# The Convergence of Security and Usability: Defining a Framework for Mobile Design

Ann-Marie Horcher and Gurvirender Tejay

Nova Southeastern University
horcher@nova.edu

**Abstract.** Security and usability have traditionally been at odds in the design process [1]. In spite of this, the usability of security is widely recognized as a key component of security effectiveness[2-4] Design principles for good security have been designed by security experts [5]. Similarly principles for designed usability have also been created by usability experts [6-8]. In both cases the design principles were defined for the traditional workstation environment, instead of the mobile environment. This study examines both security and usability design principles for conflict or convergence, specifically in relation to a mobile environment. The resulting framework of combined security-usability principles identifies which design principles are critical for success in the mobile environment.

**Keywords:** usability, security, mobile devices, design principles.

## 1 Introduction

Security and usability design principles have been articulated for the traditional workstation environment. In contrast to the workstation environment, mobile devices have significant differences in the interaction of users, and the availability of resources [9]. These realities call for a revised set of design principles that address the limitations of a mobile environment to achieve 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 [10] on a mobile device. From environmental information to e-government services to phone directories, information delivery and interaction has shifted from print to exclusively electronic [11]. E-only delivery makes technology a necessity for all instead of a non-essential luxury item [12]. Increasingly mobile devices have moved from companion devices [13] to the primary or stand-alone device for digital information access [14]. Computer crime, already a problem on the traditional workstation [15, 16], has followed computer users to the mobile platform [17]. A mobile computing platform provides challenges in security that differ from the traditional computing workstation [9], and the structured work environment [18]. To effectively design these principles for usability and security in mobile devices, attention must be paid to the following:

C. Stephanidis (Ed.): Posters, Part I, HCII 2013, CCIS 373, pp. 119–123, 2013.

- The effort required of the user to follow security protocols [19]
- appropriate security for the value of the information
- resource constraints of the devices in terms of physical form factors [20] and device capabilities [21] .

## 2 Security versus Usability Design Principles

Systems designed with both security and usability principles remain more secure, because the users do not circumvent security for functionality [22]. System design can turn in a tug-of-war between the twin priorities, with many systems designers choosing to trade off usability for security and vice versa [23]. A combined framework removes the conflicting priorities.

**Table 1.** Combined Principles of Usability and Security

| **Saltzer & Schroeder [5]** | **Shneiderman [7]** | **Nielsen [6]** | **Garfinkel [24]** |
|---|---|---|---|
| Psychological Acceptability | Internal locus of control<br>Shortcuts for experience<br>Easy reversal of actions | User control and freedom<br>Flexibility and efficiency of use<br>Match between system and the real world | Least Surprise |
| Complete Mediation | Dialog to Closure<br>Informative Feedback | Visibility of system status Error prevention<br>Help and documentation | Consistent Meaningful Vocabulary |
| Least Common Mechanism<br>. | Consistency | Consistency and standards | Consistent Controls and Placement |
| Economy of Mechanism | Reduce short-term memory load | Recognition rather than recall<br>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<br>Promote Privacy<br>Never Assume Secrets are Safe<br>Principle of Least Privilege<br>Separation of Privilege/duty | Not mentioned | Not mentioned | Good Security Now |

To articulate the concept of secure design Saltzer & Schroeder (1975) created ten principles. At least half of the secure design principles relate directly to the interface with the user. Consequently "good" security design, or design created according to the principles, already includes guidance about the usability of the interface. Similar to the security principles created by Saltzer & Schroeder [5], the usability practitioners have the two seminal sets of heuristics or principles for design. The Golden Eight from Shneiderman [7] and ten more from Jakob Nielsen [6] form the core of usability design. Mapping the Shneiderman's Golden Eight Principles for usability [7] and Nielsen's Ten Heuristics for User Interface Design [6] to Saltzer & Schroeder's security design principles [5] yields an interesting result. Usability principles are not in conflict with secure design principles. Looking at the chart shows that for all the principles that address the user interface for security there is a parallel usability principle or principles stated for the same concept in both Shneiderman's Golden Eight Principles for Usability Design and Nielsen's Ten Heuristics for User Interface Design. Furthermore, Garfinkel [24] suggests design patterns as concrete examples of solutions to common security-usability problems. Design patterns leverage the best practices of a more skilled practitioner to compensate for the lack of skill in lesser experienced designer [25].

## 3 Security-Usability Design Principles for Mobile

Mobile devices have resource constraints that further impact the design of usable security The current security-usability framework described above does not address the resource constraints upon mobile devices. Creating a framework of combined security-usability principles that address the constraints yields principles more relevant to the mobile device platform. Simply transferring security practices from desktop to mobile has not yielded satisfactory usability and user acceptance [9]. The reality is that in the traditional workstation environment of a business or research organization ignoring certain security-usability principles has minor consequences [26]. In risk management assessment of information, the vulnerabilities are weighed against the probability of the occurrence, and the loss potentially incurred from the occurrence [27]. In the resource-constrained mobile device ignoring the consequences will compromise the practical functionality of the device.The three major resource constraints of the mobile device platform are power, form factors, and user expertise. To be mobile, the devices must run from a portable and renewable power source, such as a battery [28]. Security design drains battery life reduces the usability of the device. To be convenient mobile devices must be small enough and light enough to carry easily [29]. The screens must be big enough to use but small enough to fit in pocket or purse [30] and manipulated for information gathering in a variety of settings [31]. In the absence of a formal organization to compensate for individual user deficiencies, the applications must reduce complexity [30].

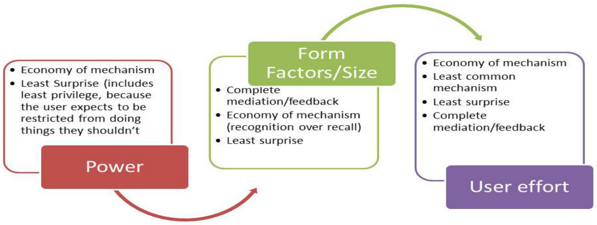
Economy of mechanism
Least Surprise (includes least privilege, because the user expects to be restricted from doing things they shouldn't
Power
Form Factors/Size
Complete mediation/feedback
Economy of mechanism (recognition over recall)
Least surprise
Economy of mechanism
Least common mechanism
Least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

**Fig. 1.** Security-usability principles addressing resource constraints of mobile devices

Based on this analysis, the combined security-usability principles that address the resource constraints are:

- Economy of mechanism
- Least surprise
- Complete mediation and feedback

The result of mapping resource constraints to the combined design principles is a framework that prioritizes conservation of resources. The framework also provides a common set of design principles that put security designers and usability designers on the same page instead of on opposing sides.

## References

1. Braz, C., Robert, J.-M.: Security and usability: the case of the user authentication methods. In: Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine, ACM, Montreal (2006)
2. Theofanos, M.F., Pfleeger, S.L.: Shouldn't All Security Be Usable? IEEE Security & Privacy 9(2), 12–17 (2011)
3. Cranor, L.F., Garfinkel, S.L.: Security and Usability: Designing Secure Systems that People Can Use. O'Reilly and Assoc. (2005)
4. Ka-Ping, Y.: Aligning security and usability. IEEE Security & Privacy 2(5), 48–55 (2004)
5. Saltzer, J.H., Schroeder, M.D.: The protection of information in computer systems. Proceedings of the IEEE 63(9), 1278–1308 (1975)
6. Nielsen, J.: Traditional dialogue design applied to modern user interfaces. Communications of the ACM 33(10), 109–118 (1990)
7. Shneiderman, B., et al.: Designing the user interface: Strategies for effective human-computer interaction, 5th edn. Addison-Wesley, Reading (2009)
8. Norman, D.A.: THE WAY I SEE IT: Systems thinking: a product is more than the product. Interactions 16(5), 52–54 (2009)
9. Oberheide, J., Jahanian, F.: When mobile is harder than fixed (and vice versa): Demystifying security challenges in mobile environments. In: Proceedings of the Eleventh Workshop on Mobile Computing Systems Applications, vol. 38, pp. 43–48 (2010)
10. Rahmati, A., Zhong, L.: Human-battery interaction on mobile phones. Pervasive and Mobile Computing 5(5), 465–477 (2009)

11. Kirk, C.P., Chiagouris, L., Gopalakrishna, P.: Some people just want to read: The roles of age, interactivity, and perceived usefulness of print in the consumption of digital information products. Journal of Retailing and Consumer Services (2011)
12. Kim, E., Lee, B., Menon, N.M.: Social welfare implications of the digital divide. Government Information Quarterly 26(2), 377–386 (2009)
13. Myers, B.A.: Using handhelds for wireless remote control of PCs and appliances. Interacting with Computers 17(3), 251–264 (2005)
14. West, J., Mace, M.: Browsing as the killer app: Explaining the rapid success of Apple's iPhone. Telecommunications Policy 34(5-6), 270–286 (2009)
15. Brenner, S.W.: History of computer crime. In: De Karl, L., Jan, B. (eds.) The History of Information Security, pp. 705–721. Elsevier Science B.V., Amsterdam (2007)
16. Lawton, G.: Web 2.0 Creates Security Challenges. Computer 40(10), 13–16 (2007)
17. Salerno, S., Sanzgiri, A., Upadhyaya, S.: Exploration of Attacks on Current Generation Smartphones. Procedia Computer Science 5(0), 546–553 (2011)
18. Green, A.: Management of security policies for mobile devices. In: Proceedings of the 4th Annual Conference on Information Security Curriculum Development, pp. 1–4 (2007)
19. Yuan, Y., et al.: Identifying the ideal fit between mobile work and mobile work support. Information & Management (2010) (in Press, corrected proof)
20. Mittal, A., Sengupta, A.: Improvised layout of keypad entry system for mobile phones. Computer Standards & Interfaces 31(4), 693–698 (2009)
21. Shih, H.-C., Wang, K.: An adaptive hybrid dynamic power management algorithm for mobile devices. Computer Networks (2011)
22. Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Computers & Security 28(6), 476–490 (2009)
23. Faily, S., Flechais, I.: To boldly go where invention isn't secure: applying security entrepreneurship to secure systems design. In: Proceedings of the 2010 Workshop on New Security Paradigms, pp. 73–84 (2010)
24. Garfinkel, S.L.: Design principles and patterns for computer systems that are simultaneously secure and usable, p. 1. Massachusetts Institute of Technology (2005)
25. Hertzum, M., Clemmensen, T.: How do usability professionals construe usability? International Journal of Human-Computer Studies 70(1), 26–42 (2012)
26. Botha, R.A., Furnell, S.M., Clarke, N.L.: From desktop to mobile: Examining the security experience. Computers & Security 28(3-4), 130–137 (2008)
27. Azer, M.A., El-Kassas, S.M., El-Soudani, M.S.: Security in Ad Hoc Networks: From Vulnerability to Risk Management. In: Proceedings of 2009 Third International Conference on Emerging Security Information, Systems and Technologies, pp. 203–209 (2009)
28. Economides, A.A., Grousopoulou, A.: Students' thoughts about the importance and costs of their mobile devices' features and services. Telematics and Informatics 26(1), 57–84 (2009)
29. Haverila, M.: What do we want specifically from the cell phone? An age related study. Telematics and Informatics (2011) (in Press, corrected proof)
30. Churchill, D., Hedberg, J.: Learning object design considerations for small-screen handheld devices. Computers & Education 50(3), 881–893 (2008)
31. McGibbon, T., et al.: Use of Mobile Technology for Information Collection and Dissemination (2011)