec
Move and Tap	form factor	Move finger to target and Tap touchscreen	NA	0.6 sec
Move Mouse	form factor	Move Mouse to target and Left Click	2.0 sec	NA
Move-no-think	form factor	Move Mouse from muscle memory	0.9 sec	NA

Actions represent a discrete activity accomplished by the user, similar to the atom in chemistry. Within the actions are smaller components, which appear within the CogTool scripts and are automatically added as an action is demonstrated. Because no password recovery was available in the High and Medium risk modes, the values are identical to password reset are used because that is the action taken by the user. Password reset is identical between the three design modes, because it is outside the webapp and is based on interaction with the Google Firebase authentication architecture.

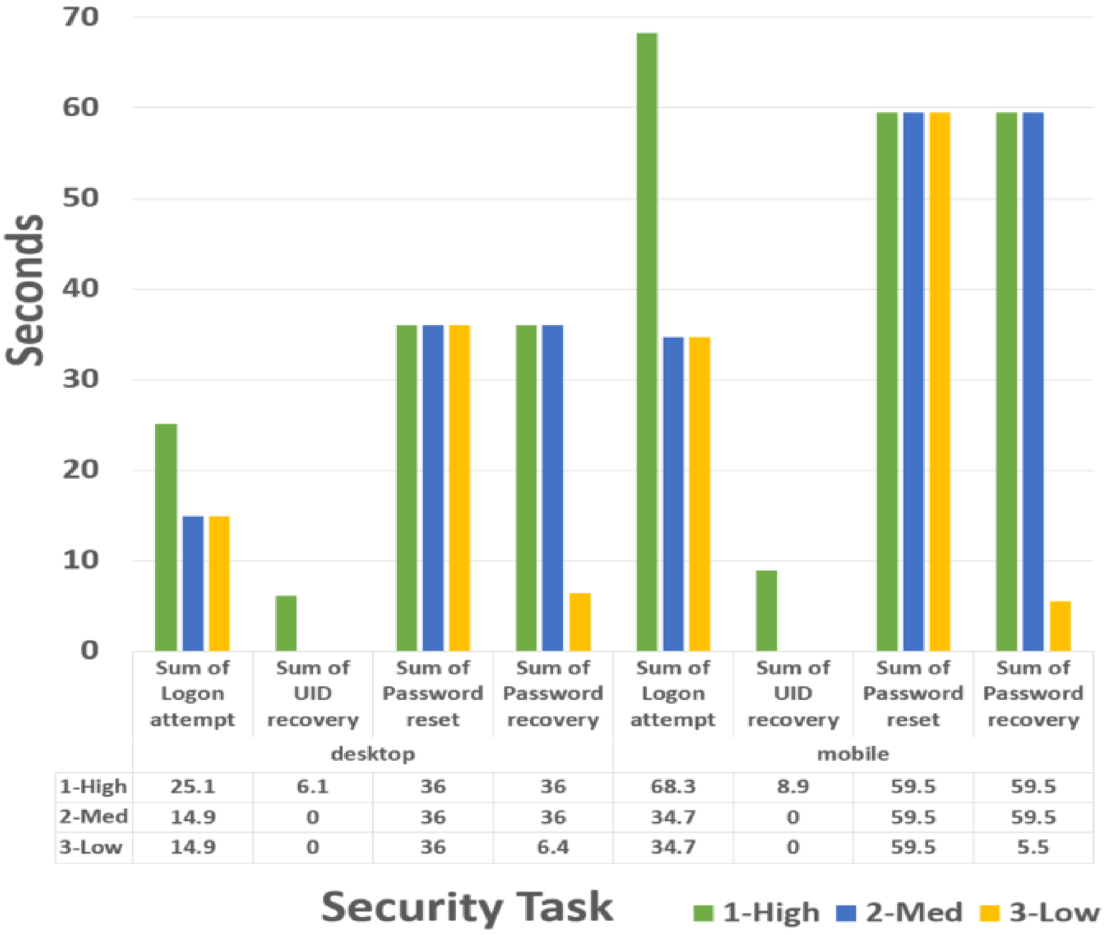


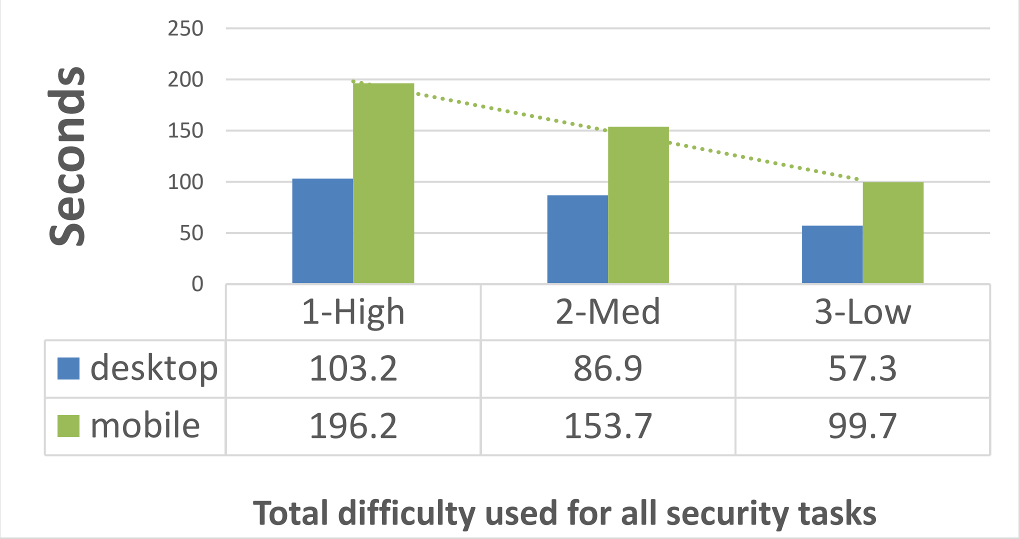
Figure 18. Compare All Security Tasks for All Risk Modes

The Cogtool score was also generated for the overall design of each version of the security interface design by combining the scores from all the security tasks (Appendix F

- CogTool Mapping Data). The scores for power consumption from a screen display were auto-generated based on the assumptions made by Cogtool. Wherever Cogtool determined a new screen had appeared, a “Look At” action was added to the script which is mapped to a use of power.

Other actions are also auto-generated by Cogtool based on the database of human performance modelling data. For example, every keyboard press automatically creates a hand movement action with the correct hand that would be used by typist using 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 (John, 2011).

An overall score for all security task demonstrations appears in Figure 19. As suggested by the greater form factor difficulty for individual actions (Table 17), 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 improvement on scores were generated for “High.”



	1-High	2-Med	3-Low
🟦 desktop	103.2	86.9	57.3
🟩 mobile	196.2	153.7	99.7

Figure 19. Total Difficulty for Each Design for All Resources

The Logon Attempt and Password Reset security tasks were projected to be the most difficult task according to the Cogtool measure. Logon Attempt is simply the successful input of a UID and password. The Logon Attempt typically occurs on every usage of an application. Making this task more usable would have frequent and high impact on user satisfaction for both desktop and mobile. But for mobile, the Cogtool score for the Logon Attempt task is three times higher for mobile versus the desktop platform (Figure 20). Moving the Logon Attempt task as designed for desktop to mobile, which is represented by "Highmobile", does not conserve the constrained resources and results in lower usability.

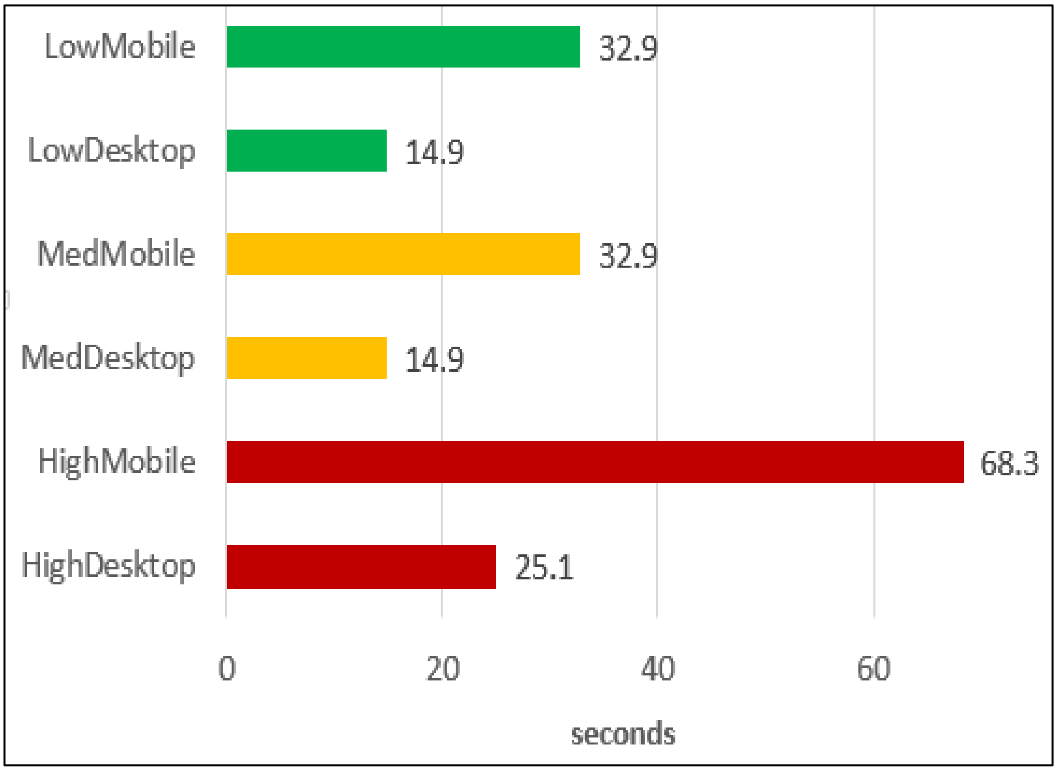


Figure 20. Difficulty in Seconds of Logon Attempt Comparison

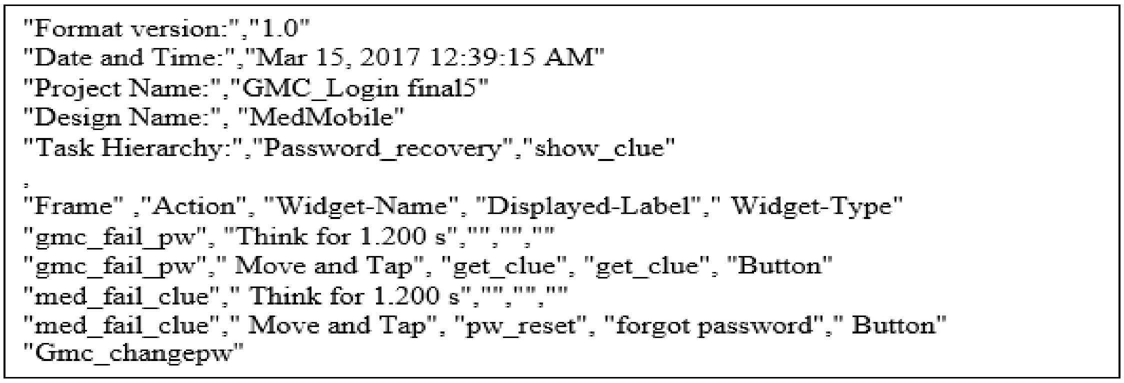
4.1.1 Understanding the Security Task Components of Constrained Resources

The Logon Attempt is broken into subtasks (Table 18). The detail shows the subtasks of inputting both UID and password are responsible for most of the difficulty.

Table 18. Detailed Difficulty Scores for Subtasks of Logon

Task	High Desktop	Med Desktop	Low Desktop	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

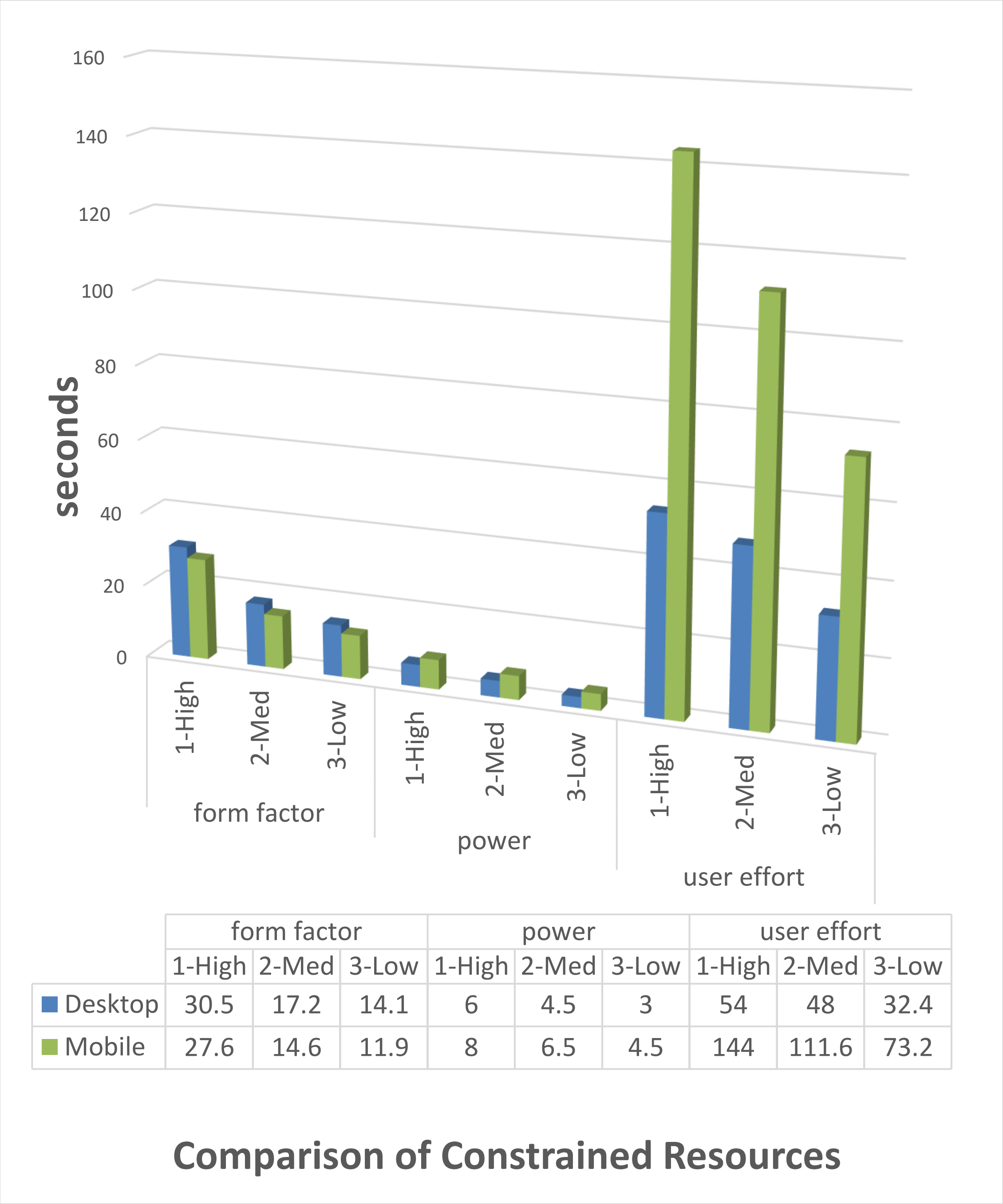
To check if the constrained resources consumed by each design are conserved, the CogTool scores for each action were mapped to the constrained resources. Each CogTool script for each sub-task of each security task was exported individually as a Comma Separated Variable (CSV) file. (Figure 21). All of the scripts were combined to



```
"Format version:","1.0"
"Date and Time:","Mar 15, 2017 12:39:15 AM"
"Project Name:","GMC_Login final5"
"Design Name:", "MedMobile"
"Task Hierarchy:","Password_recovery","show_clue"
,
"Frame" ,"Action", "Widget-Name", "Displayed-Label"," Widget-Type"
"gmc_fail_pw", "Think for 1.200 s","","",""
"gmc_fail_pw"," Move and Tap", "get_clue", "get_clue", "Button"
"med_fail_clue"," Think for 1.200 s","","",""
"med_fail_clue"," Move and Tap", "pw_reset", "forgot password"," Button"
"Gmc_changepw"
```

Figure 21. Cogtool Script

one file, and then processed with a Visual Basic (VB) program to assign constrained resources to actions. The graphs and data table below show how each constrained resource is conserved for the two revised designs, Medium and Low (Figure 22).



	form factor			power			user effort		
	1-High	2-Med	3-Low	1-High	2-Med	3-Low	1-High	2-Med	3-Low
🟦 Desktop	30.5	17.2	14.1	6	4.5	3	54	48	32.4
🟩 Mobile	27.6	14.6	11.9	8	6.5	4.5	144	111.6	73.2

Figure 22**.** Comparison of Constrained Resources

As stated previously, the Cogtool score is based on a database of multiple users performing a task generated by the ACT-R Engine (Teo, John, & Blackmon, 2012). The dependent variable for the analysis is the Cogtool score in seconds for each individual security task. The Cogtool score is a baseline, not a mean. The following equation describes the hypotheses:

H0 – Baseline $_{\text{Cogtool High}}$ <= Baseline $_{\text{Cogtool Medium}}$ or Baseline $_{\text{Cogtool Low}}$

H1 – Baseline $_{\text{Cogtool High}}$ $>$ Baseline $_{\text{Cogtool Medium}}$ and Baseline $_{\text{Cogtool Low}}$

When comparing Cogtool scores of a user interface design the previous studies use a reduction in interface completion time as the standard for indicating the measure of an improved design (John, 2011). To compare the designs the percent improvement from the control value of "High" as well as projected improvement time was calculated (Table 19). Statistical significance is not as pressing as practical significance for software design (Khansa & Liginlal, 2009). A statistically significant difference does not drive the typical user to modify behavior, particularly security behavior (Gebauer et al., 2011).

Table 19. Percent Improvement of Overall Cogtool Design

Environment	Current Design (High) in seconds	Revised Design in Seconds	Percent Improvement	Perceived Improvement in seconds (conserved resources)	Risk level
Desktop	103.2	86.9	15.79%	16.3	medium
Desktop	103.2	57.3	44.48%	45.9	low
Mobile	196.2	153.7	21.66%	42.5	medium
Mobile	196.2	99.7	49.18%	96.5	low

The user is motivated to change by a perceived less interruption time by the security interface to the primary task. The measures shown relate the following hypotheses:

- H0: CLUE will have no impact on the usability of basic authentication
- H1: CLUE will increase the user success navigating basic authentication
- H2: CLUE will improve the user experience of using basic authentication

Because the measures on both desktop and mobile show improvement from the current norm (High) for both revised designs the null hypothesis is refuted. Consequently H2 User Experience is proven because in Cogtool scores a design which takes less time to use is an improvement.

The three other hypotheses evaluated in Phase 1 of the study that explore the individual constrained resources are as follows:

- H3: CLUE will improve usability by reducing the power consumed by reducing the frequency of issuing the security challenge
- H4: CLUE will improve usability by minimizing manipulation of the device during authentication in ways such as keystrokes and screen swipes
- H5: CLUE will improve usability by conserving user effort such as memory recall, and task identification

As shown in Table 20, the Cogtool scores of the individual sub-tasks that consume the constrained resources of form factor, power, and user effort are compared to the current norm on both desktop and mobile. All three constrained resources are conserved in both the Medium and Low designs The Low risk design, as expected, conserves a higher amount of the those resources.

Table 20. Improvement for Constrained Resources in Design

Environment	**Resource**	Control (High) in seconds	Design Change in seconds	% Improved Medium	Perceived in seconds
Medium					
Desktop	form factor	30.5	17.2	43.61%	13.30
Mobile	form factor	27.6	14.6	47.10%	13.00
Desktop	power	6	4.5	25.00%	1.50
Mobile	power	8	6.5	18.75%	1.50
Desktop	user effort	54	48	11.11%	6.00
Mobile	user effort	144	111.6	22.50%	32.40
Low					
Desktop	form factor	30.5	14.1	53.77%	16.40
Mobile	form factor	27.6	11.9	56.88%	15.70
Desktop	power	6	3	50.00%	3.00
Mobile	power	8	4.5	43.75%	3.50
Desktop	user effort	54	32.4	40.00%	21.60
Mobile	user effort	144	73.2	49.17%	70.80

4.1.2 Phase 1 – Summary and Commentary of Results

Applying the design changes to traditional desktop did not result in the same magnitude of improvement as seen in mobile. This is understandable, because the design principles target **mobile** constraints. The security task for password reset did not have any design changes for any risk level on either mobile or desktop, so it would not show an improvement. The password reset is outside of the webapp created for DSR artifact.

Password recovery, only available in low risk mode, was available within the webapp and showed improvement.

Table 21. Phase 1 Summary of Results

Hypothesis	**Measurement**	**Measuring success**	**Supported**
H0 –no impact	Overall CogTool score for all security tasks	High risk Cogtool score is lower than CogTool score for the Medium and Low Risk (**Table 19**)	No
H1 – impact on usability	Overall CogTool score for all security tasks	High risk Cogtool score is higher than CogTool score for the Medium and Low Risk (Table 19)	Yes
H2 - improve the user experience	CogTool score of each security task for each platform and each security mode	CogTool score for Low and Medium risk are lower than High risk for using for overall design (Table 19)	Yes
H3 – conserving power	CogTool score for power subtasks that make up the security tasks	CogTool score for power subtasks are lower in revised design (Table 20)	Yes
H4 – reducing manipulation	CogTool score for form factor subtasks that make up the security tasks	CogTool score for form factor subtasks are lower in revised design (Table 20)	Yes
H5 – conserving user effort	CogTool score for user effort subtasks that make up the security tasks	CogTool score for user effort subtasks are lower in revised design (Table 20)	Yes
H6- Mobile vs. desktop	Overall CogTool score for each security task	CogTool score for security tasks on mobile vs. Cogtool score on desktop (Figure 18)	No

Even though the design changes result in a lower Cogtool score for Mobile in the medium and low risk modes, the scores are still not as low as in the Desktop platform. This indicates more constrained resources need to be conserved than this instantiation on the CLUE artifact to achieve parity with security usability on Desktop. Therefore H6 is refuted.

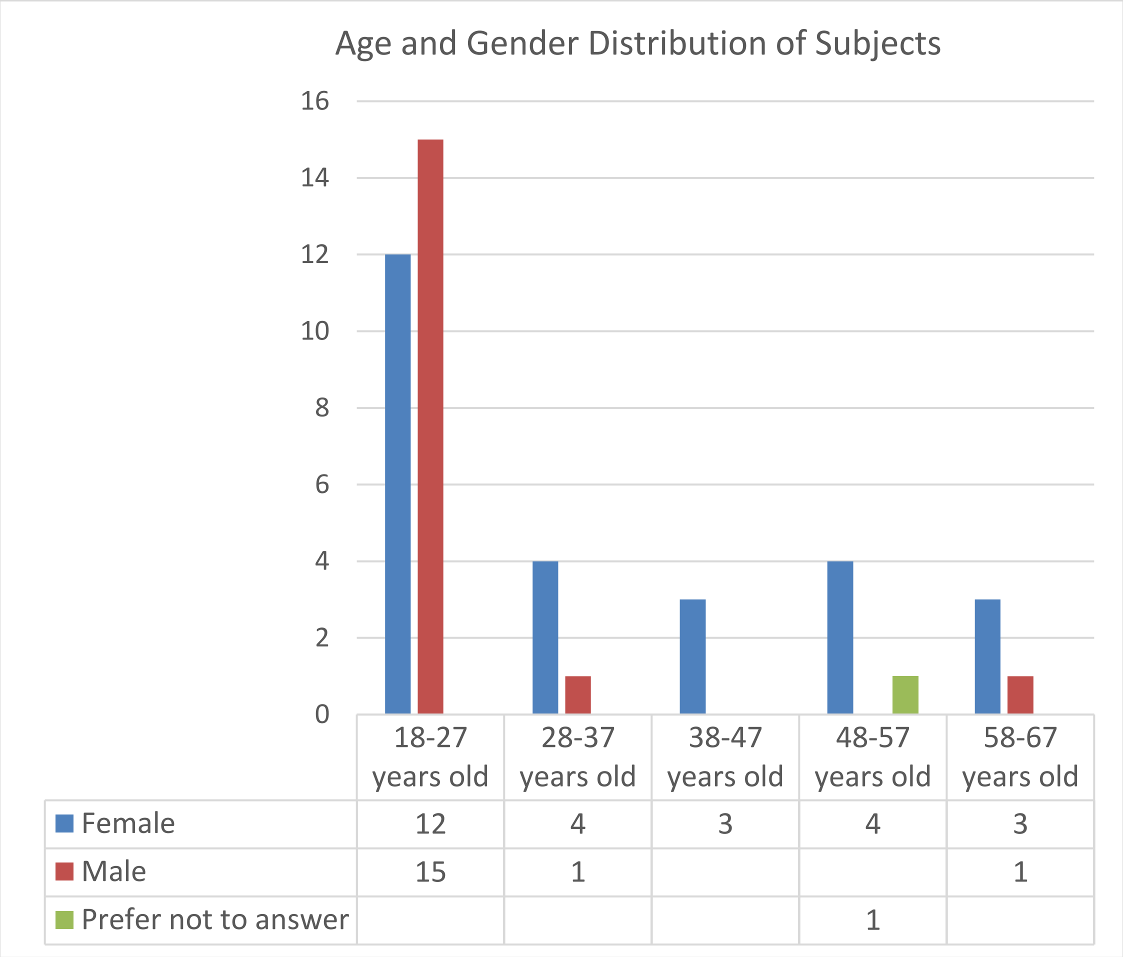
4.2 Phase 2 Usage Data

As described in 3.3.4, an artifact was created according to DSR methodology to evaluate the design principles proposed. The structure of the web application (webapp) that collects the data is described in Appendix G – Data Definitions of Firebase Usage Data. In the first use of the webapp the subjects set the risk level of various locations based on GPS. When the user logs into the webapp, the location determines the security level of the webapp. Subjects received more assistance navigating security in locations that had lower risk. The data was collected over a period of six months, and includes approximately 1700 uses of the webapp to navigate security interfaces. The next sections first discuss the demographic data about the subjects who participated in the study. Next the data from the use of the webapp is analyzed to provide support for the hypotheses proposed in 3.3.2.

4.2.1 Demographic Data

A convenience sample of forty-four individuals were successfully recruited to participate in the study. The participants were university students, small business owners, and technical women belonging to Anita Borg Institute group called Systers. The participants were grouped into five equal age ranges between greater than 18 and less than or equal to 67. Figure 23 presents the five age groups along with number of participants in each group, and separated by gender.

Within the youngest group male participants are the majority. But in the older groups females predominate. Females are also roughly 60% of the sample. Since one of the recruitment groups was made up of technical women of all ages, the predominance of women is expected. Though 118 potential participants were filled out the pre-study questionnaire to indicate interest in study, only 44 committed to participate. Even in the initial pre-study phase the interested female participants outnumbered potential male participants two to one (Appendix H Figure H 1. Gender Distribution of Potential Subjects).



	18-27 years old	28-37 years old	38-47 years old	48-57 years old	58-67 years old
🟦 Female	12	4	3	4	3
🟥 Male	15	1			1
🟩 Prefer not to answer				1	

Figure 23. Participants by Gender and Age

The pre-study questionnaire also had potential subject report their educational level (Figure 24) and technology expertise (Figure 26). All participants reported having completed High School/GED, and almost half of the participants reported having at least a Master's degree. The highest educational level reported were eight Ph.D. degrees.

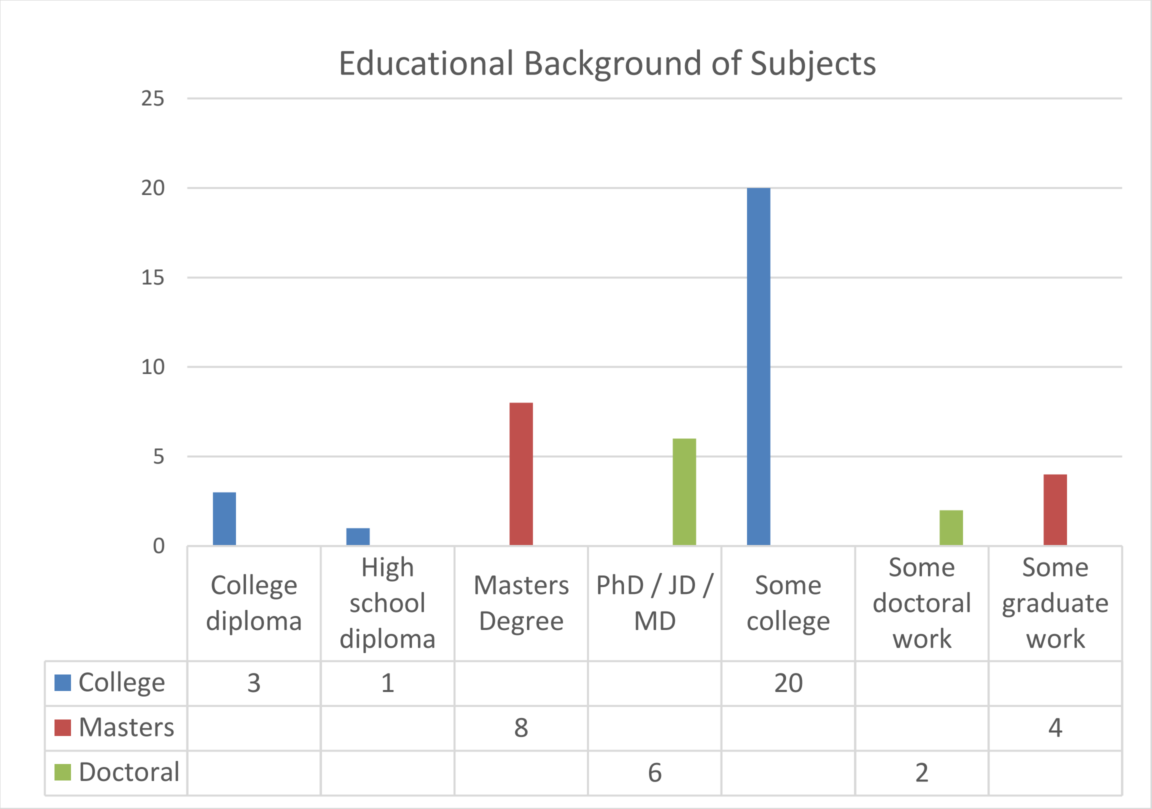
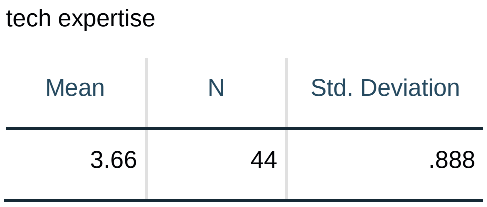


Figure 24. Educational Distribution of Subjects

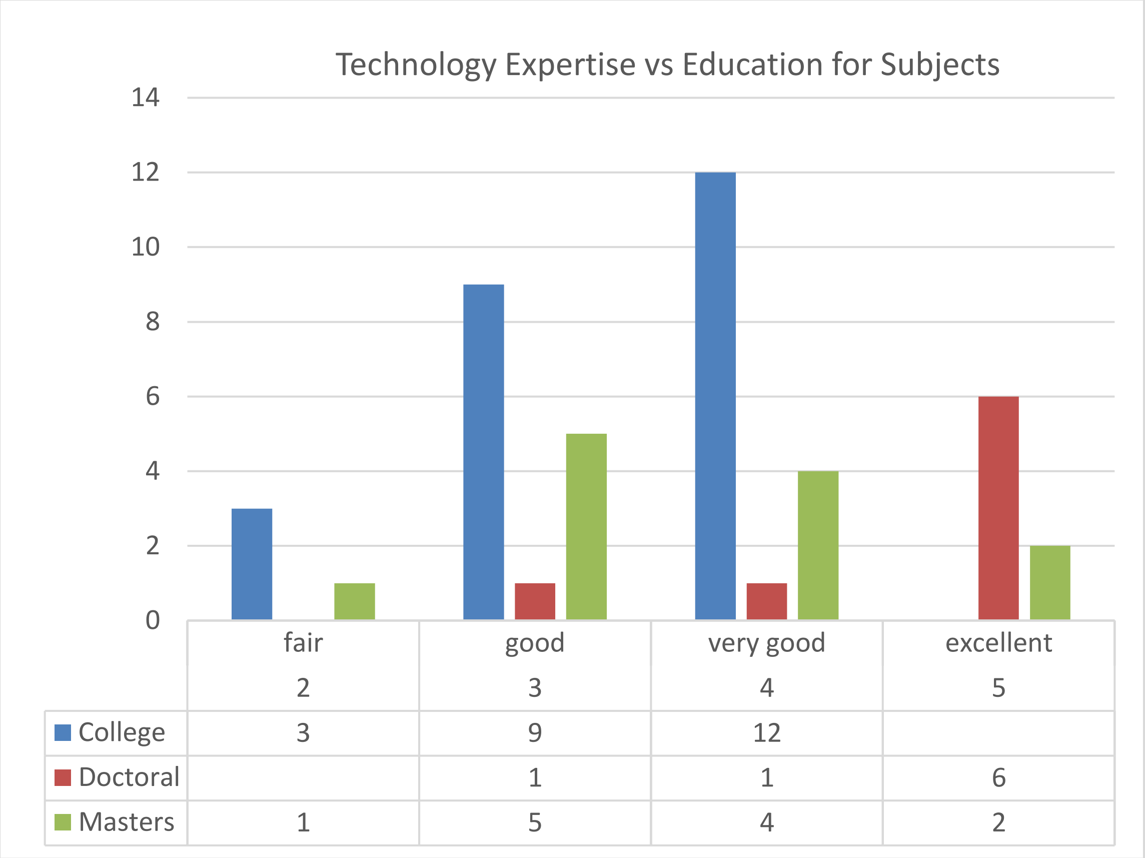
The subjects' assessment of their own technology expertise showed confidence in their skills. No one felt their ability was any less than fair. The mean value for technology expertise was 3.66, with a standard deviation of .888. The subjects with the highest levels of education assessed themselves as also having the highest levels of technology expertise.



tech expertise

Mean	N	Std. Deviation
3.66	44	.888

Figure 25. Mean and Standard Deviation of Technology Expertise



	fair 2	good 3	very good 4	excellent 5
🟦 College	3	9	12	
🟥 Doctoral		1	1	6
🟩 Masters	1	5	4	2

Figure 26. Technology Expertise vs. Education

Subjects were expected to have experience with smartphones. In the pre-study survey the subject reported themselves as using a mobile device daily or multiple times daily. This is in line with the reasoning that lead to the research questions. The smartphone phone and/or mobile device becoming the preferred delivery point for content.

Frequency of Mobile Device Use

gender	Mean	N	Std. Deviation
Female	4.77	26	.652
Male	4.94	17	.243
Prefer not to answer	5.00	1	.
Total	4.84	44	.526

Figure 27. Frequency of Mobile Device Use Mean and Standard Deviation

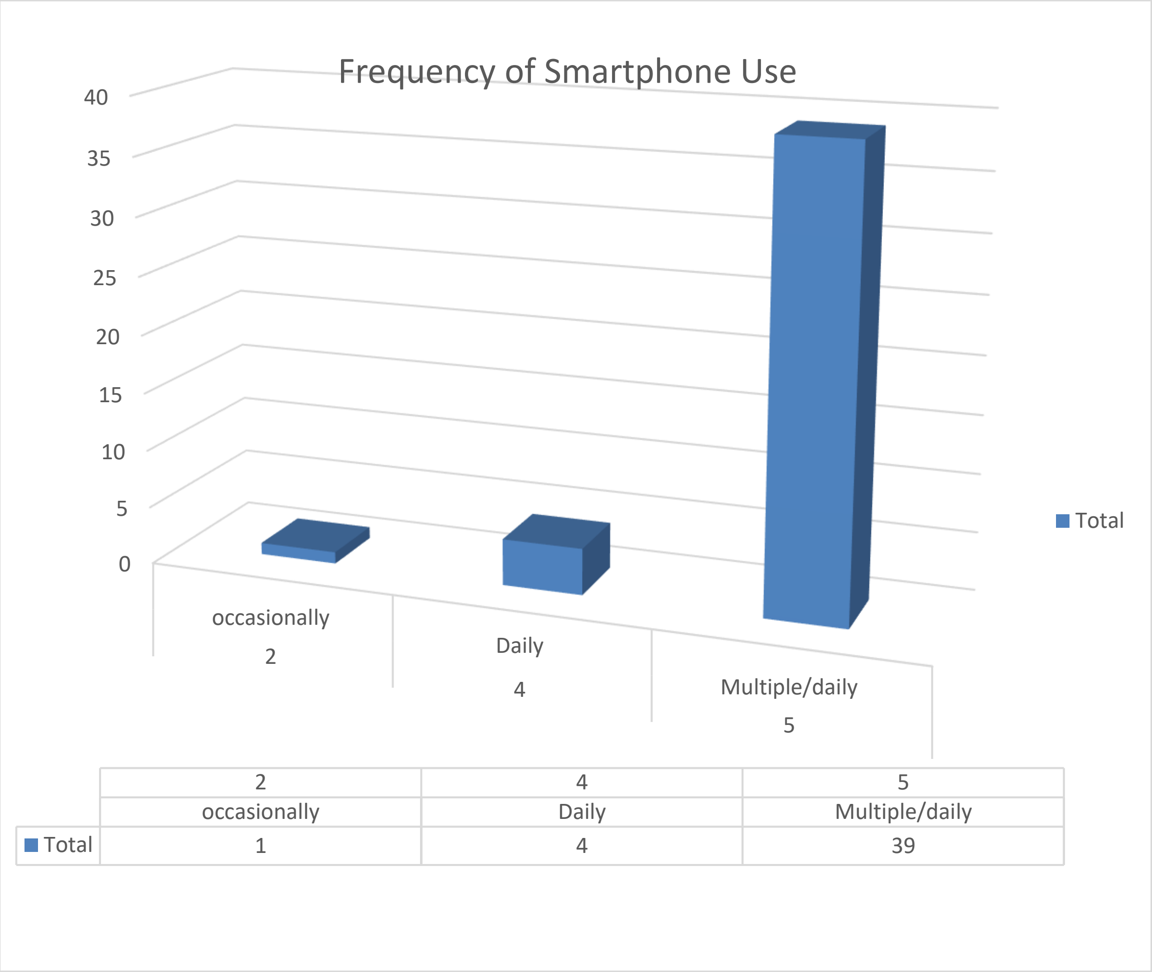


Figure 28. Frequency of Mobile Device Use

In summary, the subjects were two-thirds female, well-educated, technologically adept and daily users of mobile devices. Gender, age, and educational level were not analyzed as part of the hypotheses of the study. Use of a smartphone and technology expertise were required for successful completion.

4.2.2 Successful Usage of the Webapp

As stated in the methodology, the usage of the webapp CLUE determined the effectiveness of conserving constrained resources in the mobile security interface. The first measure taken was successful navigation of the security interface. As described in Appendix C – Task List for Study Participants, each subject performed a series of tasks. In these tasks the subject succeeded or failed in navigation of various security interfaces. The users chose which security mode they preferred to use, and how often they want to use the webapp. As discussed in 3.3.1, the successful navigation was marked by the retrieval of clue set by user. Low mode indicated password and userid retrieval success. Medium indicated userid retrieval. High, the current norm or the control, indicated success when the user needed no help, and failure when userid or password help was requested.

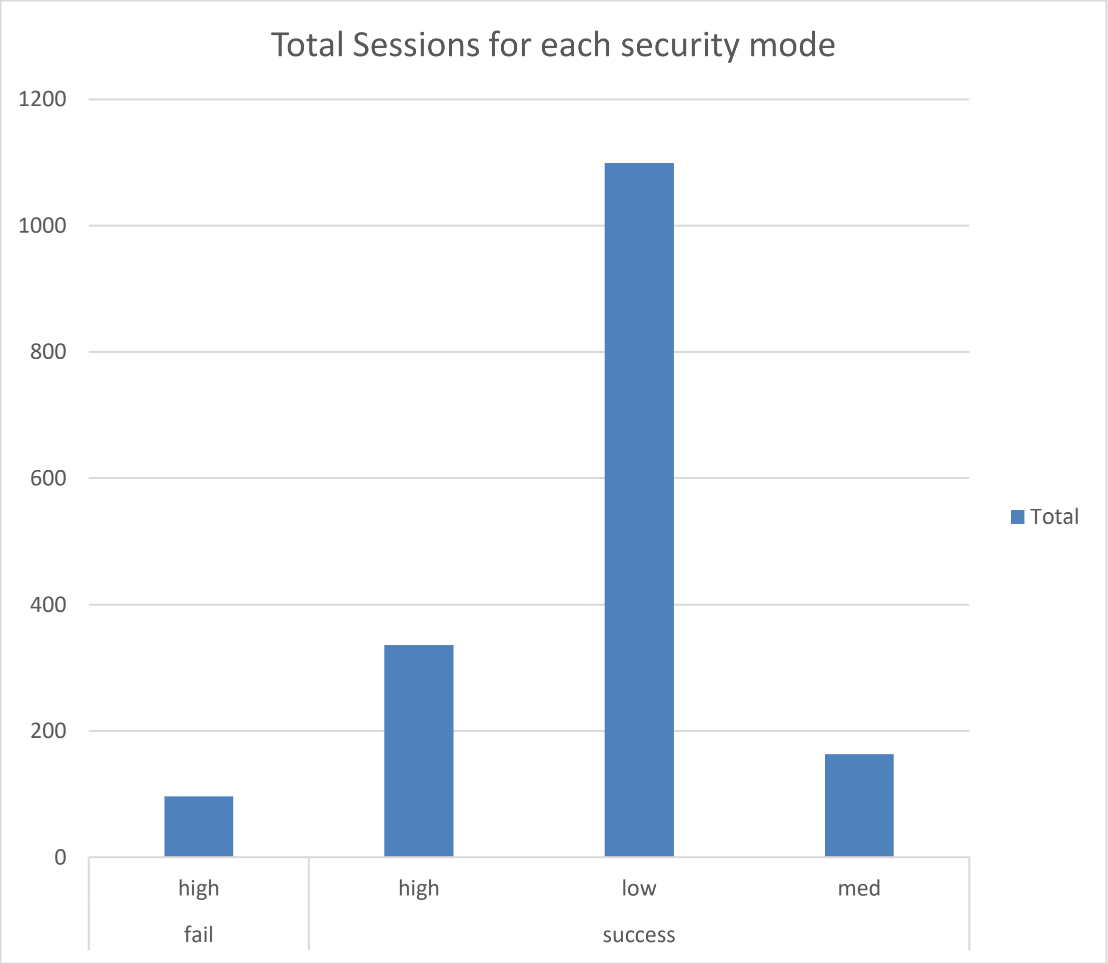


Figure 29. Sessions for Each Design Type with Success Rate

This measure shows the trend of the user preferring the low security mode which has the greatest conservation of constrained resources. It also shows unpopularity of the medium mode. This unpopularity was predicted by the Cogtool score for the medium design on the mobile platform and desktop. In Figure 30 the average duration of a session is compared to the number of total sessions and the total usage. Users who had the greatest difficulty in the first sessions stopped using the app. Anyone with more than seven sessions is using the app beyond the minimum listed in the task list. This also indicates success. Forty-five out of 54 subjects used the app beyond the training, or 83 percent.

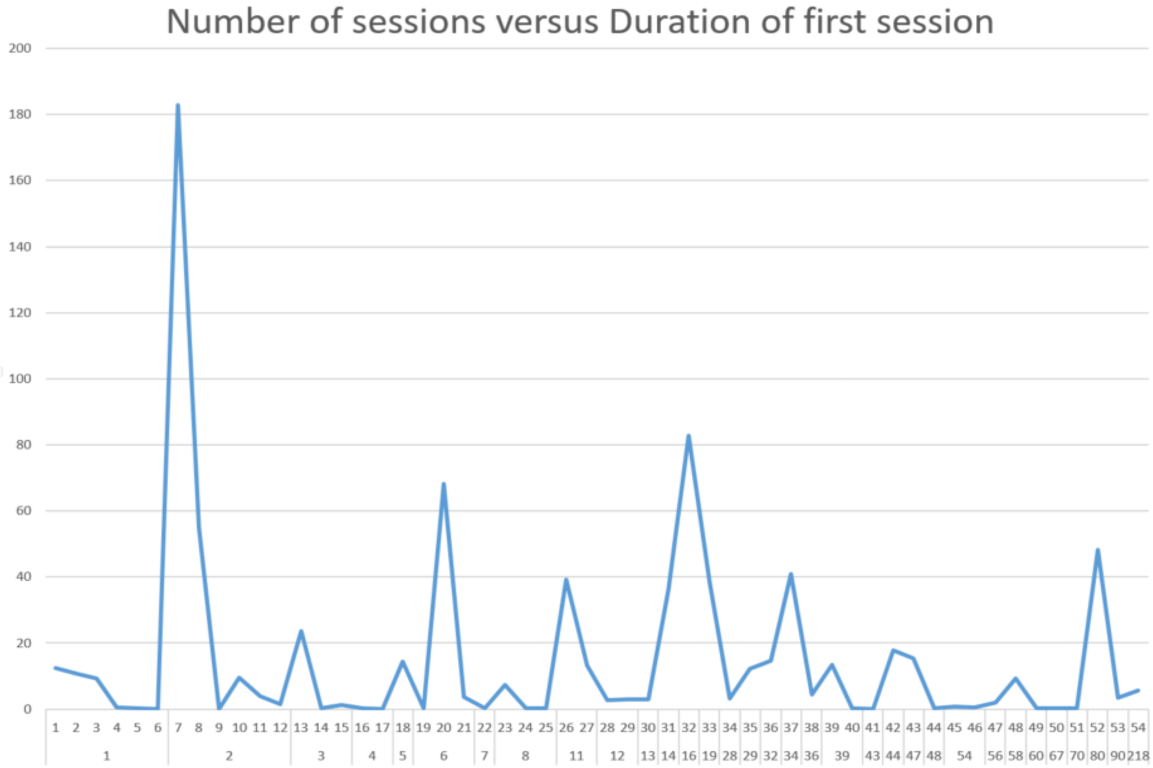


Figure 30. Number of session vs Average duration of a session

Both of these measures indicate a higher level of success when using the webapp CLUE. The zeroth hypothesis is disproven, and the H1 is proven.

4.2.3 Usage Conserving Constrained Resources

In Phase 1 – CogTool Analysis of Efficiency the seconds consumed by using power actions involving screen displays and processing was calculated using human performance modelling. The Cogtool measure of efficiency has been validated by previous studies (Abdulin 2011; Ocak and Cagiltay 2016) as being accurate for these actions on mobile. Conservation means the resources are not expended. Every action that uses a revised design mode conserves the difference between the constrained resources used by the original design and the revised design. The data about the resources consumed and conserved appears in Appendix I – Data from usage of Webapp CLUE.

Every action taken in the webapp that corresponds to one of the security tasks in Table 11 was logged. To calculate the impact of the conservation of constrained resources, each incidence of the security task was mapped to the measure of resource in seconds consumed. The measures of resource consumed and conserved appear in Appendix I – Data from usage of Webapp CLUE. Based on the usage data presented in 4.2.2, subjects preferred the webapp versions that conserved the constrained resources. The detailed usage describing which security tasks were performed by the users also shows the users prefer the "low" version of the design. The average amount of constrained resource conserved per security task is shown in Figure 31. Power is the resource that is conserved the least. User effort, or cognitive load has the largest amount of resource conserved.

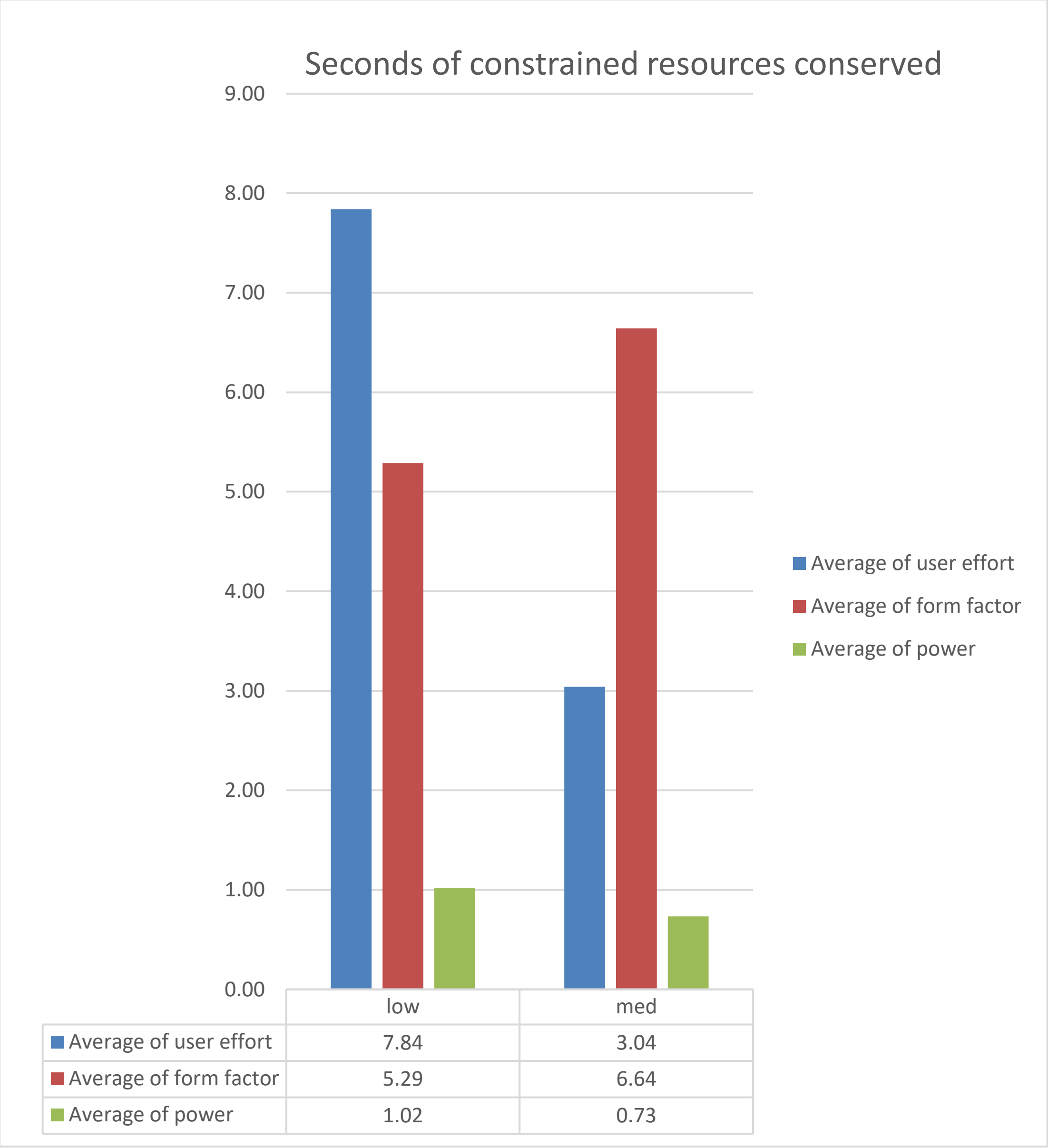


Figure 31. Average Constrained Resources Conserved per Task

4.2.4 Phase 2 – Summary of Results

Each category of resource is conserved for both low and medium modes. Hypothesis 3, which states the artifact will conserve power is supported. Hypothesis 4, which states the form factor manipulation is supported. Hypothesis 5, which states user effort will be conserved, is also supported.

Table 22. Phase 2 usage Hypotheses Proven

Hypothesis	Variables	Indicators	Supported
H0 - no impact	Security mode Success/Fail	There is no difference in the amount of successful usage (Figure 29)	No
H1- will increase the success	Success/Fail per usage and Security mode	Security modes with medium and low security will have a higher success rate (Figure 29)	Yes
H3 – conserving power	#screen displays #processes # elapsed	Medium and low security modes consume less power (Figure 31)	Yes
H4 – reducing manipulation	#keystrokes #swipes/taps #Physical button push	Medium and low security modes consume less form fate (Figure 31)	Yes
H5 – reduce user effort	# pure recall # cued recall # multi-step sequences	Medium and low security modes consume less user effort (Figure 31)	Yes

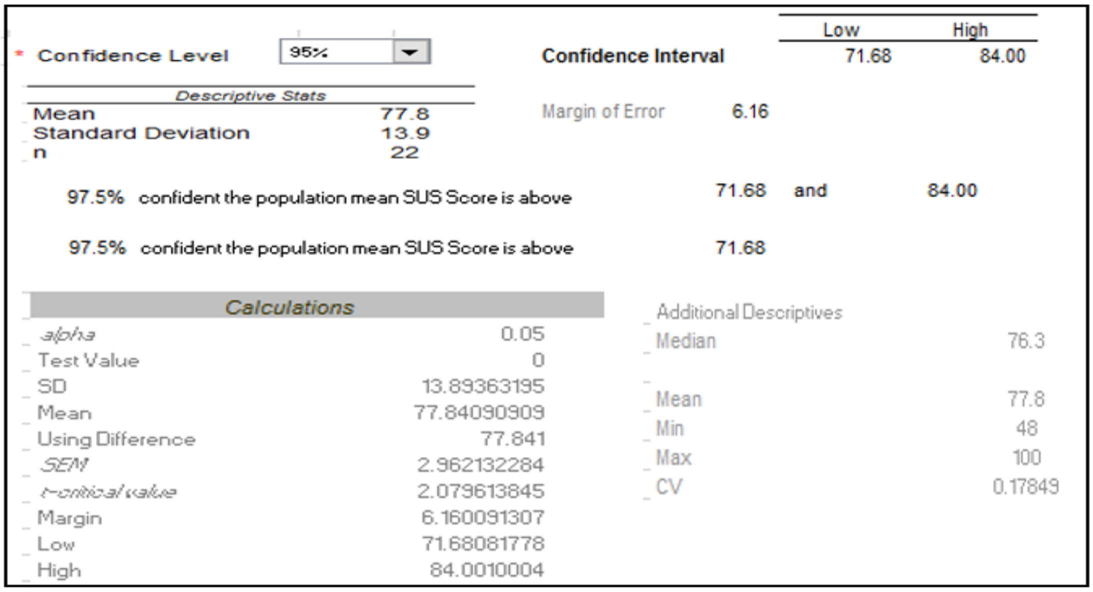
4.3 Phase 3 SUS Results for User Satisfaction

As stated in the methodology, participants of the study are asked to take a System Usability Scale (SUS) Survey to assess the webapp. In Phase 2 each subject experienced the security interface in some of the modes that conserved constrained resources on the mobile platform. These same modes were analyzed for efficiency in Phase 1 using human performance modelling.

The subjects accessed the mobile-optimized version of the SUS survey (Figure 17) in a webapp which stored the data in a no-SQL database from Google called Firebase.

The Firebase data was extracted and converted to Comma Separated Values (CSV) format. The CSV file was reformatted to present the information needed for SUS analysis.

The reliability and validity of SUS has been documented by 20 years of SUS Scores. Reliability refers to the consistent response to the items. SUS detects differences in smaller sample sizes (as few as two users) and generates reliable results. Validity refers to whether an instrument measures the target, which for SUS is perceived usability. SUS has been shown to effectively distinguish between unusable and usable systems and correlates highly with other questionnaire-based measurements of usability. These characteristics combine to make SUS an improvement to commercial alternatives and home-grown questionnaires (Sauro, 2011).



* Confidence Level 95%

	Low	High
Confidence Interval	71.68	84.00

Descriptive Stats	
Mean	77.8
Standard Deviation	13.9
n	22

Margin of Error 6.16

97.5% confident the population mean SUS Score is above 71.68 and 84.00

97.5% confident the population mean SUS Score is above 71.68

Calculations	
alpha	0.05
Test Value	0
SD	13.89363195
Mean	77.84090909
Using Difference	77.841
SEM	2.962132284
t-critical value	2.079613845
Margin	6.160091307
Low	71.68081778
High	84.0010004

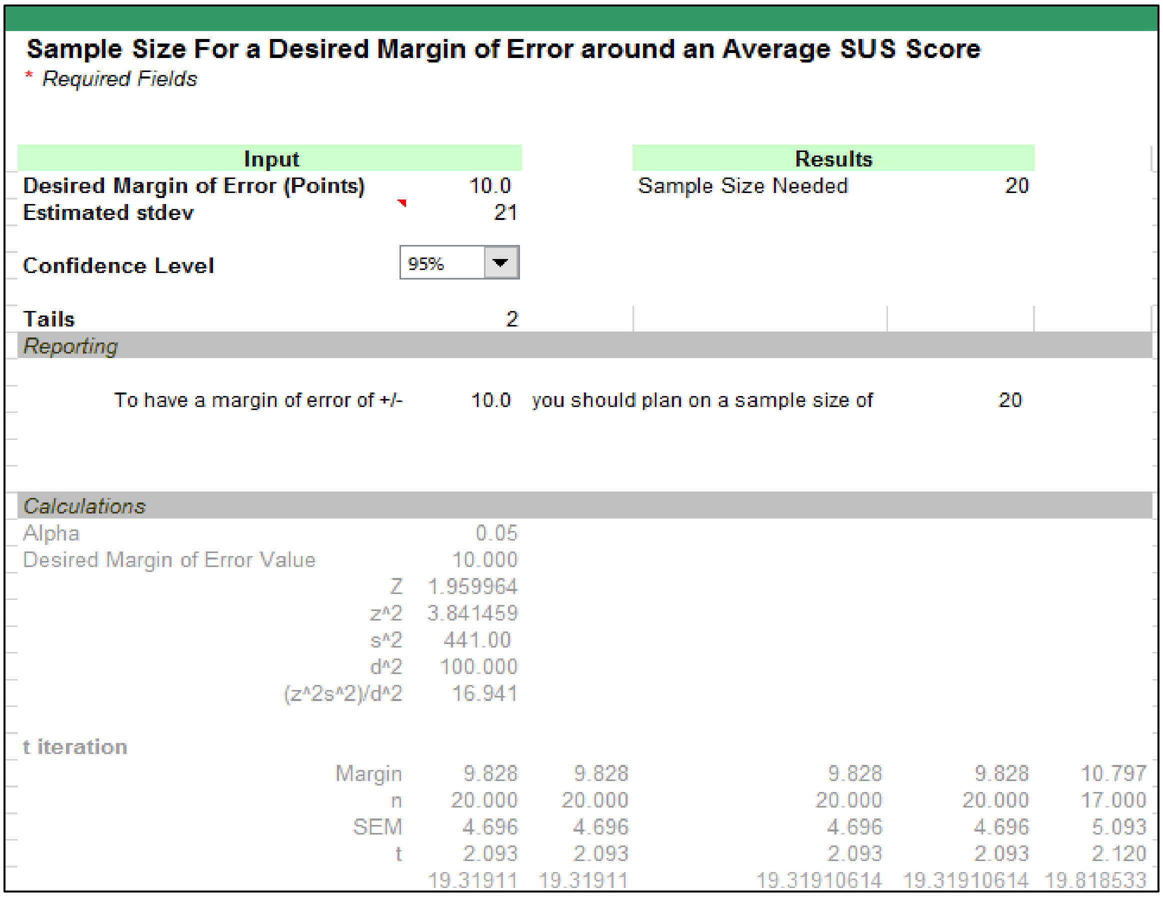
Additional Descriptives	
Median	76.3
Mean	77.8
Min	48
Max	100
CV	0.17849

Figure 32. Confidence Interval for SUS Analysis

4.3.1 Confidence Interval of SUS Data

The statistical analysis of the SUS data indicates a confidence interval of 90%.

The sample size required in SUS study for a margin of 10.0 is 20 subjects, as shown in Figure 33. The sample size for the SUS data in this research was 22 subjects, which means the study exceeded the minimum required to achieve this accuracy.



Sample Size For a Desired Margin of Error around an Average SUS Score

* *Required Fields*

Input		Results	
Desired Margin of Error (Points)	10.0	Sample Size Needed	20
Estimated stdev	21		
Confidence Level	95%		
Tails	2		

Reporting

To have a margin of error of +/- 10.0 you should plan on a sample size of 20

Calculations

Alpha	0.05
Desired Margin of Error Value	10.000
Z	1.959964
z^2	3.841459
s^2	441.00
d^2	100.000
(z^2s^2)/d^2	16.941

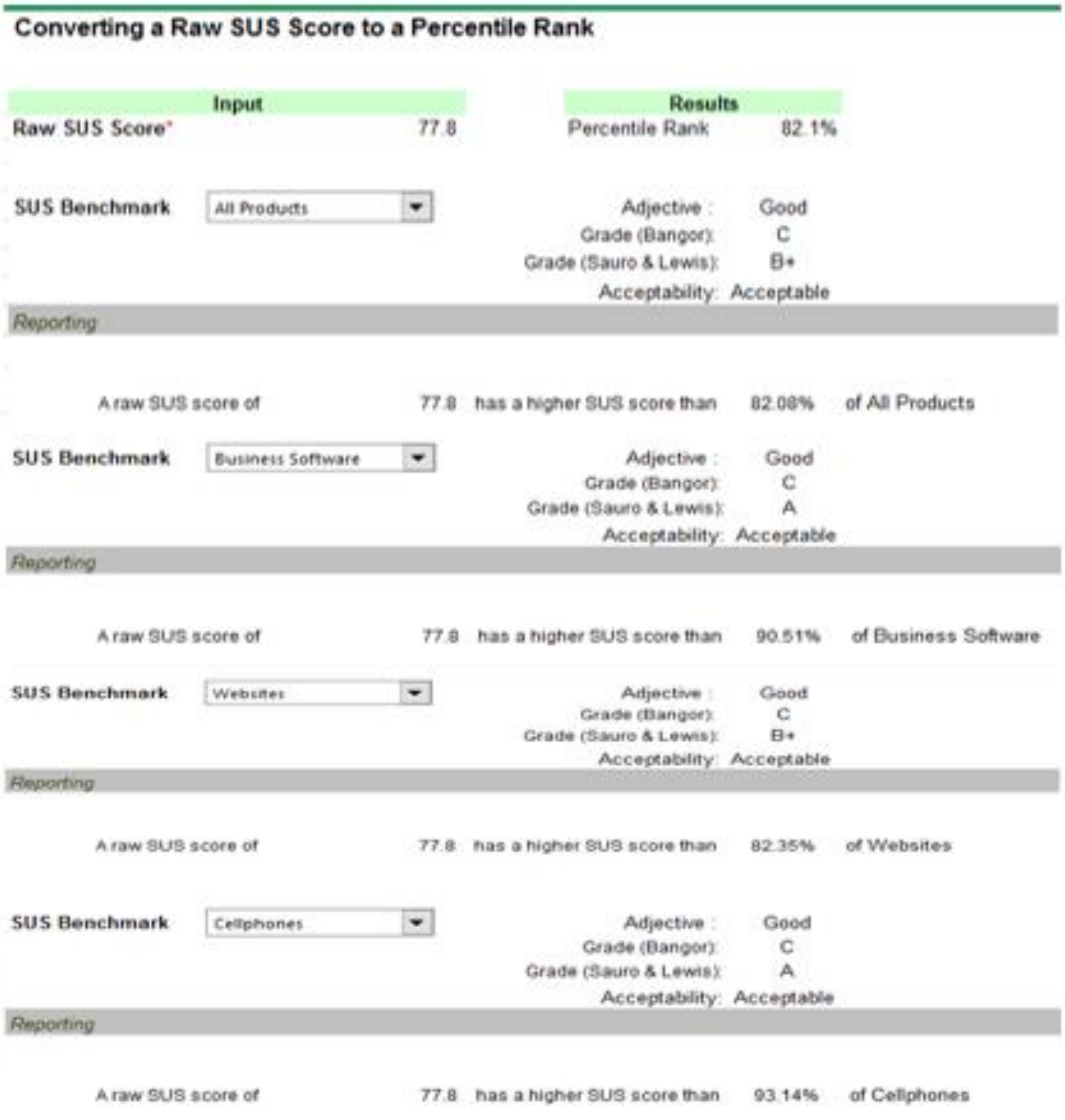
t iteration

Margin	9.828	9.828	9.828	9.828	10.797
n	20.000	20.000	20.000	20.000	17.000
SEM	4.696	4.696	4.696	4.696	5.093
t	2.093	2.093	2.093	2.093	2.120
	19.31911	19.31911	19.31910614	19.31910614	19.818533

Figure 33. Sample Size Calculation for +/- 10.0 Margin of Error SUS Accuracy

As described in Phase 3 – User Satisfaction, the SUS scale analysis converts the raw score to a letter grade and a percentile. The letter grade quickly communicates the usability of the software to the layperson in easily understandable terms. An adjective is also assigned to the usability ranging from Poor to Excellent to also communicate the usability in familiar words (Bangor, Kortum, & Miller, 2009). The type of task can affect the scoring. A single simple task will score lower than a multi-task sequence (Kortum &

Acemyan, 2013). When the percentile ranking of CLUE is compared to the various categories the letter grade changes as seen in Figure 34. The SUS analysis tool used to generate the grade provides both the Bangor value (Bangor et al., 2009) and Lewis and Sauro value (Lewis & Sauro, 2009). Bangor sets the scale for the letter grade higher, but both scores resolve to the same adjective, "Acceptable."



Converting a Raw SUS Score to a Percentile Rank

Input		Results	
Raw SUS Score*	77.8	Percentile Rank	82.1%

SUS Benchmark: All Products

Adjective : Good
Grade (Bangor): C
Grade (Sauro & Lewis): B+
Acceptability: Acceptable

Reporting

A raw SUS score of 77.8 has a higher SUS score than 82.08% of All Products

SUS Benchmark: Business Software

Adjective : Good
Grade (Bangor): C
Grade (Sauro & Lewis): A
Acceptability: Acceptable

Reporting

A raw SUS score of 77.8 has a higher SUS score than 90.51% of Business Software

SUS Benchmark: Websites

Adjective : Good
Grade (Bangor): C
Grade (Sauro & Lewis): B+
Acceptability: Acceptable

Reporting

A raw SUS score of 77.8 has a higher SUS score than 82.35% of Websites

SUS Benchmark: Cellphones

Adjective : Good
Grade (Bangor): C
Grade (Sauro & Lewis): A
Acceptability: Acceptable

Reporting

A raw SUS score of 77.8 has a higher SUS score than 93.14% of Cellphones

Figure 34. Summary of SUS Score compared to other software

The CLUE software has its highest letter grade when compared to cell phones and business software as also shown in Figure 34. The favorable comparison of CLUE to other cellphones indicates the mobile design principles improve usability perceived. All other calculations converting raw SUS scores to percentile also received an acceptable rating.

Two subscales of the SUS are used to measure learnability and usability (Sauro & Lewis, 2009). Questions #4 and #10 measure learnability and the other questions measure usability as successful use of the system. For this study a subscale was added to measure user effort. These questions addressed user perception of the system's demand on cognitive effort. A subscale was also added to address form factor. These questions addressed the user perception of interaction usability. The results of SUS data analysis appear in Table 23. The two new subscales were calculated by summing the values of the relevant questions, and then converting the sum to a percentile.

Table 23. SUS Results for Overall and Subscales

SUS scale name	Questions assessed	Description	Percentile
SUS overall	1-10	Entire questionnaire	77.8
Usability	1,2,3,5,6,7,8,9	Standard subscale (Sauro & Lewis, 2009))	77.7
Learnability	4, 10	Standard subscale (Sauro & Lewis, 2009)	78.4
Cognitive Load	4,5,7,10	Questions on cognitive effort based on conserved resources	78.8
Form Factor	2,4,6	Questions on form factor based on conserved resource	78.1

The usability as reported by SUS score did not reach the level of the 80th percentile, which is the score at which a subject would recommend the webapp to a friend (Sauro, 2011). SUS scores are frequently used to benchmark successive iterations of a design, as is appropriate for DSR.

4.3.2 Phase 3 – Summary of Results

Based on the data reported above, and the analysis of the hypotheses planned to be evaluated in Phase 3 had the results listed in Table 24.

Table 24. Hypotheses Results for Phase 3

Hypothesis	Measurement	Measuring success	Supported
H1- increase the success	Examine questions about success (#1,#2,#3,#5,#6,#7,#8, #9 on SUS)	Favorable rating received as answers on usability questions (Table 23)	Yes
H2 - improve the user experience	Examine all questions on SUS overall	Acceptable rating for SUS overall (Table 23)	Yes
H4 – reducing manipulation	Examine questions about manipulating the system (#2, #6, #8)	Positive rating received as answers on these questions (Table 23)	Yes
H5 – conserving user effort	Examine questions that address user cognitive effort (#4, #5, #7, #10)	Positive rating received as answers on these questions (Table 23)	Yes

4.4 Summary

The results of all three phases of the evaluation were reported. Each phase tested a portion of the hypotheses. The hypotheses tested in each phase and the results were summarized in a table at the end of each phase as shown in Table 10, Table 13, and Table

15. As mentioned in 3.3.3, the Cogtool score shows the new security usability principles improve the security interface on mobile, but not enough to be better than the desktop interface. As a result, hypothesis 6 is refuted for this artifact. A summary of all hypotheses and results appears in Table 25.

Table 25. Summary of All Hypotheses Results by Phase

Hypothesis	**Phase 1 Supported**	**Phase 2 Supported**	**Phase 3 Supported**
H0 - no impact	No	No	Not Evaluated
H1- increase the success	Yes	Yes	Yes
H2 - improve the user experience	Yes	Not Evaluated	Yes
H3 - conserving power	Yes	Yes	Not Evaluated
H4 - reducing manipulation	Yes	Yes	Yes
H5 - conserving user effort	Yes	Yes	Yes
H6- Mobile vs desktop	No	Not Evaluated	Not evaluated

Chapter 5

Conclusion

The following section is the final section containing a discussion of the findings and the importance. The research questions are re-visited in light of the results.

5.1 Conclusions

The first research question is: *How does the overlap or conflict between security and usability impact the design of effective usable security on mobile devices?*

By comparing the principles for usability and secure design in 3.1.1 it was shown that usability is a subset of good security. Applying usability principles to security design did not weaken the security. Any security that ignores usability principles is also ignoring principles for good security design. Working from a checklist, however, is an inaccurate means of applying design principles. Using a human performance modelling tool like Cogtool provides a communicable measure (seconds elapsed) of the usability of the design.

The Cogtool graphs provided the evidence of the high cognitive load of the touchscreen keyboard. Though the ineffectiveness of wholesale transport of workstation security design to the mobile platform has been called into question by previous research (Oberheide & Jahanian, 2010), the security model of basic authentication retains a significant foothold on mobile (Chiang & Chiasson, 2013). The lack of usability of basic authentication has generated considerable research on alternatives such as pass-faces (Dunphy, Nicholson, & Olivier, 2008), graphical passwords (Biddle et al., 2012; Bulling, Alt, & Schmidt, 2012; Chiang & Chiasson, 2013; Gao et al., 2012; Stobert & Biddle, 2013), pass-chords (Azenkot, Rector, Ladner, & Wobbrock, 2012; Leftheriotis, 2013), and gestures (Serrano et al., 2013; Singha, Misra, & Laskar, 2016), but basic authentication is still the most common security model.

The results show interaction with basic authentication on a mobile 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 (Withana, Peiris, Samarasekara, & Nanayakkara, 2015). Password meters have been successful in leading users towards stronger passwords (Carne, Carnavalet, & Mannan, 2015). 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. Similarly strong passwords and the current mobile device keyboard used in motion are usability-incompatible. Even with frequent usage, the sequence of characters inherent in a strong password cannot be input accurately with the mobile device in motion.

5.2 Implications

When creating design principles it is key to know what needs to be changed. In 3.1.3 conserving the resources of power, form factor, and user effort were identified as key to achieving usability of mobile security.

The second research question is: *Will a set of design principles structured to conserve constrained resource attain security usability?*

The Cogtool score in Phase 1 showed that the design that conserved the constrained resources would have higher usability (less seconds to navigate). The SUS score in Phase 3 showed user satisfaction was acceptable but not exceptional. The key to the lower user satisfaction is in the Phase 2 usage data. When doing keyboard-intensive tasks to add input to be retrieved during the execution on security tasks, the users shifted back to a desktop version of the interface.

Though the design does conserve all three constrained resources, the cognitive load is not sufficiently reduced to make the current design attractive to use outside the boundaries of the study. The cognitive load comes not only from recall, but from the manipulation of the touchscreen interface. Unlike a keyboard used with a workstation, the manipulation of a touchscreen does not benefit from muscle memory to speed the manipulation of the form factor and relieve the cognitive load of retrieving the password

(Lu, Yu, Yi, Shi, & Zhao, 2017). The cognitive interaction required by using the eyes to guide the user's fingers across the keyboard takes the same amount of time for the novice user and the expert user. Reducing and/or touchscreen keyboard interaction conserves both user cognitive effort and form factor manipulation effort.

The lack of popularity of the medium mode was obvious in the usage data (Figure 29). Comments on post-study survey indicated the users felt the cognitive load of deciding which security mode to use was high. They wanted a location to be safe, and their interactions with security supported by CLUE, or not safe, which is the current norm.

Even with the resource conservation, the Cogtool model of the best design interface on mobile still had a higher time score than the worse design interface on desktop. This demonstrated by the refutation of H6. Additional design changes to conserve more constrained resources are needed to make the usability of mobile basic authentication equal or better than the desktop equivalent.

5.3 Discussion

Creating a new type of security interface runs into obstacles in several areas. Security research has a history of poor participation (Kotulic & Clark, 2004). Companies who have had security breaches don't want to reveal the details because those details can reveal additional vulnerabilities. When designing security research studies the investigator must carefully structure the study to protect not only the typical Personally Identifiable Information (PII) but also security-related information. Strict interpretation of Institutional Review Board (IRB) policies written to protect human subjects from harm can also hamper security research (Garfinkel, 2008). In spite of this, security research related to psychology, sociology (Siponen, 2005), human interaction and human error (Sasse, Brostoff, & Weirich, 2001) are critical to solving security issues.

Participation in a security study for individuals is also seen as a risk. In this study approximately 118 subjects were willing to fill out a survey about security attitudes and usage, only 44 proceeded to the actual usage of the artifact. The initial recruitment reached out to 8000 possible subjects. Though no actual passwords were requested in the study, the potential participants were cautious about revealing their security behaviors. The subjects were a convenience sample, but recruited from groups where the investigator had a trusted relationship. Without some trust in the investigator, participation in security research is seen as a risk. While researchers understand the oversight provided by IRB approval (Appendix K – IRB Memo), other desirable research subjects need some sort of certification or seal of approval that identifies research that will properly protect information about their security behaviors that makes them vulnerable to social engineering.

New security paradigms are also seen as dangerous because the potential subjects typically do not understand "the new way" of handling security. In many cases the subjects do not understand all the risks of the "old way" either, but repeated usages has overcome their reluctance When it comes to security, erring on the side of the known or conservative approach makes the subject more comfortable because the potential risks of revealing personal information are so high. Once again, unless the security researcher or their organization is trusted, the subjects are reluctant to participate.

This discomfort and distrust point to the need to develop and expand the use of human performance modelling tools to predict the usability of the interface. Cogtool did correctly predict both the increased usability of the mobile security interface once the design principles were applied. Cogtool also correctly documented even the improved security interface on mobile was not as easy to use as the worst desktop. The human performance modelling can provide a measure without revealing the personal security traits/attitudes/behaviors of individual subjects.

5.3.1 Gaps in the Literature

As discussed in 2.4, current research does not provide design direction security-usability for mobile separate from desktop. The results of this research show that the design principles proposed did improve the usability of the security interface on mobile. The high success rate of users in navigating the revised interface, and the positive SUS rating demonstrates this.

Prior research does not examine the true cost of the keystroke equivalent on the mobile platform. Though the accuracy of Cogtool as a predictor of difficulty was documented on both desktop and mobile, a comparison of the difficulty of repeatedly using the same security interface on both platforms has not been done. The results show that input of security information using a keystroke equivalent is almost three times more difficult than on the desktop. Breaking down the Cogtool measure into the constrained resources used on the mobile keyboard equivalent revealed the hidden cognitive load on each stroke that was not decreased by repetition, and not caused by lack of recall. The nature of touchscreen interaction with no haptic cues like a physical keyboard, and no development of body memory makes each and every keystroke sequence as difficult as the one previous.

Previous research has focused on the use of SUS data to determine user perception of usability. The generalized nature of the SUS questions does not provide specific guidance for what to change in a system like the Cogtool mapping to the design. Phase 1 and 2 provided clearer insight into what to consider for future directions than the Phase 3 data. Having a metric to aim for (the Cogtool score for basic authentication on desktop) a method to measure (Cogtool), and specific actions to control/reduce (the actions that used the resources of power, form factor, user effort) is more attainable by the security designer than the checklist of principles. Meeting a metric makes communicating the usability more concrete than an adjective like "good."

This research looks specifically at security input rather keyboard input in general on the mobile platform. Security input for basic authentication differs from input for a text message because of the rules for strong passwords (Horcher & Tejay, 2009). To prevent a dictionary attack to guess a password, users are encouraged to choose character sequences that are not typically typed (Topkara, Atallah, & Topkara, 2007). Passwords that are easily typed by going across a row in in a keyboard (QWERTY) are also discouraged (Furnell, 2011). Research to improve typing usability on the mobile device keyboard has focused on predictive text to reduce interaction time (Sandnes, 2015; Trinh, Waller, Vertanen, Kristensson, & Hanson, 2014). 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 (Orphanides & Nam, 2017).

5.4 Recommendations

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 (Herley, 2009b). In the absence of an independent measure of the effort, it is still possible that many users 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 (Harbach, Von Zezschwitz, Fichtner, De Luca, & Smith, 2014).

When listening to music or talking, individuals are more likely to look at their device (Schwebel et al., 2012). The danger of cognitive distraction from mobile phone use reduces situation awareness and increases unsafe behavior (Nasar, Hecht, & Wener, 2008). 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 (Laatar, Kachouri, Borji, Rebai, & Sahli, 2017).

The dropped head posture adopted by the user to see the screen affects not only visibility of surroundings but also balance and gait (Kao, Higginson, Seymour, Kamerdze, & Higginson, 2015). 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 (United States Figure Skating Association, 1998), 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 is in motion even as a pedestrian decreases usability and safety.

Distractions caused by mobile phone use while driving have clearly shown the connection between texting and traffic accidents (Lipovac, Đerić, Tešić, Andrić, & Marić, 2017). In the United States, hands-on use of a mobile phone has been regulated in 14 states and has resulted in a reduction of traffic accidents particularly for less-experienced drivers (Zhu, Rudisill, Heeringa, Swedler, & Redelmeier, 2016). There is conflicting evidence on the impact of conversation as a distraction. Drivers taking calls related to work experienced a higher level of distraction (Engelberg, Hill, Rybar, & Styer, 2015), but those who were conversing had decreased levels of driver fatigue in a monotonous driving situation (Saxby, Matthews, & Neubauer, 2017).

The damage done while driving is exacerbated by the distances travelled during the distraction, roughly 100 yards at 55 mph in 4 seconds (Muttart, Fisher, Knodler, & Pollatsek, 2007). A typical pedestrian walks at 3 feet per second (Kao et al., 2015) 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 (Mwakalonge, Siuhi, & White, 2015).

More complex typing tasks and greater memory recall tasks induce dual-task interference while walking (Lim, Amado, Sheehan, & Van Emmerik, 2015). 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 (Sandnes, 2015; Trinh, Waller, Vertanen, Kristensson, & Hanson, 2014). 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 (Orphanides & Nam, 2017).

The lack of usability for security inputs on a touchscreen also points to a need for a better design of the touchscreen keyboard construct. Previous work in this area has focused on auto-correction and predicting input (Al-Khalifa et al. 2014). A security-input optimized keyboard may alleviate the issues that hamper the usability of touchscreen input, just as text-optimized keyboards improve text input usability (Bi et al. 2010). 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, URLs and other data (Hong et al. 2015). A similar technique could be used.

Voice and haptic interfaces have improved to become a viable “eyes-off” option (Arif, Pahud, Hinckley, & Buxton, 2013). 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 (Harris, 2005). 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.

Using GPS location to set the security level of the webapp was appreciated by the users. No keyboard input was necessary, other than to name the location. To get access to the most usable security mode, some users would set their current location as “safe”, and then delete the location after retrieving the desired security hints/clues. This indicates a need for a time duration of security access. Currently the norm for granting security access defaults to permanent access. Designing an auto-expiration of 30 minutes as the default, with the option to select permanent access, would protect the user whose location may be safe at the time, but not perhaps later. Similarly the user might choose to designate a medical facility as safe for a time while assistance is being rendered, and then have access auto-expire.

Several users suggested the use of pictures to remind themselves of passwords instead of text strings as their input to the webapp. Others used speech to text capabilities as an alternative to the mobile keyboard. For exceeding small screens, such as the smartwatch, one-handed security entry with eyes off is highly desirable. Instead of trying to type, a series of timed taps could form a pattern for unlocking. Similar to the passphrase, the user thinks of a rhythmic pattern or song to trigger recall of the authentication sequence.

As options to the touchscreen keyboard for authentication, drawing a pattern and fingerprint reading have become popular. Each of these options can be executed "eyes-off" and in less than four seconds, making them safer for mobile authentication in motion.

5.5 Summary

In this chapter the results communicated in Chapter 4 were mapped to the research questions. In response to research question 1, usability was shown to be a subset of security. Good choices in security design lead to good choices for usability and vice versa. In response to research question 2, the results showed that conserving the constrained resources identified on mobile (power, form factor, and user effort/cognitive load) did improve the usability of the security interface and the success rate of navigating security. However, the comparison to the desktop platform, the improvement still did not match the usability level of the desktop equivalent. The gaps in the literature identified in the Chapter 2 literature were also mapped to the results. In particular the cost of the keystroke and the difference between security and normal input have not been examined. Finally the future directions for research in this area are discussed based on the results of the research.

Appendix A - Use Cases Descriptions and Diagrams

The following four security-related tasks describe typical use of basic authentication.

Task 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 when the user knows both the UID and the password.

Task 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 (Herley, 2009), 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.

Task 3: Password Reset

The password reset task 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 must copy the temporary password and provide a new strong password. The user is also prompted to create a password hint to allow potential recovery of the password in locations which are low risk.

Task 4: Password Recovery (Get hint)

The password recovery task is only available at a low risk location. It provides an avenue to successful authentication other than the password reset process. The user sees the recall cue only if one was set when prompted during password change. The diagrams below shows the paths taken through the interface based on location mode. The four security tasks modelled in the CogTool appear along the path to authentication.

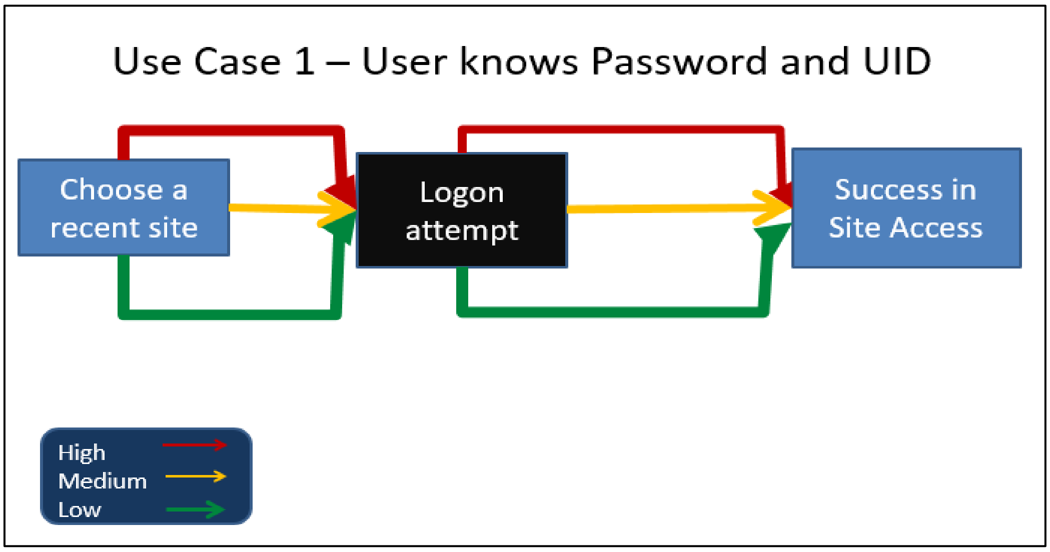


Figure A 1. Use case 1 – User Knows Password and UID

In the first case the user knows the both the UID and the password (

Figure A 1. Use case 1 – User Knows Password and UID). This is the simplest path. The user successfully recalls the password and UID from memory, and also successfully manipulates the form factors of the equipment.

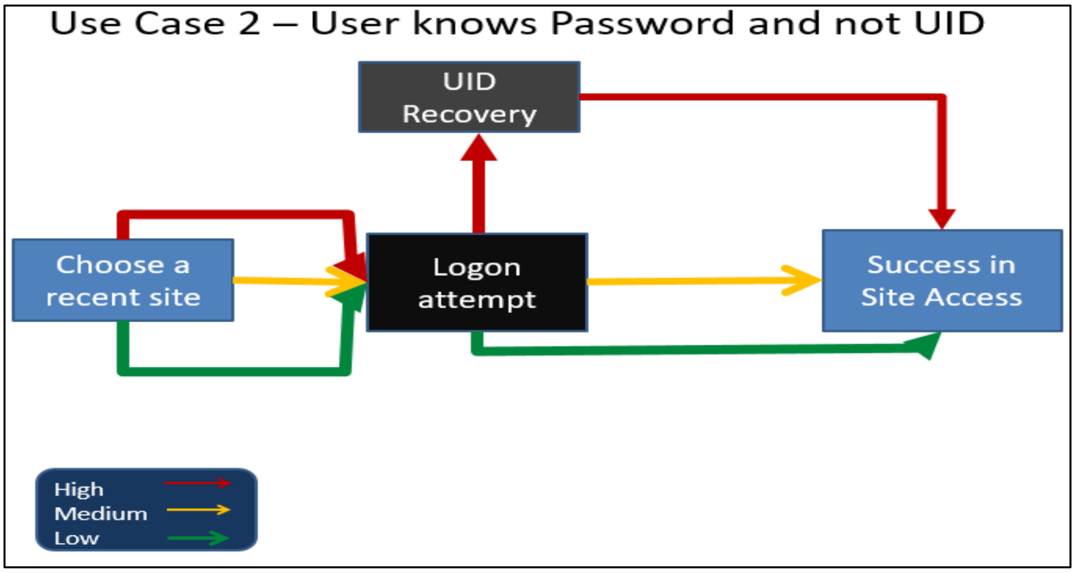


Figure A 2. Use case 2 – User knows password and not UID

In use case 2 the user knows the password and not the UID. For the security designs represented as Medium and Low risk there is no need of UID recovery because the UID is supplied to the user.

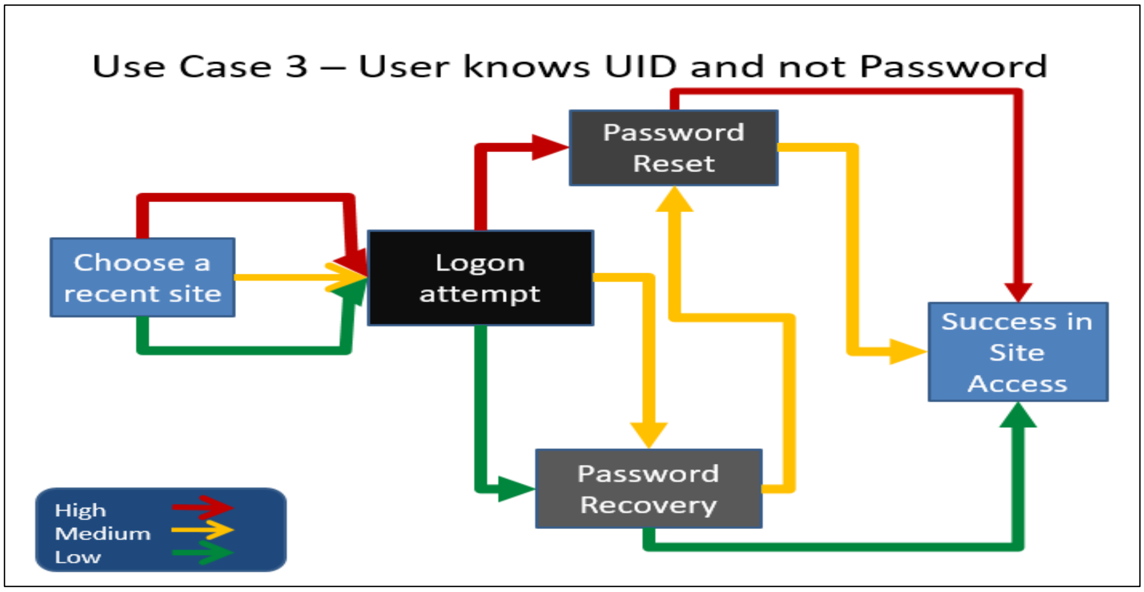


Figure A 3. Use Case 3 – User knows UID and not password

In use case 3 the user knows the UID and not the password (Figure A 3. Use Case 3 – User knows UID and not password). For the security designs represented as Medium and High there is no option of password recovery because a password hint is only available in Low risk mode. In Medium mode the password recovery is presented but the user will not receive a password clue because of the risk level. Medium and High designs must go through the password reset to achieve success, which requires much more manipulation of the security interface than the password recovery. The Low risk mode displays a password clue which allows the user to retrieve the password from memory using cued recall instead of the free recall that is the only option available in Medium and High risk designs.

In use case 4 the user doesn’t know the UID or the password (Figure A 4). In the security interface design for High risk, the user must recover the UID and reset the password to achieve successful authentication. In the security interface design for Medium risk the UID is supplied so only the password reset task is needed to achieve successful authentication. Finally the security interface design for Low risk mode only uses the password recovery task, similar to use case 3.

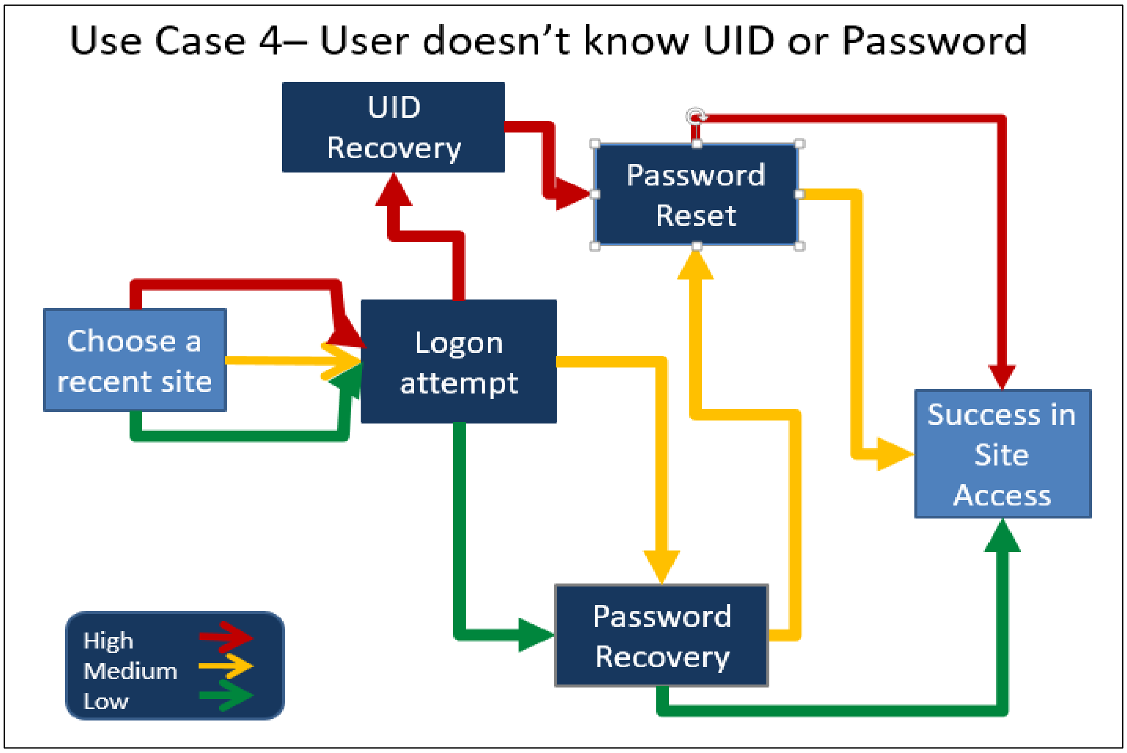


Figure A 4. Use Case 4 - User does not know UID or Password

Each security task receives a CogTool score indicating its difficulty in seconds elapsed. The score for each security mode will be based on adding up the score of the security tasks that make up the path from choice of site to success in site access.

Appendix B - CogTool Wireframes

CogTool is an open source, general purpose user interface prototyping tool developed at Carnegie-Mellon University. It uses a human performance model to automatically evaluate how efficiently a skilled user can complete a task. In this study it is used to measure the efficiency of three versions of basic authentication on both desktop and mobile devices.

To use Cogtool a designer creates a storyboard of a design. In this study images of the actual screens were used to produce the story board. The tasks included in navigating the security interface were demonstrated by interacting with the storyboard like the software. As a result CogTool creates a baseline of the current version of basic authentication on mobile and desktop, and measures the improvements made by conserving constrained resources on mobile.

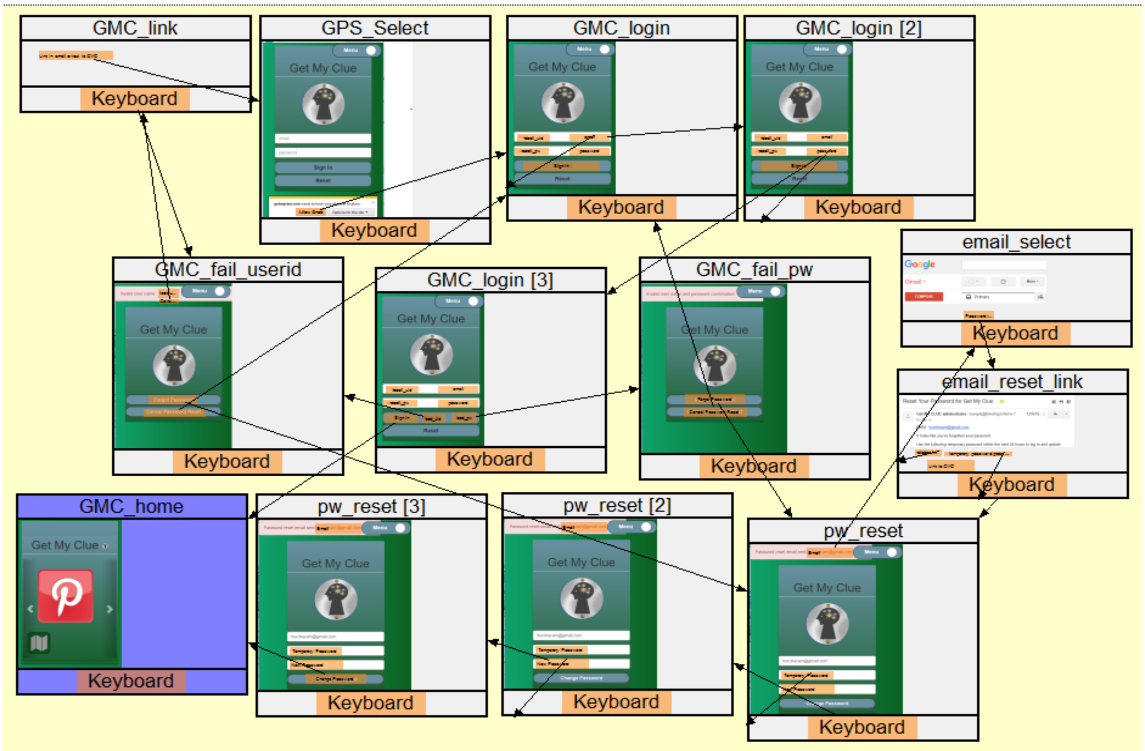


Figure B 1. High Risk Desktop Design in CogTool

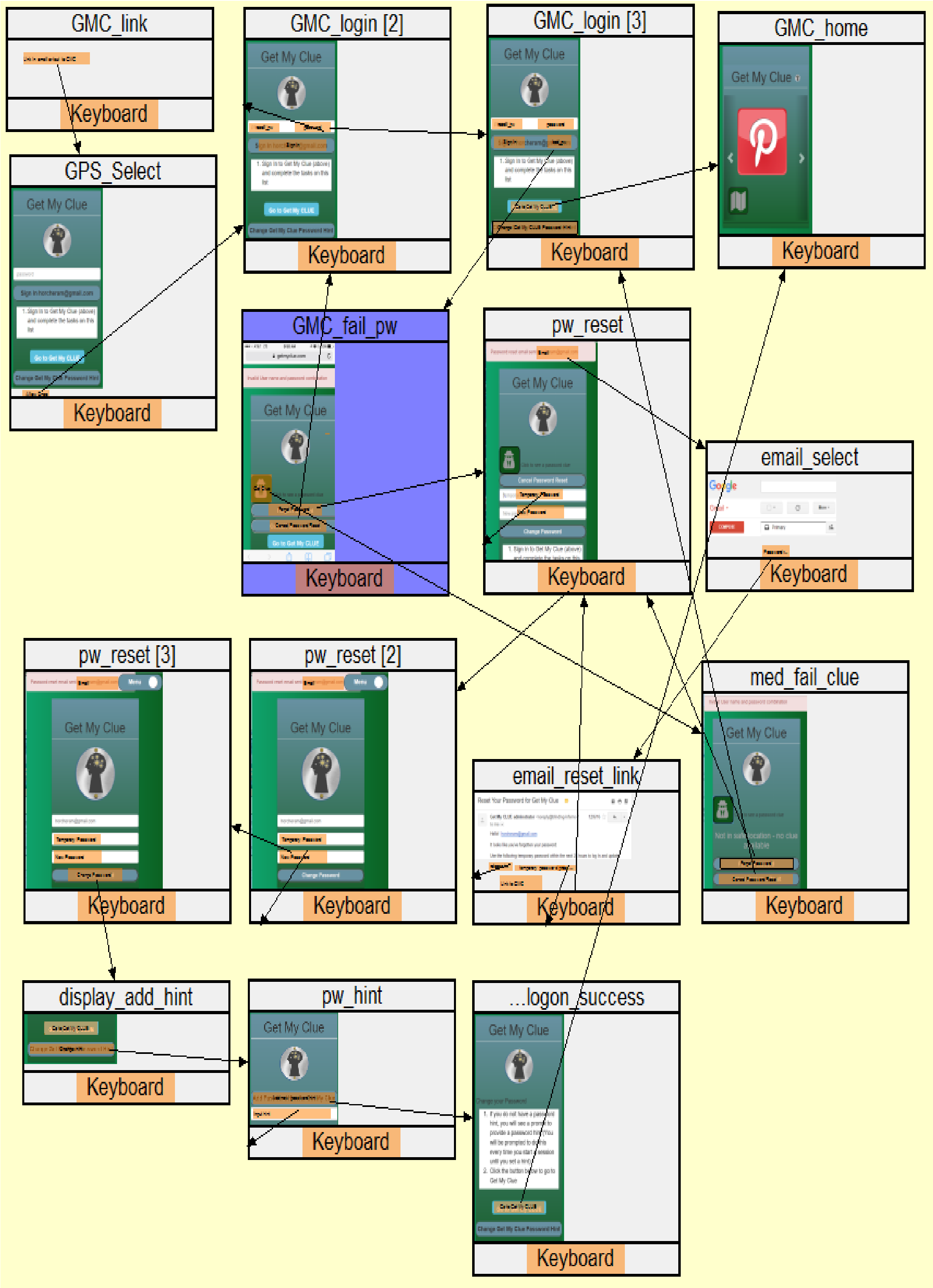


Figure B 2. Medium Risk Desktop Design in CogTool

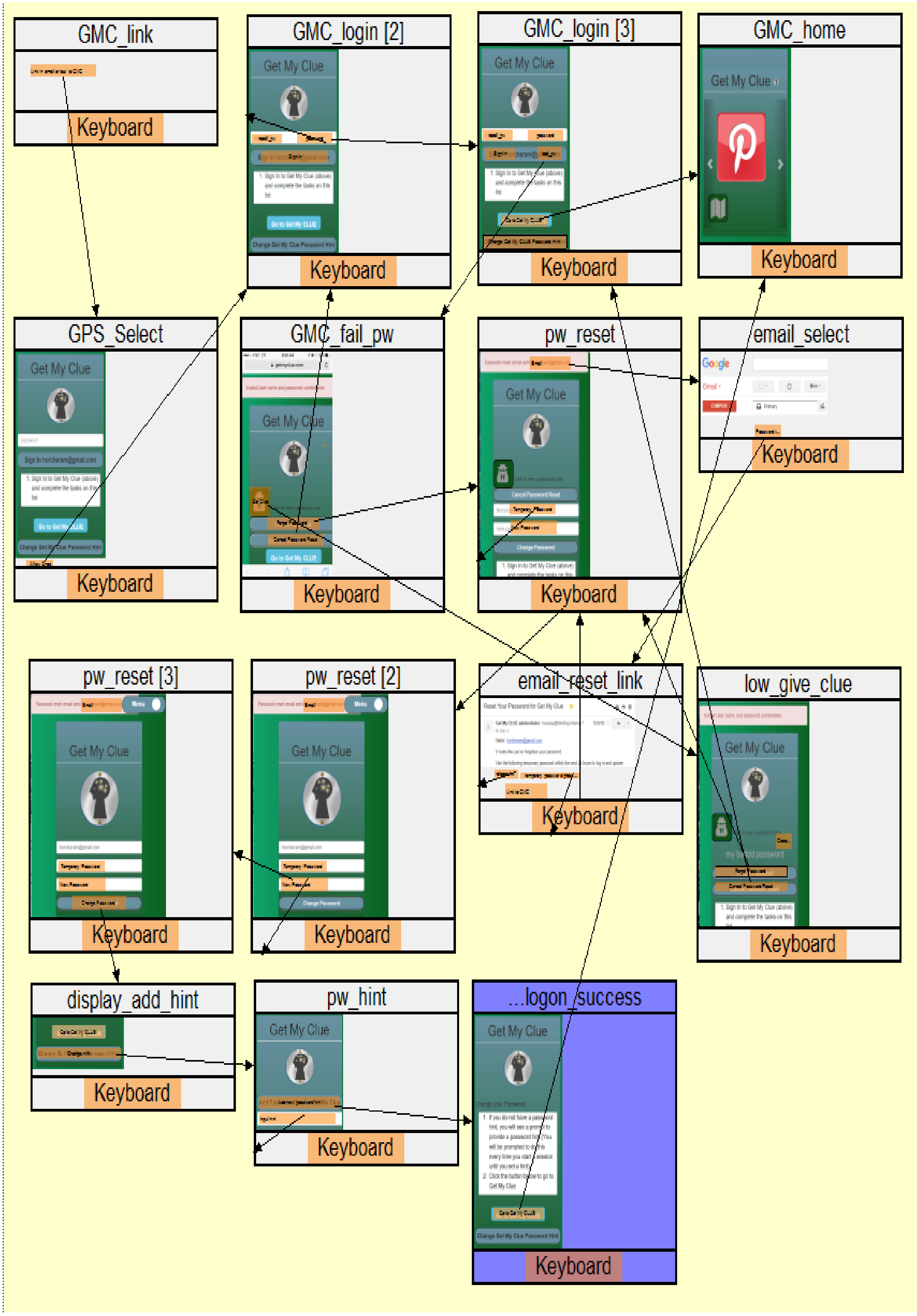


Figure B 3. Low Risk Desktop Design in CogTool

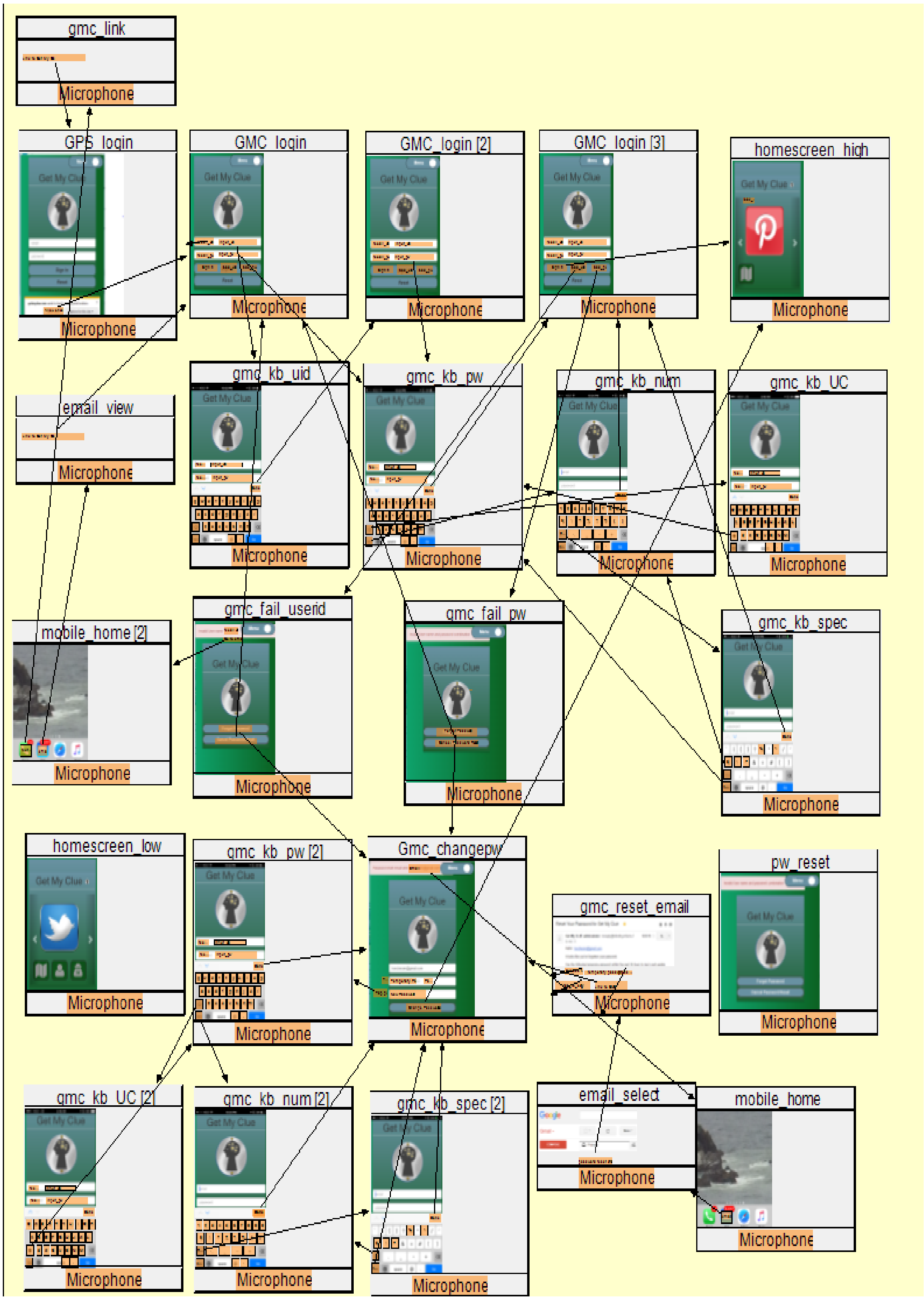


Figure B 4. High Risk Mobile Design

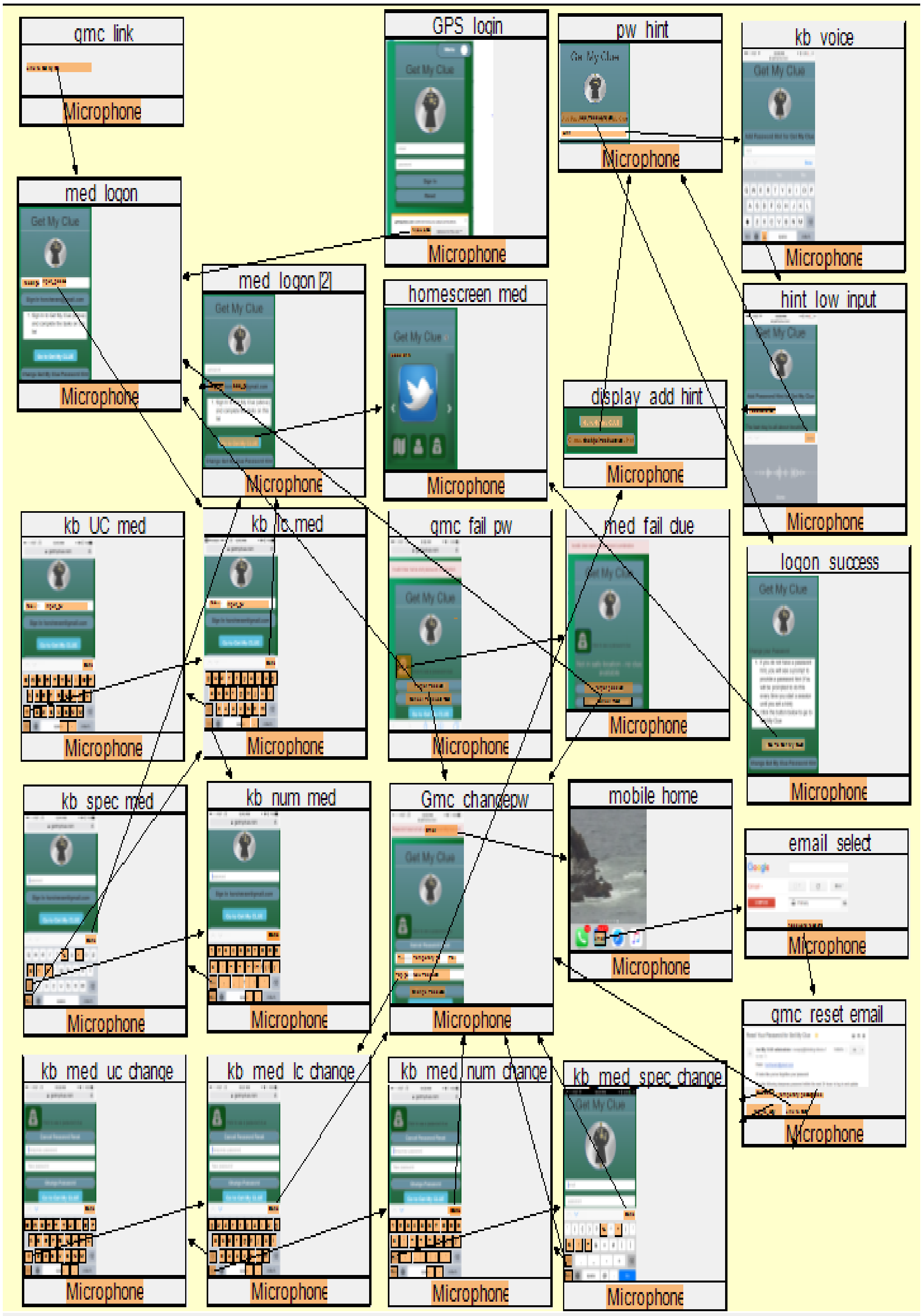


Figure B 5. Medium Risk Mobile Design

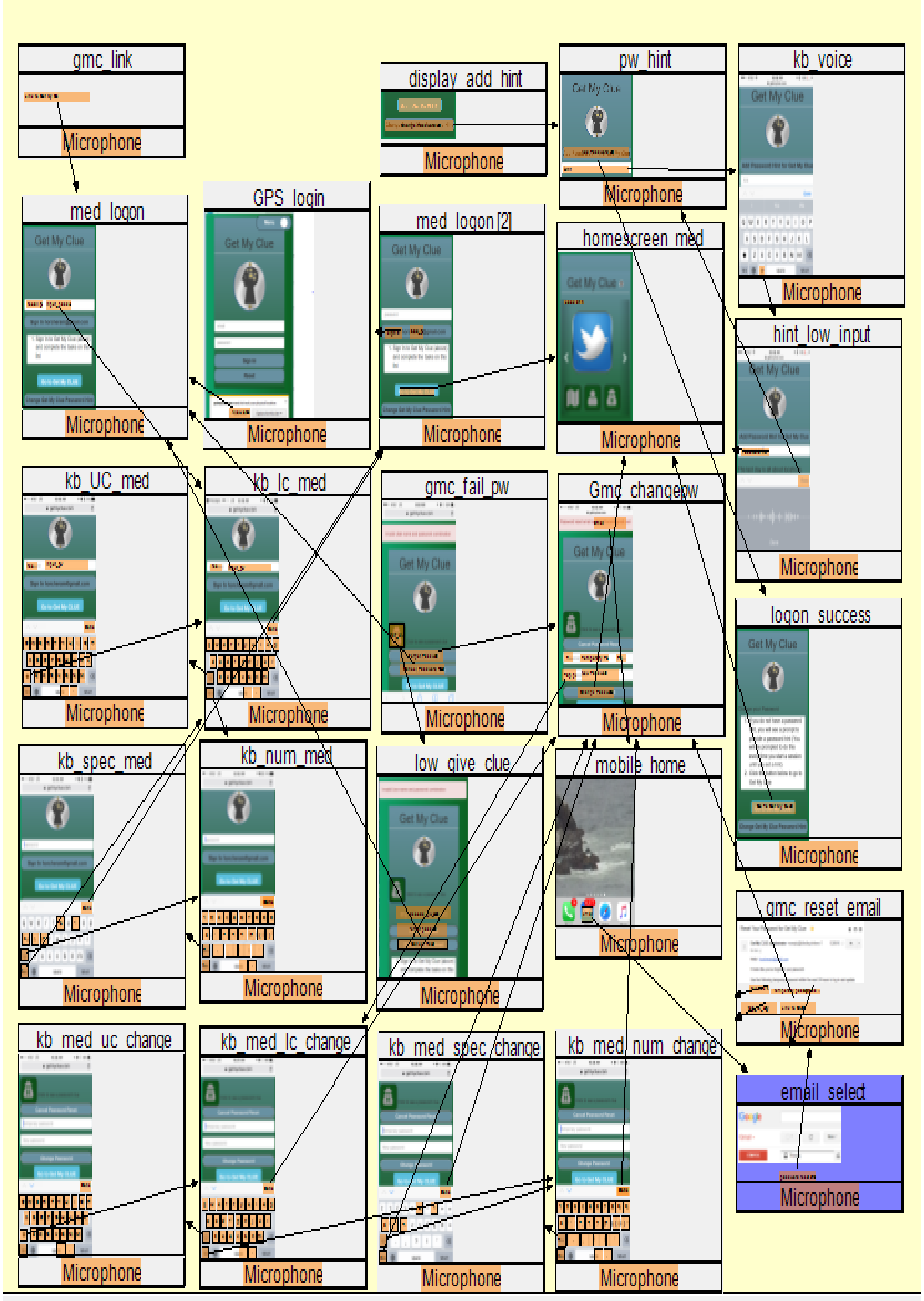


Figure B 6. Low Risk Mobile Design

Appendix C – Task List for Study Participants

The study participants received links to a web page with instructions to perform a task. There was a signup task, nine tasks interacting with the Get My CLUE app, and one task filling out the post-study survey. The links were delivered via email and text message.

Group 1 – Add a Website

1. Sign In to Get My Clue (above) and complete the tasks on this list
2. Click the button below to go to Get My Clue
3. Click on Menu --> Websites
4. Click on
5. Choose Select Website from the list
6. Choose a website off the list
7. Hit submit to see it on your list of websites

Group 2 - Add userid and Passwords to a Website

1. Sign In to Get My Clue (above) and complete the tasks on this list
2. Click the button below to go to Get My Clue
3. Click on Menu --> Websites
4. Click on any website from the list
5. Add a userid clue and a password clue if prompted. Then click on the website again

Group 3 – The home screen carousel

1. Sign In to Get My Clue (above) and complete the tasks on this list
2. Click the button below to go to Get My Clue
3. Click on large icon of any web site in the carousel

4. Click on to see a userid hint
5. Click on to see a userid hint
6. Click on to see a password hint
7. Click Menu --> Sign out.
8. Click the button Confirm Sign out.

Group 4 - Change your Password

1. Type the wrong password above and click on Sign In (above)
2. Click on to see a password hint
3. Click on Forgot Password
4. Check your email for the temporary password and copy it into the screen
5. Put in a new password and hit Change Password
6. if you do not have a password hint, you will see a prompt to provide a password hint (You will be prompted to do this every time you start a session until you set a hint)
7. Click the button below to go to Get My Clue

Group 5 – Set a new Password Hint

1. Sign In to Get My Clue (above) and complete the tasks on this list
2. Since you changed your password you might need a new hint. Click below to Change Get My CLUE Password Hint
3. Put in a new password hint for Get My CLUE
4. Click Add Get My CLUE Password Hint to update your password clue.
5. Click the button below to go to Get My Clue

Group 6 – Add categories to determine risk for websites

1. Sign In to Get My Clue (above) and complete the tasks on this list

2. Click the button below to go to Get My Clue
3. Click on Menu --> Websites
4. Click on Search
5. Type part of a category name or website name. The website list will show only the sites that meet your search.

Group 7 – Add password hint

1. Sign In to Get My Clue (above) and complete the tasks on this list
2. Click below to Change Get My CLUE Password Hint
3. Put in a new password hint for Get My CLUE
4. Click Add Get My CLUE Password Hint to update your password clue.
5. Click the button below to go to Get My Clue

Group 8 - Add locations and use web app in different locations

1. Sign In to Get My Clue (above) and complete the tasks on this list
2. Click the button below to go to Get My Clue
3. Click on Menu --> Locations
4. Click to add a new location
5. Choose a risk level for your current location
6. Type a short name for your location
7. Type a description for your location
8. Click Submit new to add your current location. If you are at a location already in your locations, you will see an error message
9. Click on Menu --> Websites
10. Choose any website and click on it

Group 9a – Use the web application in a new location. User must be in a new location

1. Sign In to Get My Clue (above) and complete the tasks on this list
2. Make sure you are in a location different from the previous task
3. Click the button below to go to Get My Clue
4. Click on Menu --> Locations
5. Click to add a new location
6. Add your current location as medium risk
7. Remember to Submit New for the new location
8. Refresh your screen
9. Click on Menu -- > Websites Notice that the password clue does not appear
10. Choose any website and click on it

Group 9b – Repeat previous task group in a new location

1. Sign In to Get My Clue (above) and complete the tasks on this list
2. Make sure you are in a location different from the previous task
3. Click the button below to go to Get My Clue
4. Click on Menu --> Locations
5. Click to add a new location
6. Add your current location as medium risk
7. Remember to Submit New for new location
8. Refresh your screen
9. Click on Menu -- > Websites Notice that the password clue does not appear
10. Choose any website and click on it

Appendix D – Experimental Procedure Checklist

1. Have potential subjects fill out the pre-study survey from Appendix E. The informed consent form is included in the survey. Subjects who do not give consent are removed from the study at this point and their data discarded.
2. Extract data from pre-study survey on websites commonly used by the subject and pre-load information into the CLUE web application to decrease the configuration needed by the subject before achieving any meaningful usage.
3. Add subject email provided after consent to the data table listing emails allowed to use the web application.
4. Send email and text message to the potential subject with a link to create an account in the Get My CLUE app.
5. After confirming the subject signed up by checking the list of users in Firebase authentication, add the subject to the list of subjects being directed through the tasks of the study.
6. Send a text and email daily to direct the subject to perform the nine groups of tasks listed in Appendix C. Group 9 involved 2 emails and task messages to direct the subject through tasks at different points in the day.
7. Send the subject a link in email and text to complete the final survey.
8. Send the subject a link in email and text to request a gift card.

Appendix E – Pre-Study Questionnaire

Answer all the questions in the survey.

At the end of the survey there is an opportunity to share additional comments.

1. `D1 Please choose your age range ***This question is required.**

18-27 years old28-37 years old38-47 years old48-57 years old58-67 years oldOver 68 years oldunder 18

○ ○ ○ ○ ○ ○ ○

2. `D2 Please choose your gender ***This question is required.**

- ○ Male
- ○ Female
- ○ Prefer not to answer

3. `D3 Please choose your level of technology expertise ***This question is required.**

PoorFairGoodVery GoodExcellent

○ ○ ○ ○ ○

4. `D4 Please choose your level of education ***This question is required.**

Some high school	High school diploma	Some college	College diploma	Some graduate work	Masters Degree	Some doctoral work	PhD / JD / MD
○	○	○	○	○	○	○	○

5. `D5 How often do you use a smart phone and/or tablet? ***This question is required.**

NeverOccasionallySeveral times a weekDailyMultiple times a day

○ ○ ○ ○ ○

6. `s1 Do you find security a barrier to using apps and websites on a smartphone or tablet? ***This question is required.**

Not a barrierSomewhat of a barrierModerate barrierExtreme barrier

Not a barrierSomewhat of a barrierModerate barrierExtreme barrier

○ ○ ○ ○

7. `s2 How often do you forget your passwords? ***This question is required.**

NeverRarelyOccasionallyFrequentlyDaily

○ ○ ○ ○ ○

8. `s3 How often do you disable security on your smartphone to make it more convenient to use or lend? ***This question is required.**

NeverRarelyOccasionallyFrequentlyDaily

○ ○ ○ ○ ○

9. `s4 The risk of my smartphone/tablet being compromised when I use it in my home is . . . ? ***This question is required.**

LowMediumHigh

○ ○ ○

10. `s5 The risk of my smartphone/tablet being compromised when I use it at work is . . . ? ***This question is required.**

LowMediumHigh

○ ○ ○

11. `s6 The risk of my smartphone/tablet being compromised when I use it in public spaces is . . . ? ***This question is required.**

LowMediumHigh

○ ○ ○

12. `s7 The risk of my smartphone/tablet being compromised when I am in an emergency situation is . . . ? ***This question is required.**

LowMediumHigh

○ ○ ○

13. `s8 How important is it for medical personnel to access medical information on my smartphone/tablet in an emergency? ***This question is required.**
Low importanceMedium importanceHigh important

○ ○ ○

14. `c1 Which of these social network sites do you use? (Mark all that apply) ***This question is required.**

- □Facebook
- □Google +
- □Linked-in
- □Twitter
- □None
- □Other - Write In (Required) Please enter an 'other' value for this selection.□ *** This question is required.**

15. `r1 The information stored on a social network site is . . . ? ***This question is required.**
Low riskMedium riskHigh risk

○ ○ ○

16. `c2 Which of these entertainment sites do you use? (Mark all that apply) ***This question is required.**

- □Youtube
- □Netflix
- □Hulu Plus
- □Amazon Prime
- □None
- □Other - Write In (Required) Please enter an 'other' value for this selection.□ *** This question is required.**

17. `r2 The information on an entertainment site is . . . ? ***This question is required.**
Low riskMedium riskHigh risk

○ ○ ○

18. `c3 Which of these shopping sites do you use? (Mark all that apply) ***This question is required.**

- □Amazon

- □eBay
- □Barnes and Noble
- □None
- □Other - Write In (Required) Please enter an 'other' value for this selection. *This question is required.

19.`r3The information on an shopping site is . . . ? *This question is required.

Low risk Medium risk High risk

○ ○ ○

20.`c4 Which of these social media/blogging sites do you use? (Mark all that apply) *This question is required.

- □Twitter
- □Medium
- □Pinterest
- □Instagram
- □Snapchat
- □None
- □Other - Write In (Required) Please enter an 'other' value for this selection. *This quetion is required.

21.`r4The information on an blogging site I read is . . . ? *This question is required.

Low risk Medium risk High risk

○ ○ ○

22.`c5 Which of these personal and family medical information sites do you use? (Mark all that apply) *This question is reuired.

- □About One
- □WebMD Health Manager
- □Health Vault
- □Blue Cross Blue Shield
- □Medicare
- □None

- □ Other - Write In (Required) Please enter an 'other' value for this selection. ________ * **This question is required.**

23. `r5 The information on a personal and family medical information site is . . . ? ***This question is required.***
Low riskMedium riskHigh risk

○ ○ ○

24. `c6 Which of these travel and navigation sites do you use? (Mark all that apply) ***This question is required.***

- □ Google Maps
- □ Map Quest
- □ Trip Advisor
- □ Airline sites
- □ Expedia
- □ None
- □ Other - Write In (Required) Please enter an 'other' value for this selection. ________ * **This question is required.**

25. `r6 The information stored on a travel and navigation site is . . . ? ***This question is required.***
Low riskMedium riskHigh risk

○ ○ ○

26. `c7 Which of these news sites do you use? (Mark all that apply) ***This question is required.***

- □ CNN
- □ ABC
- □ Fox
- □ MSN
- □ None
- □ Other - Write In (Required) Please enter an 'other' value for this selection. ________ * **This question is required.**

27. `r7 The information stored on a news site is . . . ? ***This question is required.***
Low riskMedium riskHigh risk

○ ○ ○

28. `c8 Which of these bank and financial services do you use? (Mark all that apply) *This question is required.

- □ Chemical Bank
- □ Isabella Bank
- □ Chase
- □ American Express
- □ TIAA CREF
- □ None
- □ Other - Write In (Required) Please enter an 'other' value for this selection. □ * This question is required.

29. `r8 The information stored on a bank or financial site is . . . ? *This question is required.

Low risk Medium risk High risk

○ ○ ○

30. `c9 Which of these mail services do you use? (Mark all that apply) *This question is required.

- □ Gmail
- □ AOL
- □ Yahoo
- □ Juno
- □ Microsoft Live
- □ None
- □ Other - Write In (Required) Please enter an 'other' value for this selection. □ * This question is required.

31. `r9 The information stored on a mail site is . . . ? *This question is required.

Low risk Medium risk High risk

○ ○ ○

32. `c20 What other sites do you use?

33. By submitting this survey you give consent to participate in the study.

- ○ Yes
- ○ No

34. Please provide your email address to receive an invitation to install Get My Clue. ***This question is required.**

35. Provide the phone number of a cell phone from which you will use the app.

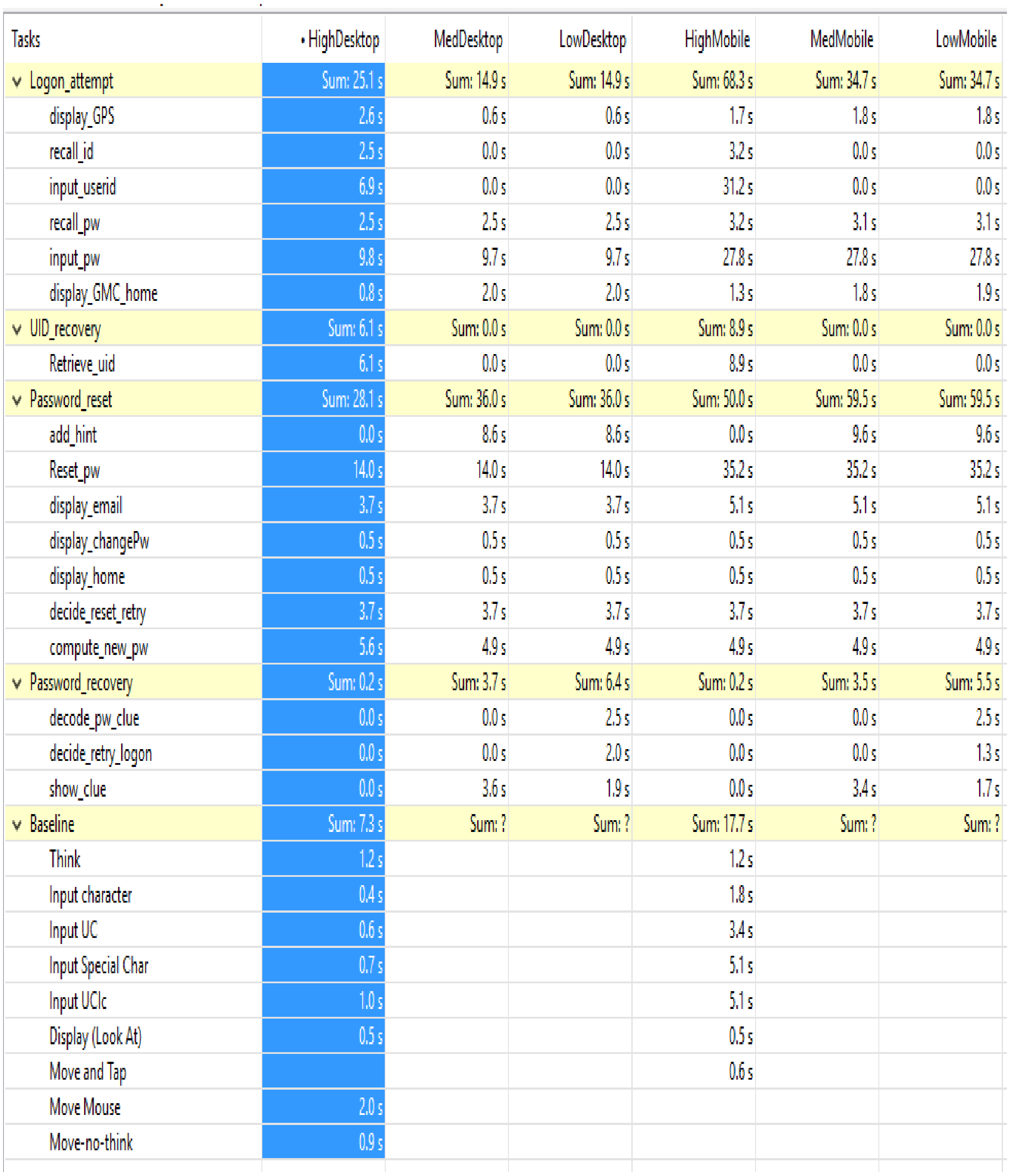
36. Please add any comments or questions.

Thank you for taking the survey. Please contact getmyclue@gmail.com for more information about the study.

You will receive your invitation to access the app in your email provided in the survey and texted to the mobile number you provided.
The responses provided will be used to configure your use of Get My Clue, the easiest way to remember your passwords

Appendix F - CogTool Mapping Data

CogTool measures for the security interface designs created using the design principles that conserve the constrained resources appear below.



Tasks	• HighDesktop	MedDesktop	LowDesktop	HighMobile	MedMobile	LowMobile
Logon_attempt	Sum: 25.1 s	Sum: 14.9 s	Sum: 14.9 s	Sum: 68.3 s	Sum: 34.7 s	Sum: 34.7 s
display_GPS	2.6 s	0.6 s	0.6 s	1.7 s	1.8 s	1.8 s
recall_id	2.5 s	0.0 s	0.0 s	3.2 s	0.0 s	0.0 s
input_userid	6.9 s	0.0 s	0.0 s	31.2 s	0.0 s	0.0 s
recall_pw	2.5 s	2.5 s	2.5 s	3.2 s	3.1 s	3.1 s
input_pw	9.8 s	9.7 s	9.7 s	27.8 s	27.8 s	27.8 s
display_GMC_home	0.8 s	2.0 s	2.0 s	1.3 s	1.8 s	1.9 s
UID_recovery	Sum: 6.1 s	Sum: 0.0 s	Sum: 0.0 s	Sum: 8.9 s	Sum: 0.0 s	Sum: 0.0 s
Retrieve_uid	6.1 s	0.0 s	0.0 s	8.9 s	0.0 s	0.0 s
Password_reset	Sum: 28.1 s	Sum: 36.0 s	Sum: 36.0 s	Sum: 50.0 s	Sum: 59.5 s	Sum: 59.5 s
add_hint	0.0 s	8.6 s	8.6 s	0.0 s	9.6 s	9.6 s
Reset_pw	14.0 s	14.0 s	14.0 s	35.2 s	35.2 s	35.2 s
display_email	3.7 s	3.7 s	3.7 s	5.1 s	5.1 s	5.1 s
display_changePw	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s
display_home	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s	0.5 s
decide_reset_retry	3.7 s	3.7 s	3.7 s	3.7 s	3.7 s	3.7 s
compute_new_pw	5.6 s	4.9 s	4.9 s	4.9 s	4.9 s	4.9 s
Password_recovery	Sum: 0.2 s	Sum: 3.7 s	Sum: 6.4 s	Sum: 0.2 s	Sum: 3.5 s	Sum: 5.5 s
decode_pw_clue	0.0 s	0.0 s	2.5 s	0.0 s	0.0 s	2.5 s
decide_retry_logon	0.0 s	0.0 s	2.0 s	0.0 s	0.0 s	1.3 s
show_clue	0.0 s	3.6 s	1.9 s	0.0 s	3.4 s	1.7 s
Baseline	Sum: 7.3 s	Sum: ?	Sum: ?	Sum: 17.7 s	Sum: ?	Sum: ?
Think	1.2 s			1.2 s		
Input character	0.4 s			1.8 s		
Input UC	0.6 s			3.4 s		
Input Special Char	0.7 s			5.1 s		
Input UClc	1.0 s			5.1 s		
Display (Look At)	0.5 s			0.5 s		
Move and Tap				0.6 s		
Move Mouse	2.0 s					
Move-no-think	0.9 s					

Figure F 1. CogTool Measures for Get My CLUE, high Desktop is current norm

Appendix G – Data Definitions of Firebase Usage Data

The data for Phase 2 was collected using a webapp written in AngularJS framework. The data was store in the NoSQL database Firebase provided by Google. The data was extracted from Firebase in CSV files and loaded to Excel and SPSS for analysis.

Common Fields

Field name	Type	Description
transID	String	Firebase generated unique transaction identifier
firebaseUID	String	Unique identifier for Firebase user created when user registers
startedAt	Timestamp	Time in milliseconds from January 1, 1960. Recorded when action starts
Email	Email	Email address of the user (used before FirebaseUID is generated)
endedAt	Timestamp	Time in milliseconds from January 1, 1960.
url	URL	Universal Resource Locator for a web page
security_mode	String	High, medium, or low. High is the control condition
Startdate	Timestamp	Time and date an event started DOW MMM DD YYYY HH:MM:SS
Userid	String	User identifier (email)
userkey	String	User identifier BTOA
category	String	Category for the transaction (depends on table)
Appname	String	Application name

Data Source Tables From FireBase

- answers - answers to the SUS survey
    - Unique Transaction ID
        - answer -
        - answerval
        - email
        - firebaseUID
        - qname
        - startedAt
- clues – successful uses of the app to retrieve clues based on security mode
    - Unique Transaction ID
        - appname
        - category
        - firebaseUID

- security_mode
- startdate
- startedAt
- url
- userid
- userkey

- comments – comments made at end of post-study survey
  - Unique Transaction ID
    - answer
    - email
    - firebaseUID
    - startedAt
- users – information about user approved locations
  - userkey
    - email
    - firebaseUID
    - geofire – GeoFire info on locations
    - locations – descriptive info on locations
    - nickname – location nickname
    - pwc – password clue for GetMyCLUE
    - websites
- gmcClues – uses of clues to access apps
  - Unique Transaction ID
    - appname
    - category
    - firebaseUID
    - security_mode
    - startdate
    - startedAt
    - url
    - userid
    - userkey
- gmcClues – session information on use of the GetMyCLUE app
  - Unique Transaction ID
    - appname
    - category
    - firebaseUID
    - security_mode
    - startdate
    - startedAt
    - url
    - userid
    - userkey
- resetpw – password resets for CLUE
  - Unique Transaction ID
    - appname
    - startdate

- startedAt
- userid
- userkey

- sessions –session information for CLUE
  - Unique Transaction ID
    - enddate
    - endedAt
    - firebaseUID
    - mobileDevice
    - startdate
    - startedAt
    - userid
    - userkey
- taskusage – CLUE usage for specific tasks
  - Unique Transaction ID
    - appname
    - category
    - firebaseUID
    - security_mode
    - startdate
    - startedAt
    - url
    - userid
    - userkey

Appendix H – Recruitment and Demographic Data

This appendix includes information about both the potential pool of subjects and the pool that proceeded to the study. The findings discuss the difficulties of getting participation in security research. The high attrition rate of subjects demonstrates this. Unlike typical information systems research, the women outnumber the men two to one. This is due to the convenience sample containing, among others, a large group of technical women.

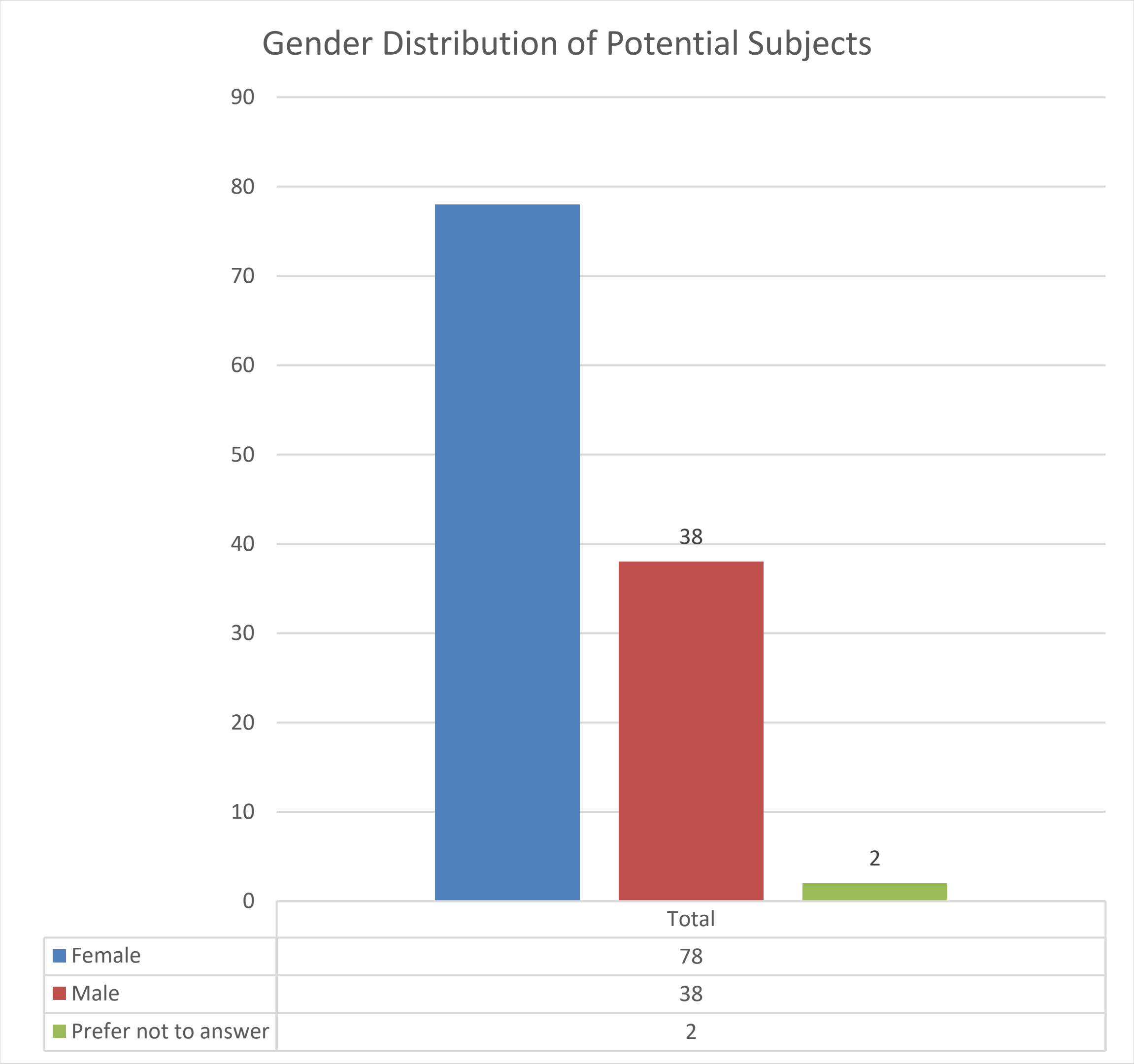
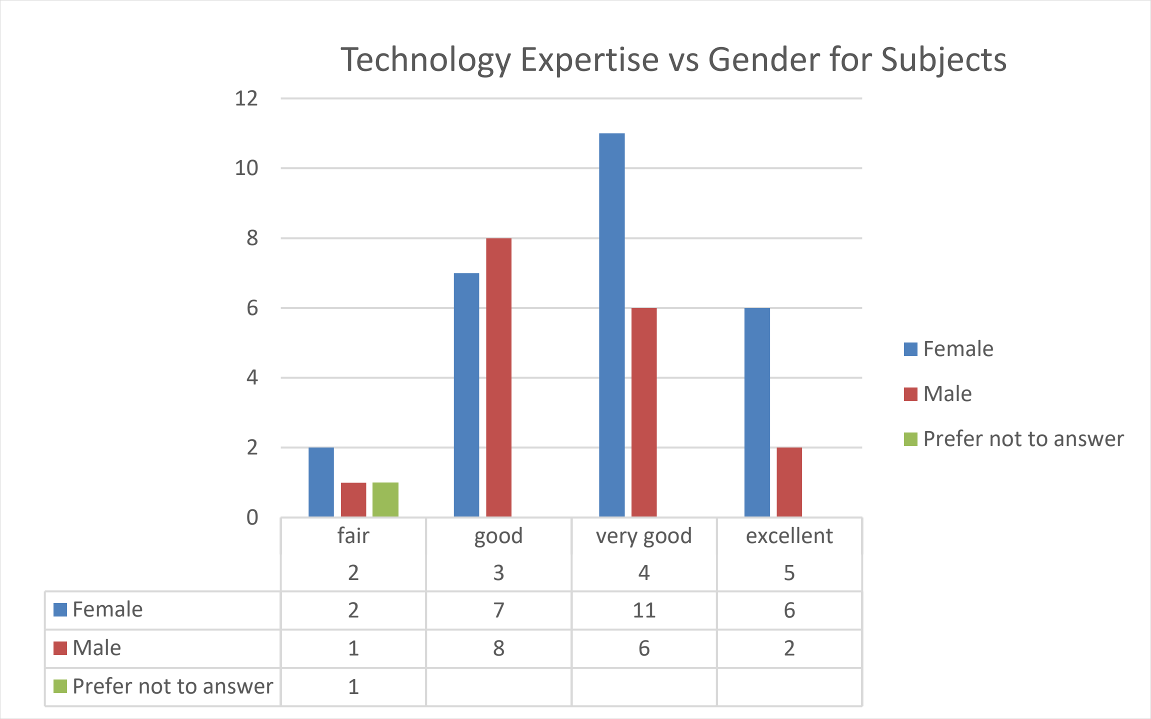
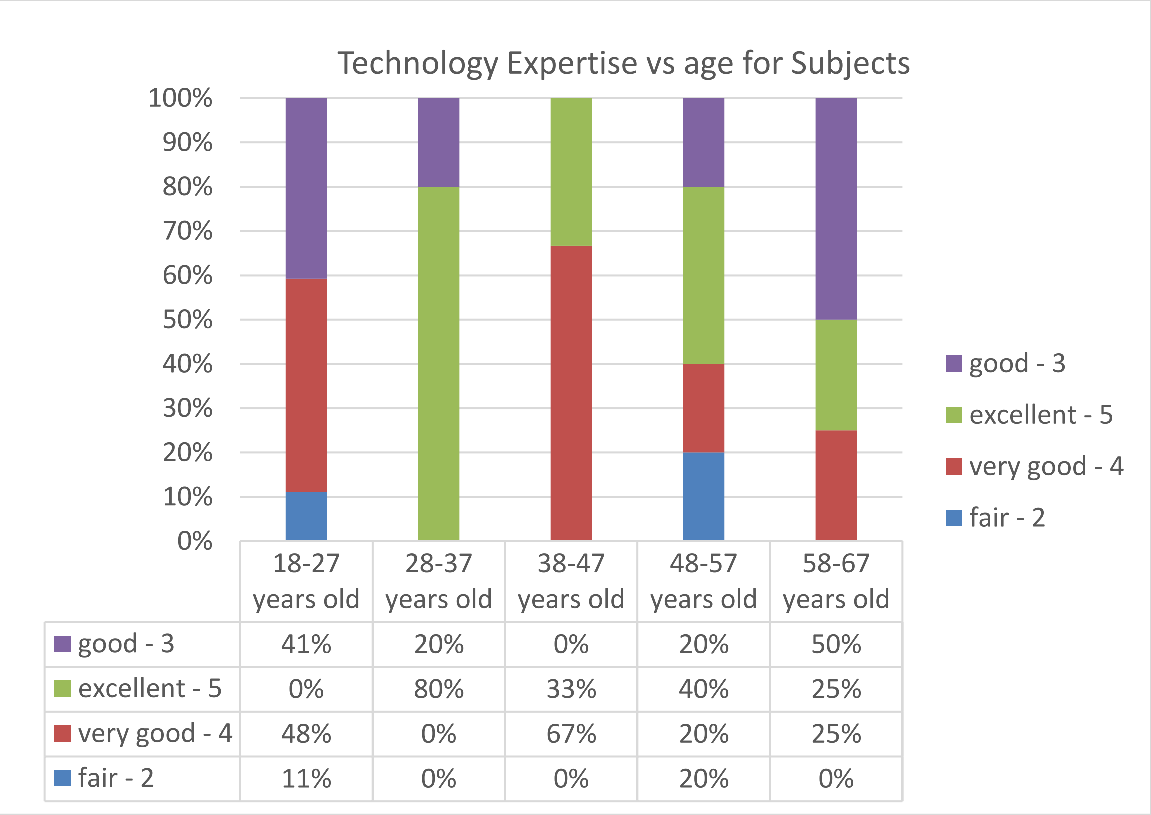


Figure H 1. Gender Distribution of Potential Subjects



	fair 2	good 3	very good 4	excellent 5
🟦 Female	2	7	11	6
🟥 Male	1	8	6	2
🟩 Prefer not to answer	1			

Figure H 2. Technology Expertise vs. Gender for Subjects



	18-27 years old	28-37 years old	38-47 years old	48-57 years old	58-67 years old
🟪 good - 3	41%	20%	0%	20%	50%
🟩 excellent - 5	0%	80%	33%	40%	25%
🟥 very good - 4	48%	0%	67%	20%	25%
🟦 fair - 2	11%	0%	0%	20%	0%

Figure H 3. Technology Expertise vs. age for Subjects

Appendix I – Data from usage of Webapp CLUE

“High mobile” and “High desktop” represent the current norm. The effort conserved is the difference between the effort consumed by a security task in control mode and the effort consumed in the revised mode (Table I 2). There were 1700 separate uses of the webapp to navigate the security interface.

Table I 1. Constrained Resource Consumed by Security Task and Risk

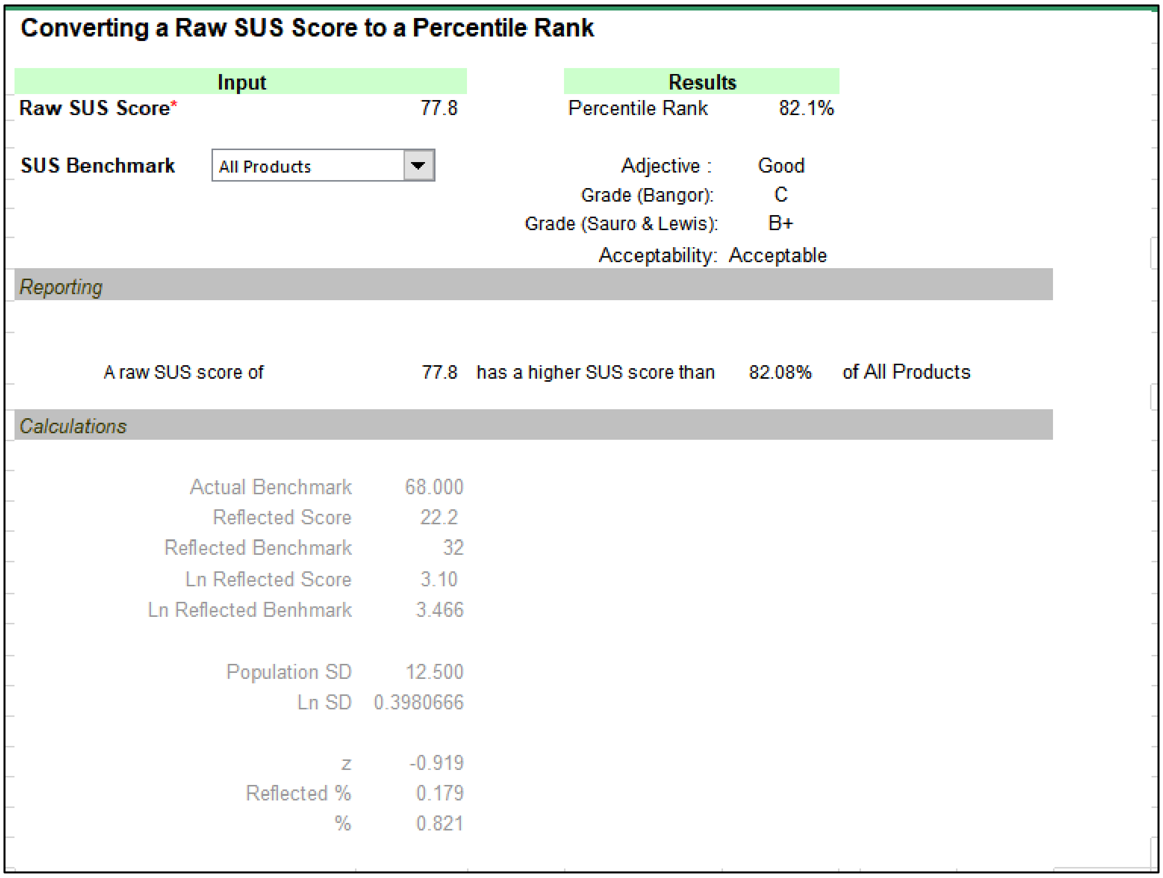
Row Labels	Clue	High Mobile	Med Mobile	Low Mobile	High Desktop	Med Desktop	Low Desktop
form factor		**27.6**	**14.6**	**11.9**	30.5	17.2	14.1
Logon Attempt	URL	16.4	7.2	7.2	14	7.2	7.2
Password recovery	Clue	3.7	3.7	1	5	5	1.9
UID recovery	Userid	3.8	0	0	6.5	0	0
Password reset		3.7	3.7	3.7	5	5	5
power		**8**	**6.5**	**4.5**	6	4.5	3
Logon Attempt	URL	1.5	0.5	0.5	1.5	0.5	0.5
Password recovery	Clue	3	3	1	2	2	0.5
UID recovery	Userid	0.5	0	0	0.5	0	0
Password reset		3	3	3	2	2	2
user effort		**144**	**111.6**	**73.2**	54	48	32.4
Logon Attempt	URL	50.4	25.2	25.2	9.6	7.2	7.2
Password recovery	Clue	43.2	43.2	4.8	20.4	20.4	4.8
UID recovery	Userid	7.2	0	0	3.6	0	0
Password reset		43.2	43.2	43.2	20.4	20.4	20.4

Table I 2. Seconds of Time Conserved Using the Revised Design.

	Clue	High Mobile	Med Mobile	Low Mobile	High Desktop	Med Desktop	Low Desktop
form factor							
Logon Attempt	URL	0	9.2	9.2	0	6.8	6.8
Password recovery	Clue	0	0	2.7	0	0	3.1
UID recovery	Userid	0	3.8	3.8	0	6.5	6.5
Password reset		0	0	0	0	0	0
power							
Logon Attempt	URL	0	1	1	0	1	1
Password recovery	Clue	0	0	2	0	0	1.5
UID recovery	Userid	0	0.5	0.5	0	0.5	0.5
Password reset		0	0	0	0	0	0
user effort							
Logon Attempt	URL	0	25.2	25.2	0	2.4	2.4
Password recovery	Clue	0	0	38.4	0	0	15.6
UID recovery	Userid	0	7.2	7.2	0	3.6	3.6
Password reset		0	0	0	0	0	0

Appendix J – Calculations for System Usability Scale

This appendix contains all the calculations for changing the raw SUS score to a percentile rank for the five different categories of software. All the categories could be used to describe the CLUE webapp. Though the actual SUS score doesn't change, the same score varies in how it compares to other products in a category.



Converting a Raw SUS Score to a Percentile Rank

Input		Results	
Raw SUS Score*	77.8	Percentile Rank	82.1%
SUS Benchmark	All Products	Adjective :	Good
		Grade (Bangor):	C
		Grade (Sauro & Lewis):	B+
		Acceptability:	Acceptable

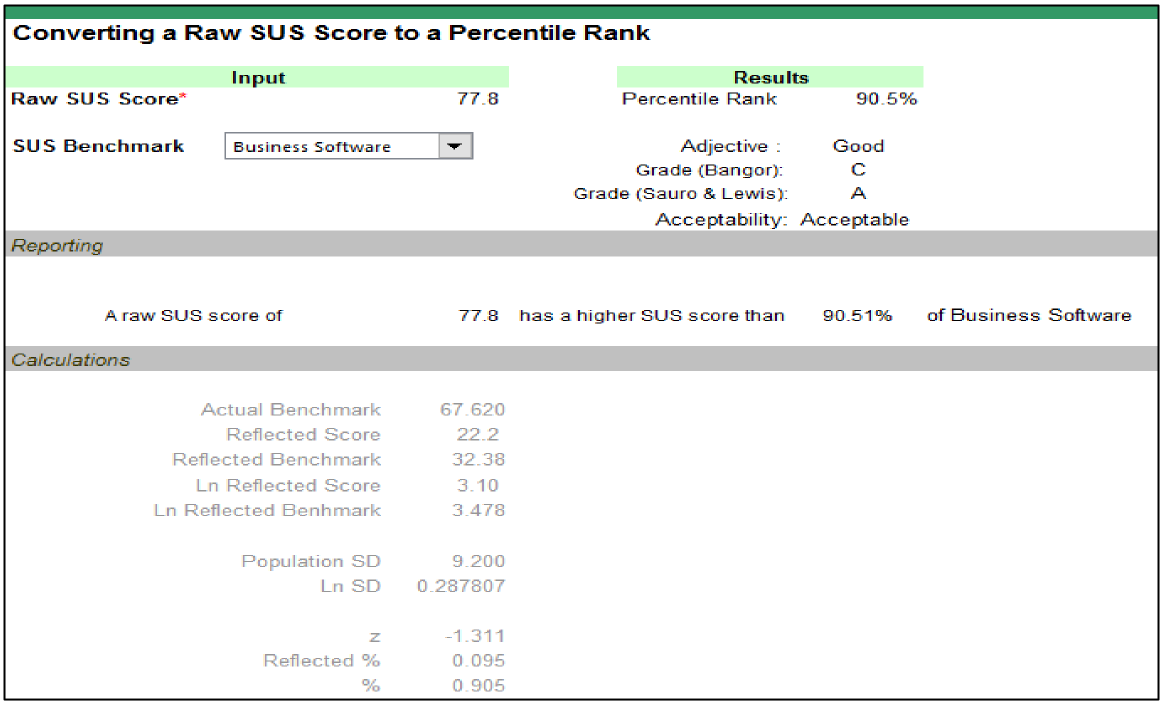
Reporting

A raw SUS score of 77.8 has a higher SUS score than 82.08% of All Products

Calculations

Actual Benchmark	68.000
Reflected Score	22.2
Reflected Benchmark	32
Ln Reflected Score	3.10
Ln Reflected Benhmark	3.466
Population SD	12.500
Ln SD	0.3980666
z	-0.919
Reflected %	0.179
%	0.821

Figure J 1. SUS Calculation CLUE vs All ProductsFigure



Converting a Raw SUS Score to a Percentile Rank

Input			Results	
Raw SUS Score*	77.8		Percentile Rank	90.5%
SUS Benchmark	Business Software		Adjective :	Good
			Grade (Bangor):	C
			Grade (Sauro & Lewis):	A
			Acceptability:	Acceptable

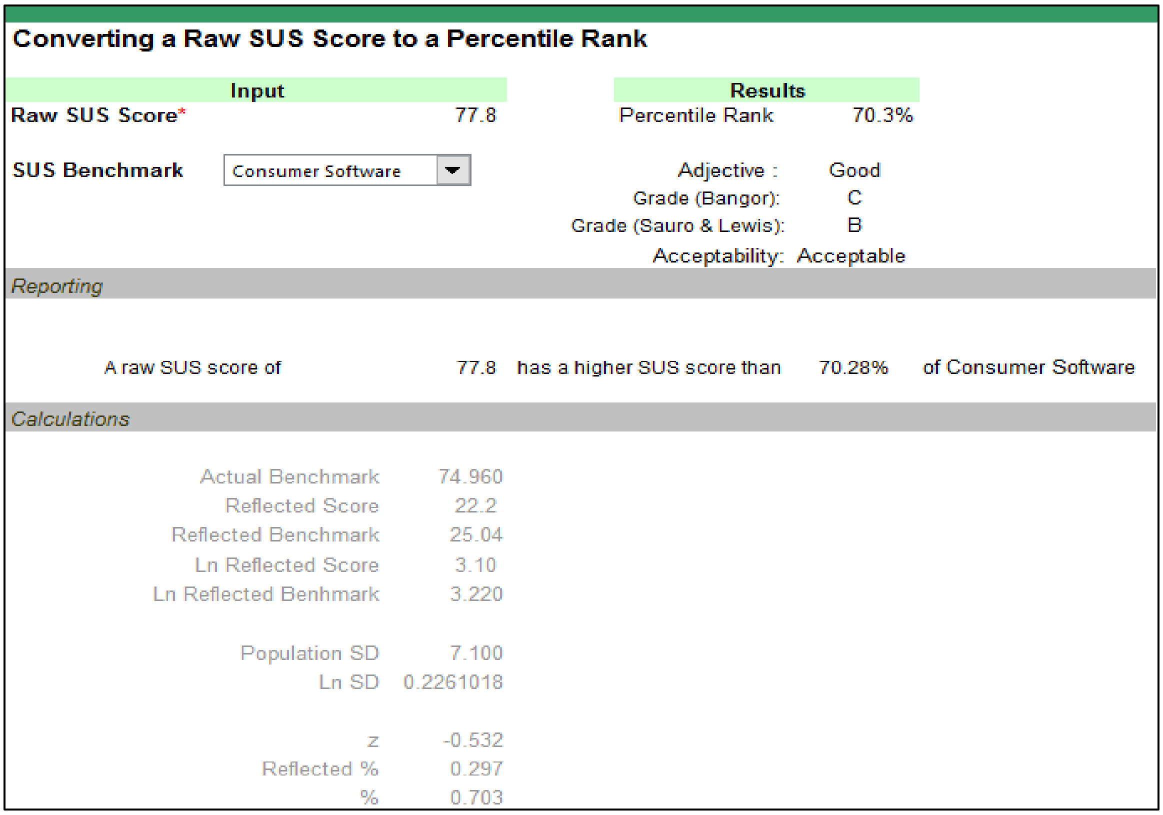
Reporting

A raw SUS score of 77.8 has a higher SUS score than 90.51% of Business Software

Calculations

Actual Benchmark	67.620
Reflected Score	22.2
Reflected Benchmark	32.38
Ln Reflected Score	3.10
Ln Reflected Benhmark	3.478
Population SD	9.200
Ln SD	0.287807
z	-1.311
Reflected %	0.095
%	0.905

Figure J 2. SUS Score for GMC vs. Business Software



Converting a Raw SUS Score to a Percentile Rank

Input			Results	
Raw SUS Score*	77.8		Percentile Rank	70.3%
SUS Benchmark	Consumer Software		Adjective :	Good
			Grade (Bangor):	C
			Grade (Sauro & Lewis):	B
			Acceptability:	Acceptable

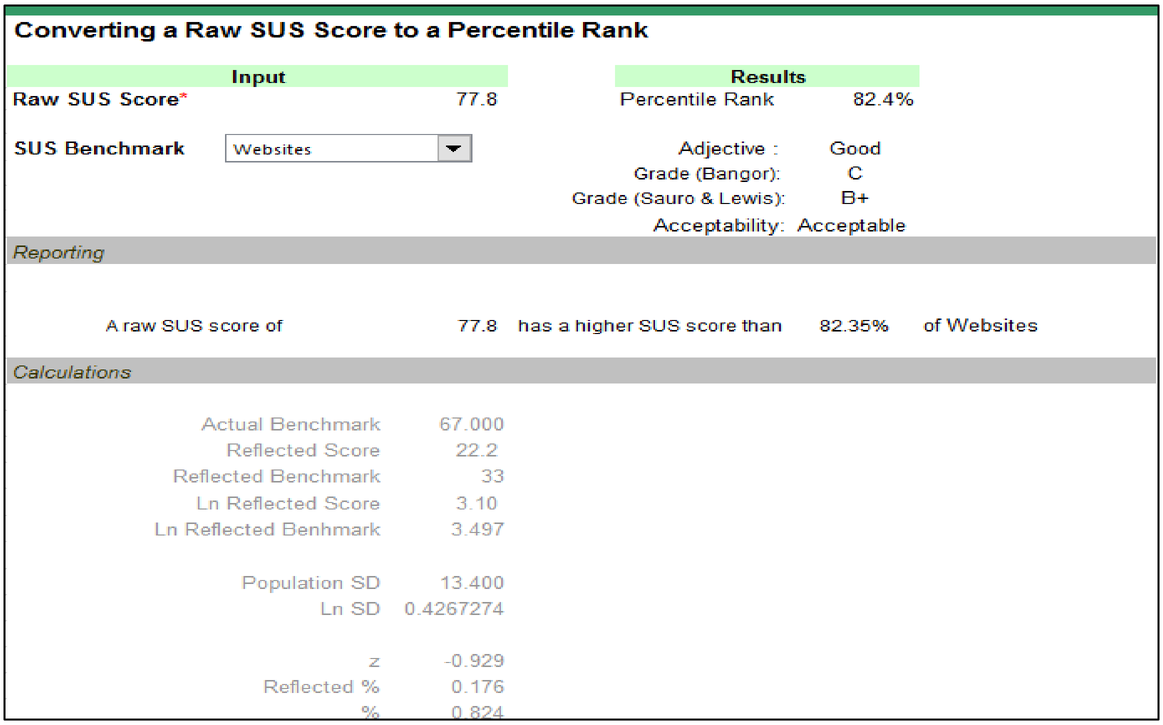
Reporting

A raw SUS score of 77.8 has a higher SUS score than 70.28% of Consumer Software

Calculations

Actual Benchmark	74.960
Reflected Score	22.2
Reflected Benchmark	25.04
Ln Reflected Score	3.10
Ln Reflected Benhmark	3.220
Population SD	7.100
Ln SD	0.2261018
z	-0.532
Reflected %	0.297
%	0.703

Figure J 3. SUS Score for GMC vs. Consumer SoftwareFigure J 1.



Converting a Raw SUS Score to a Percentile Rank

Input			Results	
Raw SUS Score*		77.8	Percentile Rank	82.4%
SUS Benchmark	Websites		Adjective :	Good
			Grade (Bangor):	C
			Grade (Sauro & Lewis):	B+
			Acceptability:	Acceptable

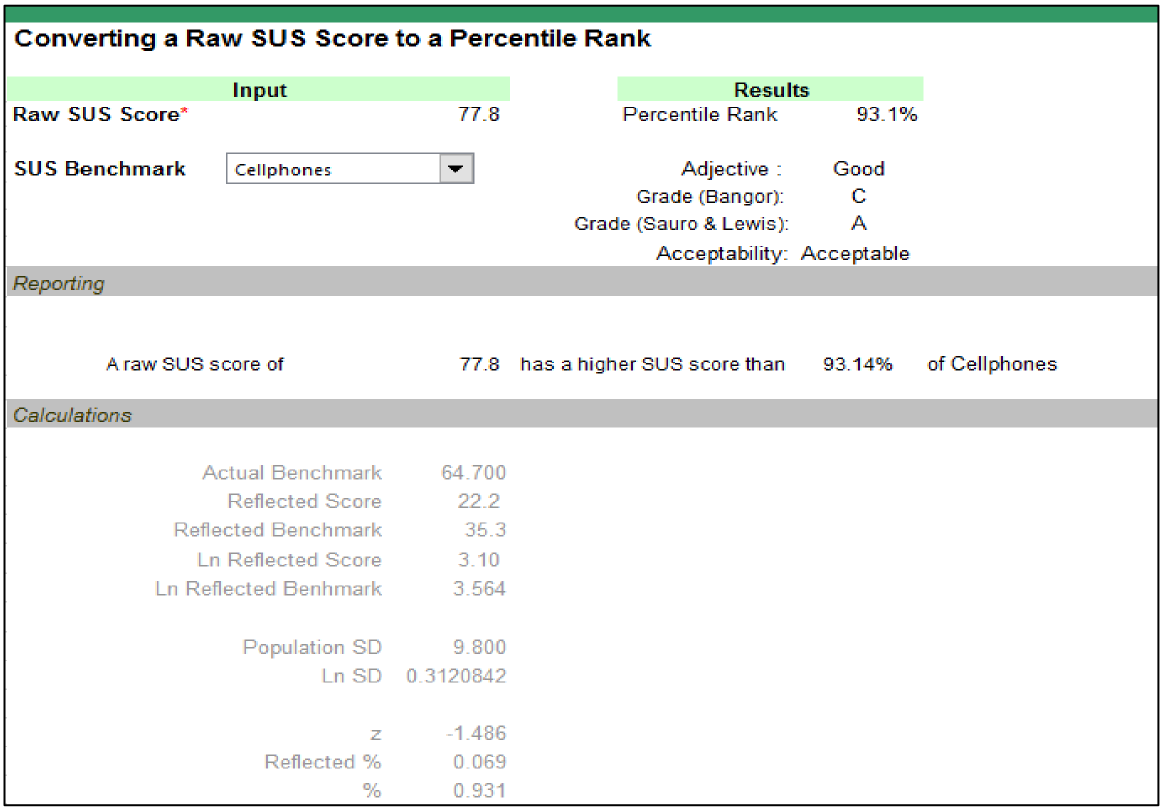
Reporting

A raw SUS score of 77.8 has a higher SUS score than 82.35% of Websites

Calculations

Actual Benchmark	67.000
Reflected Score	22.2
Reflected Benchmark	33
Ln Reflected Score	3.10
Ln Reflected Benhmark	3.497
Population SD	13.400
Ln SD	0.4267274
z	-0.929
Reflected %	0.176
%	0.824

Figure J 4. SUS Score for GMC vs. Websites.



Converting a Raw SUS Score to a Percentile Rank

Input			Results	
Raw SUS Score*		77.8	Percentile Rank	93.1%
SUS Benchmark	Cellphones		Adjective :	Good
			Grade (Bangor):	C
			Grade (Sauro & Lewis):	A
			Acceptability:	Acceptable

Reporting

A raw SUS score of 77.8 has a higher SUS score than 93.14% of Cellphones

Calculations

Actual Benchmark	64.700
Reflected Score	22.2
Reflected Benchmark	35.3
Ln Reflected Score	3.10
Ln Reflected Benhmark	3.564
Population SD	9.800
Ln SD	0.3120842
z	-1.486
Reflected %	0.069
%	0.931

Figure J 5. SUS Score for GMC vs. Cellphones

Appendix K – IRB Memo

NOVA SOUTHEASTERN UNIVERSITY

Office of Grants and Contracts

Institutional Review Board

MEMORANDUM

To: Ann-Marie Horcher

From: Ling Wang, Ph.D.

Institutional Review Board

Signature

Date: Dec. 8, 2014

Re: *Evaluation of a mobile security Interface designed with security usability principles to conserve constrained resources*

IRB Approval Number: wang07151401

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

References

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

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Aiello, L. M., & Ruffo, G. (2012). LotusNet: Tunable privacy for distributed online social network services. *Computer Communications, 35*(1), 75-88.

Al-Khalifa, H. S., Al-Mohsin, M., Al-Twaim, M., & Al-Razgan, M. S. (2014). Soft Keyboard UX Evaluation: An Eye Tracking Study. *Proceedings of the 6th International Conference on Management of Emergent Digital EcoSystems,* 78-84.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security, 28*(6), 476-490.

Almuairfi, S., Veeraraghavan, P., & Chilamkurti, N. (2013). A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. *Mathematical and Computer Modelling, 58*(1), 108-116.

Anand, B., Thirugnanam, K., Sebastian, J., Kannan, P. G., Ananda, A. L., Chan, M. C., & Balan, R. K. (2011). Adaptive display power management for mobile games. *Proceedings of the 9th international conference on Mobile systems, applications, and services*, 57-70.

Androutsos, A. (2011). Access link bandwidth externalities and endogenous internet growth: a long-run economic approach. *International Journal of Network Management., 21*(1), 21-44.

Arif, A., Pahud, M., Hinckley, K., & Buxton, W. (2013). 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, MobileHCI 2013*, 486-491.

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

Azer, M. A., El-Kassas, S. M., & El-Soudani, M. S. (2009). Security in Ad Hoc Networks: From Vulnerability to Risk Management. *Proceedings of 2009 Third*

International Conference on Emerging Security Information, Systems and Technologies, 203-209.

Bangor, A., Kortum, P., & Miller, J. (2009). Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of Usability Studies, 4*(3), 114-123.

Barkhuus, L., & Polichar, V. (2011). Empowerment through seamfulness: smart phones in everyday life. *Personal and Ubiquitous Computing, 15*(6), 629-639.

Basin, D., Cremers, C., & Meier, S. (2012). Provably repairing the ISO/IEC 9798 standard for entity authentication. *Proceedings of the First international conference on Principles of Security and Trust*, 129-148.

Bellamy, R., John, B., & Kogan, S. (2011). Deploying CogTool: integrating quantitative usability assessment into real-world software development. *Proceedings of the 33rd International Conference on Software Engineering*, 691-700.

Ben-Asher, N., Meyer, J., Moller, S., & Englert, R. (2009). An Experimental System for Studying the Tradeoff between Usability and Security. *2009 International Conference on Availability Reliability and Security (Ares) Proceedings* 882-887.

Bernal, J. F. M., Ardito, L., Morisio, M., & Falcarin, P. (2010). 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*, 510-514.

Bhensook, N., & Senivongse, T. (2012). An assessment of security requirements compliance of cloud providers. *Proceedings of the 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom)*, 520-525.

Bi, X., Smith, B. A., & Zhai, S. (2010). Quasi-qwerty soft keyboard optimization. *Proceedings of the SIGCHI conference on Human factors in computing systems*, 283-286.

Biddle, R., Chiasson, S., & Oorschot, P. C. V. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys, 44*(4), 1-41.

Bishop, M. (2005). Psychological acceptability revisited. In L. F. Cranor & S. L. Garfinkel (Eds.), *Security and Usability* (pp. 1-12). Sebastopol, CA: O'Reilly and Associates.

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

Bliss, A. (2015, 2015-11-06). How Long Is The Average Email Address? *FreshPerspectives Blog.* Retrieved from http://www.freshaddress.com/fresh-perspectives-blog/long-email-addresses/

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2008). From desktop to mobile: Examining the security experience. *Computers & Security, 28*(3-4), 130-137.

Bowen, J., Reeves, S., & Schweer, A. (2013). A tale of two studies. *Proceedings of the Fourteenth Australasian User Interface Conference - Volume 139,* 81-89.

Bruun, A., Gull, P., Hofmeister, L., & Stage, J. (2009). Let your users do the testing: a comparison of three remote asynchronous usability testing methods. *Proceedings of the 27th international conference on Human factors in computing systems*, 1619-1628.

Bulling, A., Alt, F., & Schmidt, A. (2012). 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*, 3011-3020.

Capek, J., Hub, M., Myskova, R., & Roudny, R. (2010). Petri nets-based models for basic authentication procedure. *Proceedings of the 2010 international conference on Communication and management in technological innovation and academic globalization*, 57-61.

Card, S. K., Moran, T. P., & Newell, A. (1980). The keystroke-level model for user performance time with interactive systems. *Commun. ACM, 23*(7), 396-410.

Carne, X. D., Carnavalet, D., & Mannan, M. (2015). A Large-Scale Evaluation of High-Impact Password Strength Meters. *ACM Transactions on Information and System Security (TISSEC), 18*(1), 1-32.

Chiang, H.-Y., & Chiasson, S. (2013). 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, MobileHCI 2013*, 251-260.

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

Churchill, D., & Hedberg, J. (2008). Learning object design considerations for small-screen handheld devices. *Computers & Education, 50*(3), 881-893.

Cranor, L. F., & Garfinkel, S. L. (2005). *Security and Usability: Designing Secure Systems that People Can Use*: O'Reilly Media.

D'Aubeterre, F., Singh, R., & Iyer, L. (2008). Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. *Eur J Inf Syst, 17*(5), 528-542.

Dubois, P. F. (2007). Guest Editor's Introduction: Python: Batteries Included. *Computing in Science and Engg., 9*(3), 7-9.

Dunphy, P., Nicholson, J., & Olivier, P. (2008). Securing passfaces for description. *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS),* 24-35.

Dunphy, P., & Olivier, P. (2012). On automated image choice for secure and usable graphical passwords. *Proceedings of the 28th Annual Computer Security Applications Conference*, 99-108.

Dykstra-Erickson, E. (2000). Interview: Ben Shneiderman and Allison Druin. *interactions, 7*(2), 59-65.

Economides, A. A., & Grousopoulou, A. (2009). Students' thoughts about the importance and costs of their mobile devices' features and services. *Telematics and Informatics, 26*(1), 57-84.

Engelberg, J. K., Hill, L. L., Rybar, J., & Styer, T. (2015). Distracted driving behaviors related to cell phone use among middle-aged adults. *Journal of Transport & Health, 2*(3), 434-440.

Everitt, K. M., Bragin, T., Fogarty, J., & Kohno, T. (2009). A comprehensive study of frequency, interference, and training of multiple graphical passwords. *Proceedings of the SIGCHI conference on Human factors in computing systems*, 889-898.

Finstad, K. (2010). Response interpolation and scale sensitivity: evidence against 5-point scales. *Journal of Usability Studies, 5*(3), 104-110.

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th international conference on World Wide Web,* 657-666.

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? . *Computer Fraud & Security.* Retrieved from http://www.sciencedirect.com/science/article/B6VNT-4S807WG-F/2/0c9e7de7efb8df6814a63948a149cb5a

Furnell, S. (2011). Assessing password guidance and enforcement on leading websites. *Computer Fraud & Security, 2011*(12), 10-18.

Gao, H., Ma, L., Jia, W., & Ye, F. (2012). Multiple password interference in graphical passwords. Journal of Information and Computer Security*, 5*(1), 11-27.

Garfinkel, S. L. (2005). *Design principles and patterns for computer systems that are simultaneously secure and usable.* (Doctoral dissertation), Massachusetts Institute of Technology, Boston, MA.

Garfinkel, S. L. (2008). IRBs and security research: myths, facts and mission creep. *Proceedings of the 1st Conference on Usability, Psychology, and Security*, 1-5.

Gebauer, J., Kline, D. M., & He, L. (2011). 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, 4*(2), 52-62.

Google. (2017a). Firebase Authentication. *Firebase.*

Google. (2017b). Firebase Realtime Database. *Firebase.*

Harbach, M., Von Zezschwitz, E., Fichtner, A., De Luca, A., & Smith, M. (2014). It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception. *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS),* 213-230.

Harris, R. A. (2005). Chapter 8 - Crafting Voice Interfaces *Voice Interaction Design* (pp. 203-222). San Francisco: Morgan Kaufmann.

Haverila, M. (2011). What do we want specifically from the cell phone? An age related study. *Telematics and Informatics, 29*(1), 110-122.

Hayashi, E., Riva, O., Strauss, K., Brush, A. J. B., & Schechter, S. (2012). Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS),* 1-11.

Heeringa, S., West, B., & Berglund, P. (2010). *Applied survey data analysis*: CRC Press.

Herley, C. (2009b). 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*, 133-144.

Hertzum, M., & Clemmensen, T. (2012). How do usability professionals construe usability? *International Journal of Human-Computer Studies, 70*(1), 26-42.

Herzberg, A., & Margulies, R. (2012). Training Johnny to Authenticate (Safely). *IEEE Security & Privacy, 10*(1), 37-45.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly, 28*(1).

Holleis, P., Luther, M., Broll, G., & Souville, B. (2013). A DIY power monitor to compare mobile energy consumption in situ. *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, 416-421.

Holleis, P., Scherr, M., & Broll, G. (2011). 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*, 204-221.

Hong, J., Heo, S., Isokoski, P., & Lee, G. (2015). SplitBoard: A Simple Split Soft Keyboard for Wristwatch-sized Touch Screens. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 1233-1236.

Horcher, A.-M., & Tejay, G. P. (2009). 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*, 113-118.

Hosmer, C., Jeffcoat, C., Davis, M., & McGibbon, T. (2011). Use of mobile technology for information collection and dissemination. *Data & Analysis Center for Software*, *77*.

Howarth, J., Smith-Jackson, T., & Hartson, R. (2009). Supporting novice usability practitioners with usability engineering tools. *International Journal of Human-Computer Studies, 67*(6), 533-549.

Hudert, S., Niemann, C., & Eymann, T. (2010). On computer simulation as a component in information systems research. *Proceedings of the 5th international conference on Global Perspectives on Design Science Research*, 167-179.

Hwang, W., & Salvendy, G. (2010). Number of people required for usability evaluation: the 10 plus or minus 2 rule, *Communications of the ACM, 53*(5), 130-133.

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

John, B. E., Swart, C., Bellamy, R. K. E., Blackmon, M. H., & Brown, R. (2013). An open source approach to information scent. *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, 355-360.

Jokela, T., Iivari, N., Matero, J., & Karukka, M. (2003). The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11. *Proceedings of the Latin American conference on Human-computer interaction*, 53-60.

Ka-Ping, Y. (2004). Aligning security and usability. *IEEE Security & Privacy, 2*(5), 48-55.

Kao, P.-C., Higginson, C. I., Seymour, K., Kamerdze, M., & Higginson, J. S. (2015). Walking stability during cell phone use in healthy adults. *Gait & Posture, 41*(4), 947-953.

Karypidis, A., & Lalis, S. (2007). OmniStore: Automating data management in a personal system comprising several portable devices. *Pervasive and Mobile Computing, 3*(5), 512-536.

Keith, M., Shao, B., & Steinbart, P. J. (2007). The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies, 65*(1), 17-28.

Khansa, L., & Liginlal, D. (2009). Valuing the flexibility of investing in security process innovations. *European Journal of Operational Research, 192*(1), 216-235.

Kim, D., Dunphy, P., Briggs, P., Hook, J., Nicholson, J. W., Nicholson, J., & Olivier, P. (2010). Multi-touch authentication on tabletops. *Proceedings of the SIGCHI conference on Human factors in computing systems*, 1093-1102.

Knight, A., Pyrzak, G., & Green, C. (2007). When two methods are better than one: combining user study with cognitive modeling. *CHI '07 Extended Abstracts on Human Factors in Computing Systems*, 1783-1788.

Kortum, P., & Acemyan, C. Z. (2013). How low can you go?: is the system usability scale range restricted? *Journal of Usability Studies, 9*(1), 14-24.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

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

Lee, K.-W., & Ewe, H.-T. (2007). Passphrase with Semantic Noises and a Proof on Its Higher Information Rate. *Proceedings of the 2007 International Conference on Computational Intelligence and Security Workshops*, 652-655.

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

Lenox, T., Pilarski, N., Leathers, L., & (2012). The Effects of Interruptions on Remembering Task Information. *Journal of Information Systems Applied Research, 5*(4), 11-22.

Lerner, R. M. (2012). At the forge: twitter bootstrap. *Linux Journal, 2012*(218), 6.

Lewis, J., & Sauro, J. (2009). The Factor Structure of the System Usability Scale. In M. Kurosu (Ed.), *Human centered design* (Vol. 5619, pp. 94-103): Springer Berlin Heidelberg.

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

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

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology, 22 140*, 55.

Lim, J., Amado, A., Sheehan, L., & Van Emmerik, R. E. A. (2015). Dual task interference during walking: The effects of texting on situational awareness and gait stability. *Gait & Posture, 42*(4), 466-471.

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., & Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 501-510.

Lipovac, K., Đerić, M., Tešić, M., Andrić, Z., & Marić, B. (2017). Mobile phone use while driving-literary review. *Transportation Rsearch Part F: Traffic Psychology and Behaviour, 47*, 132-142.

Lu, Y., Yu, C., Yi, X., Shi, Y., & Zhao, S. (2017). BlindType: Eyes-Free Text Entry on Handheld Touchpad by Leveraging Thumb's Muscle Memory. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, (2), 1-24.*

Mairiza, D., & Zowghi, D. (2010). An ontological framework to manage the relative conflicts between security and usability requirements. *Managing Requirements Knowledge (MARK), 2010 Third International Workshop on*, 1-6.

Morris, R., & Thompson, K. (1979). Password security: A case history. *Communications of the ACM, 22*(11), 594-597.

Muttart, J., Fisher, D., Knodler, M., & Pollatsek, A. (2007). Driving Without a Clue: Evaluation of Driver Simulator Performance During Hands-Free Cell Phone Operation in a Work Zone. *Transportation Research Record: Journal of the Transportation Research Board, 2018*, 9-14.

Mwakalonge, J., Siuhi, S., & White, J. (2015). Distracted walking: Examining the extent to pedestrian safety problems. *Journal of Traffic and Transportation Engineering (English Edition), 2*(5), 327-337.

Nasar, J., Hecht, P., & Wener, R. (2008). Mobile telephones, distracted attention, and pedestrian safety. *Accident Analysis & Prevention, 40*(1), 69-75.

Nassi, I., & Shneiderman, B. (1973). Flowchart techniques for structured programming. *ACM SIGPLAN Notice*s, *8*(8), 12-26.

Nelson, D., & Vu, K.-P. L. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior, 26*(4), 705-715.

Nielsen, J. (1990). Traditional dialogue design applied to modern user interfaces. *Communications of the ACM, 33*(10), 109-118.

Nielsen, J. (2011). Kindle Fire Usability Findings. Retrieved from http://www.useit.com/alertbox/kindle-fire-usability.html

Oberheide, J., & Jahanian, F. (2010). 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*, 43-48.

Ocak, N., & Cagiltay, K. (2016). Comparison of Cognitive Modeling and User Performance Analysis for Touch Screen Mobile Interface Design. *International Journal of Human–Computer Interaction*, 1-9.

Orphanides, A. K., & Nam, C. S. (2017). Touchscreen interfaces in context: A systematic review of research into touchscreens across settings, populations, and implementations. *Applied Ergonomics, 61*, 116-143.

Parhi, P., Karlson, A. K., & Bederson, B. B. (2006). Target size study for one-handed thumb use on small touchscreen devices. *Proceedings of the 8th conference on Human-computer interaction with mobile devices and services*, 203-210.

Park, H., & Redford, S. (2007). Client certificate and IP address based multi-factor authentication for J2EE web applications. *Proceedings of the 2007 conference of the center for advanced studies on Collaborative research*, 167-174.

Park, T., Lee, J., Hwang, I., Yoo, C., Nachman, L., & Song, J. (2011). E-Gesture: a collaborative architecture for energy-efficient gesture recognition with hand-worn sensor and mobile devices. *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*, 260-273.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611.

Pfleeger, S. L., & Pfleeger, C. P. (2009). Harmonizing privacy with security principles and practices. *IBM Journal of Research and Development*, *53*(2), 273-289.

Pinkas, B., & Sander, T. (2002). Securing passwords against dictionary attacks. *Proceedings of the 9th ACM conference on Computer and Communications Security*, 161-170.

Poremba, S. M. (2014, February 7). How a Single Username Puts Your Security at Risk. Retrieved from https://www.tomsguide.com/us/single-username-risks,news-18288.html.

Qing, L., & Clark, G. (2013). Mobile Security: A Look Ahead. *IEEE Security & Privacy, 11*(1), 78-81.

Ramos, M., Valente, M. T., Terra, R., & Santos, G. (2016). AngularJS in the wild: a survey with 460 developers. *Proceedings of the 7th International Workshop on Evaluation and Usability of Programming Languages and Tools*, 9-16.

Riva, O., Qin, C., Strauss, K., & Lymberopoulos, D. (2012). Progressive Authentication: Deciding When to Authenticate on Mobile Phones. *Proceedings of the 21sth conference on USENIX Security Symposium*, 301–316.

Roberts, M. (2010). *Internet Password Notebook: A pocket-sized Internet address organizer for all of your usernames and passwords (Volume 2)*: CreateSpace.

Saltzer, J. H., & Kaashoek, M. F. (2009). *Principles of Computer System Design: An Introduction*: Morgan Kaufmann Publishers Inc.

Sandnes, F. E. (2015). Reflective Text Entry: A Simple Low Effort Predictive Input Method Based on Flexible Abbreviations. *Procedia Computer Science, 67*, 105-112.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link'; a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal, 19*(3), 122-131.

Sauro, J. (2011). *A practical guide to the system usability scale (SUS)*: Amazon Digital Services LLC.

Sauro, J., & Lewis, J. R. (2011). When designing usability questionnaires, does it hurt to be positive? *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2215-2224.

Saxby, D. J., Matthews, G., & Neubauer, C. (2017). The relationship between cell phone use and management of driver fatigue: It's complicated. *Journal of Safety Research, 61*, 129-140.

Schmettow, M., Vos, W., & Schraagen, J. M. (2013). With how many users should you test a medical infusion pump? Sampling strategies for usability tests on high-risk systems. *Journal of Biomedical Informatics, 46*(4), 626-641.

Schmidt, D. C., Fayad, M., & Johnson, R. E. (1996). Software patterns. *Communications of the ACM, 39*(10), 37-39.

Schwebel, D. C., Stavrinos, D., Byington, K. W., Davis, T., O'Neal, E. E., & de Jong, D. (2012). Distraction and pedestrian safety: How talking on the phone, texting, and listening to music impact crossing the street. *Accident Analysis & Prevention, 45*, 266-271.

Serrano, M., Lecolinet, E., & Guiard, Y. (2013). Bezel-Tap gestures: quick activation of commands from sleep mode on tablets. *Proceedings of the SIGCHI conference on Human factors in computing systems*, 3027-3036.

Shankar, A., Lin, H., Brown, H.-F., & Rice, C. (2015). Rapid Usability Assessment of an Enterprise Application in an Agile Environment with CogTool. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, 719-726.

Shirazi, A. S., Henze, N., Dingler, T., Kunze, K., & Schmidt, A. (2013). 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*, 362-371.

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., Elmqvist, N., & Diakopoulos, N. (2016). *Designing the user interface: strategies for effective human-computer interaction*.

Simon, H. A. (1996). *The Sciences of the Artificial*. Boston, MA: MIT Press.

Singha, J., Misra, S., & Laskar, R. H. (2016). Effect of variation in gesticulation pattern in dynamic hand gesture recognition system. *Neurocomputing, 208*, 269-280.

Siponen, M. T. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and Organization*, *15*(4), 339-375.

Smith, R. E. (2012). A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles. *IEEE Security & Privacy, 10*(6), 20-25.

Stajano, F. (2011). Pico: no more passwords! In B. Christianson, B. Crispo, J. Malcolm, & F. Stajano (Eds.), *Security Protocols XIX. Security Protocols 2011. Lecture Notes in Computer Science* (Vol. 1174, pp. 49-81). Berlin, Heidelberg: Springer.

Steer, J., & Popli, A. (2008). “Building secure business applications at Microsoft” by J. Steer and A. Popli. *Information Security Technical Report, 13*(2), 104.

Stobert, E., & Biddle, R. (2013). Memory retrieval and graphical passwords. *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS),* 1-14.

Teo, L.-H., John, B., & Blackmon, M. (2012). CogTool-Explorer: a model of goal-directed user exploration that considers information layout. *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2479-2488.

Theofanos, M. F., & Pfleeger, S. L. (2011). Shouldn't All Security Be Usable? *IEEE Security & Privacy, 9*(2), 12-17.

Tilson, D., Sorensen, C., & Lyytinen, K. (2012). Change and Control Paradoxes in Mobile Infrastructure Innovation: The Android and iOS Mobile Operating Systems Cases. *Proceedings of the 45th Hawaii International Conference on System Science (HICSS - 2012),* 1324-1333.

Topkara, U., Atallah, M. J., & Topkara, M. (2007). Passwords decay, words endure: secure and re-usable multiple password mnemonics. *Proceedings of the 2007 ACM symposium on Applied computing*, 292-299.

Trinh, H., Waller, A., Vertanen, K., Kristensson, P. O., & Hanson, V. L. (2014). Phoneme-based predictive text entry interface. *Proceedings of the 16th international ACM SIGACCESS conference on Computers & accessibility,* 351-352.

Turpe, S. (2008). When it comes to Testing, is Usability the Closest Analogy to Security? *Software Testing Verification and Validation Workshop, 2008. ICSTW '08. IEEE International Conference on,* 302-304.

United States Figure Skating Association. (1998). *The Official Book of Figure Skating*: Simon & Schuster.

Vaishnavi, V., & Kuechler, B. (2015). *Design Science Research Methods and Patterns: Innovating Information and Communication Technology*: CRC Press.

Virginia Tech. (2011). When users resist: how to change management and user resistance to password security. *Pamplin.* Retrieved from http://www.magazine.pamplin.vt.edu/fall11/passwordsecurity.html.

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L., Cook, J., & Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*(8), 744-757.

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: a usability evaluation of PGP 5.0. *Proceedings of the 8th conference on USENIX Security Symposium,* 169–184..

Withana, A., Peiris, R., Samarasekara, N., & Nanayakkara, S. (2015). 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,* 3661-3670.

Yang, L., & Zhiyong, G. L. (2010). Internet's impact on expert–citizen interactions in public policymaking—A meta analysis. *Government Information Quarterly, 27*(4), 431-441.

Zezschwitz, E. v., Dunphy, P., & Luca, A. D. (2013). 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,* 261-270.

Zhu, M., Rudisill, T. M., Heeringa, S., Swedler, D., & Redelmeier, D. A. (2016). The association between handheld phone bans and the prevalence of handheld phone conversations among young drivers in the United States. *Annals of Epidemiology, 26*(12), 833-837.e831.