

# A Perception Oriented Approach for Usable and Secure Interface Development

Mehmet Göktürk and İbrahim Şişaneci

Gebze Institute of Technology, Gebze, Kocaeli, Turkey  
{Gokturk, sisaneci}@gyte.edu.tr

**Abstract.** Developers generally try to make their systems secure by adding Information Security measures and components to User Interfaces. While applying these measures, usability of interfaces may decrease seriously. Developing secure and usable user interfaces became a necessity due to the fact that security and usability are both indispensable for users. To develop secure and usable interfaces, first, users' perception of information security is analyzed. In this study, An Enhanced Users' Perception of Information Security Model (EU-PoIM) and Perception Oriented Usable & Secure Interface Development Model (POSUIDM) are proposed to empower developers in developing both secure and usable user interfaces.

**Keywords:** Enterprise UX structure and process, security perception, usable security, perception oriented approach.

## 1 Introduction

With the rapid developments in Information Technology, more complicated information security threats occur in every part of digital life. Many computers and digital devices are exposed to these threats via their interfaces. In order to cope with these, developers generally try to make their systems secure by adding Information Security (InfoSec) measures and components to User Interfaces (UI). As these measures are applied, usability of interfaces may decrease seriously. Developing secure and usable user interfaces became a necessity due to the fact that security and usability are both indispensable requirements for users. To develop secure and usable interfaces, first, users' perception of InfoSec (PoI) must be analyzed. Then, constructing a users' perception model according to the analysis is necessary.

The organization of this paper is as follows. In Section 2, usability and security related work is reviewed briefly. Next, methodology is presented in Section 3. In Section 4, Perception Oriented Approach and motivation of the approach are explained. Moreover, an Enhanced Users' Perception of Information Security Model (EUPoIM) is described with relation among features of user interface design, usability principles and EUPoIM. Next, in Section 5, Perception Oriented Usable & Secure Interface Development Model (POSUIDM) is proposed to empower developers in developing both secure and usable user interfaces. Finally, the conclusions and future work are presented in Section 6.

## 2 Literature Review

Usable and Secure Interface Development is an interdisciplinary issue that is closely related with human computer interaction (HCI), information security (InfoSec) and psychology disciplines. Research related this topic can be grouped into three categories such as Usability & Security, Privacy & Security and Perception of information security.

Computers are essential for people, yet most users have a tendency to use easy one regardless of its security. Unfortunately, unsecured systems aren't usable for long due to possible security compromises. Most studies agree that it's necessary to design both secure and usable systems, but there is less agreement about how to reach this goal [1-4].

A balance must be established between these two needs. To provide a balance, a systematic usability analysis and taxonomy are revealed under the main titles of "human factors in information security" and "user resistance against the information security measures" by Schultz in 2001[5].

Two methods have been developed; applying usability to secure systems and applying security to usable systems. However, since both methods do not reach the goal, user-centric security and usability approach has been used by Zurko's rule based user-centric authentication engine, by Fidas's password management and "human in the loop" framework [6-9].

From the perspective of privacy & security studies, an excessive amount of anonymity on the web and in particular the increase in the information sharing issue comes many privacy problems together. Many studies are emphasized why studies on privacy and security is critical today [10, 11].

From the perspective of perception of information security, Huang's study in 2010, one of the important studies on perception of information security, stated that understanding of the people's perception of information security may be possible with revealing how individuals perceive different threats and which factors affect them. In Huang's study, threat based perception of information security can be expressed under the main factors such as knowledge, impact, severity, controllability, possibility and awareness. Computer experience of users also affects their perception significantly where users with more experience concern less security issues. Another output of their work is that users' understandings of type of loss are very different [12].

In addition to above, an interesting e-commerce study proposed design elements that might positively affect user' perception of information security and tested on e-commerce web application [13, 14].

## 3 Methodology

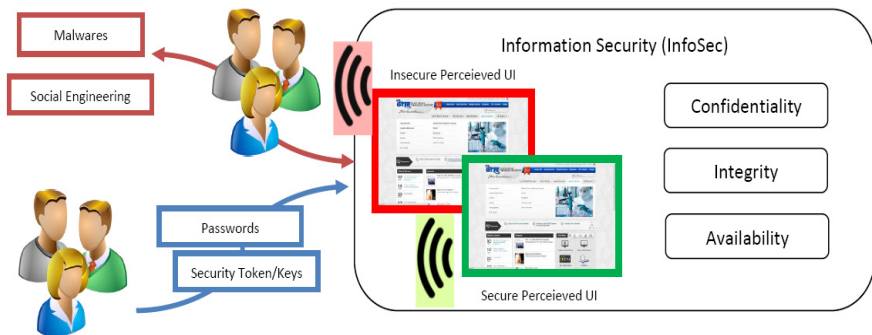
Usability and Security, both of which are not functional requirements for many applications, cannot be measured directly. As information security can be measured by risk

assessment, Usability can be evaluated by usability testing, cognitive walkthrough, heuristic evaluation, paper prototyping and empirical methods such as surveys.

The validity of proposed models, derived from literature research, is tested with usability tests/experiments and surveys in a case study through preparing sample user interfaces as future work.

## 4 Perception Oriented Approach

Perception is defined as “a major part of human intelligence and a key component in understanding human behavior” [15]. In other words, it is the mechanism with which a person evaluates external inputs, which, in turn, determines the behavioral response. As many human oriented efforts, perception, a key component of human behavior, should be effectively directed [16]. Perception of information security must be taken into account by developers in order to be successful when security & usability components to user interface are applied. Otherwise, these efforts could be ignored by user. Users can be the weakest link in information security chain or a victim of cyber threats. Moreover, they also give up using the system easily. The relationship among users, user interfaces and information security is depicted in the Figure 1. Users' perception varies according to threats and countermeasures on user interfaces. Accordingly, a user interface is evaluated as "secure perceived interface" or "insecure perceived interface" by users usually [17].



**Fig. 1.** Users, Threats, Countermeasures, User Interfaces and Information Security Relationship Diagram

### 4.1 Motivation and Axioms

With guidance of research questions listed below, sample axioms in Table 1 were derived and put forward to evaluate the relationship between user interfaces and perception of information security [18-23].

- How computer users' perception of InfoSec is formed? Which factors affect this perception?
- How will users react as a result of this perception?
- Which design elements/components are related to this perception model and what extent?
- Which factors are supported and what features are included by interfaces?

**Table 1.** Sample Axioms

<b>Axioms</b>
Education, culture and ownership factors affect the perception of information security.
Interfaces with full of security components or security elements come to the fore has low usability.
I/O components used in the UI and the status of them whether are usable by mouse/keyboard influences the perception of information security.
Color usage in interfaces affects the perception of information security
Metaphor usage in interfaces affects the perception of information security
Whether user interface components are text-based or graphics-based, affects the perception of InfoSec
Perception of information security can be expressed under the main factors such as knowledge, impact, severity, controllability, possibility and awareness.
Factors of users' computer experience and possible type of loss affects the perception of InfoSec
The language and tone of the language used in user interfaces influences the perception of InfoSec
Whether there is a privacy notification in the interface, perception of information security.

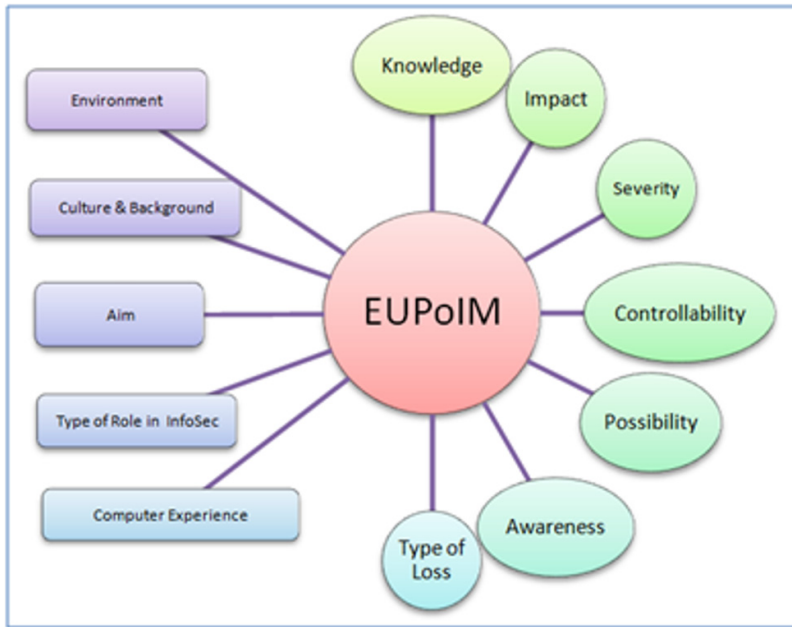
Generally, perception of information security has three primary dimensions: background, look & feel and organizational driven perception. Many factors of these dimensions such as education, culture, ownership, knowledge, impact, severity, controllability, possibility, awareness, users' computer experience and possible type of loss affect the perception of information security. [24-26]

In UI side, mostly related with look & feel dimension, UI features (color, metaphor, I/O components, security components, language & tone of the language) of interfaces and text-based or graphics-based design have particular influence on the perception of information security [27].

Perception of information security can change depending on the environment (individual/institutional usage, as a duty or as a hobby) type of role in InfoSec (end user, system administrator, expert user) [28].

#### **4.2 Enhanced Users' Perception of InfoSec Model (EUPoIM)**

Enhanced Users' Perception of InfoSec Model (EUPoIM) has been constructed by integrating threat based perception of information security factors with the additional factors expressing the case of "human as an actor in the information security".



**Fig. 2.** Enhanced Users' Perception of Information Security Model

These additional factors derived from environment of usage, the role in information security and sample user behaviors such as violating InfoSec rules and operating incorrect actions. For example, many people can respond very diversely to InfoSec notification in the private usage and business environments. In other words, the EU-PoIM deals with both the threat based perception of information security and counter measure based perception of information security.

Relationship among features of user interface design, usability principles and EU-PoIM is shown in Table 2 in short [29-31].

The main factors of usability are learnability<sup>1</sup>, utility<sup>2</sup>, efficiency<sup>3</sup>, memorability<sup>4</sup>, error management<sup>5</sup> and satisfaction<sup>6</sup>.

<sup>1</sup> The ability of the user to discover and understand product capabilities and how to use them.

<sup>2</sup> The completeness and appropriateness of the product in achieving end-user goals.

<sup>3</sup> The ease of use of the product in helping end-users to accomplish their critical tasks.

<sup>4</sup> The extent to which a casual user can remember how a product works and retain proficiency with it.

<sup>5</sup> The degree to which users enjoy using and interacting with the product.

<sup>6</sup> How errors are prevented, recovered from, and managed to minimize loss and user frustration.

**Table 2.** Relation among features of UI design, usability principles and EUPoIM

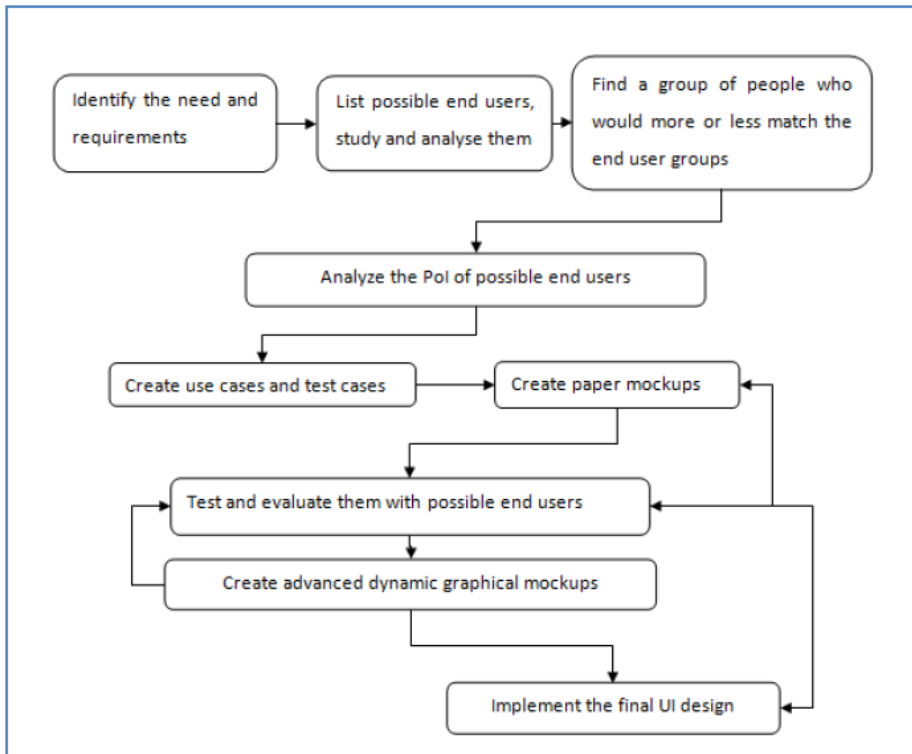
Components/Features	Usability Factor	EUPoIM <sup>7</sup>	Explanation
Professional looking overall design	Satisfaction	(AW)(E)(A)	Provides higher usability and security
Text-based or graphics-based UI	Efficiency, Satisfaction	(K)(AW)(E)(CE)(R)(C) (P)(A)	Depends computer experiences and environments.
Self learning features	Learnability, Satisfaction	(K)(AW)(E)(CE)(C)(R)	Provides higher usability but lower security
Language & tone of the language	Satisfaction	(K)(P)(C)(AW)	Provides high usability but low security
Sense of being limited	Satisfaction	(C)(E)	Provides lower usability and security
Availability or State Information Feedback	Satisfaction, Utility	(K)(S)(P)(AW)	Provides higher usability and security
Fast operation completion	Efficiency	(C)(L)(E)(R)	Provides higher usability and lower security
Full of security components or security elements come to fore	Satisfaction, Utility	(K)(I)(S)(C)	Provides lower usability but higher security
Using privacy notification	Error management, Satisfaction	(K)(S)(C)(P)(AW)(L)	Provides lower usability but higher security
Correct Alert	Error management,	(S)(I)(L)(P)(AW)	Provides higher usability and security
Detailed Error Message	Error management	(S)(I)(P)(AW)	Provides higher usability but lower security
Color usage	Memorability, Error management	(K)(AW)(S)(P)(A)	Several different and proper color usage provides higher usability and security. Many and in consistent color usage provides lower usability and security.
Using Metaphors	Learnability, Predictability, Memorability, Satisfaction	(K)(AW)(P)(A)	Provides higher usability but lower security
Using Step by Step Wizard	Efficiency, Memorability, Satisfaction	(K)(C)(AW)	Provides higher usability and security
Using Tabbed Panels	Efficiency, Memorability, Satisfaction	(K)(C)(AW)(A)	Provides higher usability and security
Using Confirmation Dialog	Satisfaction, Error management	(I)(S)(C)(P)(AW)	Provides lower usability but higher security
Using Graphical Password	Memorability, Satisfaction	(C)(AW)(A)	Provides lower usability but higher security
Using virtual keyboard	Memorability, Utility	(C)(AW)(E)	Provides lower usability but higher security
Using components which are able to hide input value	Satisfaction	(S)(C)(AW)(L)(E)	Provides lower usability but higher security
Using components which deactivates keyboard shortcuts or can be controllable by keyboard/mouse	Efficiency, Utility, Memorability	(C)(E)(R)	Provides lower usability but higher security
Using components which are able auto complete/recommend possible values	Learnability, Efficiency	(K)(P)(AW)(E)	Provides higher usability and security

## 5 Perception Oriented Usable and Secure Interface Development Model (POSUIDM)

Perception Oriented Usable & Secure Interface Development Model (POSUIDM) is based on user-centric security and usability approach (in Figure 3). It starts with identification the need and requirements. First, the aim of UI should be specified and the idea of the product and design requirements should be studied. Then, following stages are listing possible end users and finding a group of sample end users. Then, analyzing the

<sup>7</sup> (C) Controllability, (K) Knowledge, (S) Severity, (I) Impact, (P) Possibility, (A) Aim, (AW) Awareness, (E) Environment, (L) Type of Loss, (R) Type of Role, (CE) Computer Experiences.

perception of information security of possible end users is the most important stage in POUIDM. In this stage, background driven, look & feel driven and organizational perceptions of possible end users must be extracted with the help of EUPoIM.



**Fig. 3.** Perception Oriented Usable & Secure Interface Development Model (POSUIDM)

POUIDM flow continues with creating use cases and test cases including usability test and perception of information security analysis and paper mockups dealing with the result of the perception of information security analysis. Next, testing and evaluation which includes the usability test and perception of information security analysis reviews besides functionality tests and creating advanced dynamic graphical mockups are iterative stages which provide good feedbacks to previous stages. Finally, implementation is performed based on the Usable & Secure perceived UI design.

## 6 Discussion/Conclusion

It is apparent that perception in look & feel dimension can only be manipulated by UI developers. To vary other dimensions, additional efforts (awareness, education etc.) must be spent by different actors other than UI developers such as back end developers. In general, UI side mainly deals with look & feel driven perception of perception of

information security. In this study, relationship among features of UI design, usability principles and EUPoIM are demonstrated concisely. It is evident that perception oriented security is an interesting parameter to focus and consists of multiple dimensions. Furthermore, Enhanced Users' Perception of InfoSec Model and Perception Oriented Usable & Secure Interface Development Model are proposed for the development of both secure and usable interfaces. It is also emphasized that user-centric usable security and users' perception of information security are fertile research areas.

## References

1. Cranor, L.F.: Security and Usability: Designing Secure Systems That People can Use. O'reilly (2007)
2. Möckel, C.: Usability and Security in EU E-Banking Systems Towards an Integrated Evaluation Framework. In: IEEE/IPSJ International Symposium on Applications and the Internet (2011)
3. Yeratziotis, A., Pottas, D., Van Greunen, D.: A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm. *International Journal of Human-Computer Interaction* 28(10), 678–694
4. Kainda, R., Flechais, I., Roscoe, A.W.: Security and Usability: Analysis and Evaluation. In: International Conference on ARES 2010, pp. 275–282 (2010)
5. Schultz, E.E., Proctor, R.W., Lien, M.-C., Salvendy, G.: Usability and Security An Appraisal of Usability Issues in Information Security Methods. *Computers & Security* 20(7), 620–634 (2001)
6. Zurko, M.E., Simon, R.T.: User-centered security. In: Proceedings of the 1996 Workshop on New Security Paradigms, pp. 27–33. ACM (September 1996)
7. Fidas, C.A., Voyiatzis, A.G., Avouris, N.M.: When security meets usability: A user-centric approach on a crossroads priority problem. In: 2010 14th Panhellenic Conference on Informatics (PCI), pp. 112–117. IEEE (September 2010)
8. Cranor, L.F.: A Framework for Reasoning About the Human in the Loop. In: UPSEC 2008 Proceedings of the 1st Conference on Usability, Psychology, and Security, vol. 8, pp. 1–15 (2008)
9. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. *Computers & Security* 24(2), 124–133 (2005)
10. Flinn, S., Lumsden, J.: User perceptions of privacy and security on the web. In: *Privacy Security and Trust* (2005)
11. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measuring User Confidence in Smartphone Security and Privacy. In: Symposium on Usable Privacy and Security (SOUPS), Washington, DC, USA, July 11-13 (2012)
12. Huang, D.L., Rau, P.L.P., Salvendy, G.: Perception of Information Security. *Behaviour & Information Technology* 29(3), 221–232 (2010)
13. Kamoun, F., Halaweh, M.: User Interface Design and E-Commerce Security Perception: An Empirical Study. *International Journal of E-Business Research* 8(2), 15 (2012)
14. Chanko, E.: Factors that influence users' perceptions of trust in e-commerce. School of Humanities and Informatics, University of Skövde, SWEDEN, M.Sc. dissertation in Computer Science (2004)
15. Salvendy, G.: *Handbook of Human Factors and Ergonomics*. Wiley-Interscience, New York (1997)



16. Cooper, D.: Psychology, Risk & Safety: Understanding How Personality & Perception can Influence Risk Taking. *Professional Safety* 48, 39–46 (2003)
17. Parsons, K., McCormac, A., Butavicius, M., Ferguson, L.: *Human Factors and Information Security: Individual, Culture and Security Environment*. Australian Government, Department of Defence, Defence Science and Technology Organization, Command, Control, Communications and Intelligence Division (2010)
18. Arteaga, J.M., González, R.M., Martín, M.V., Vanderdonck, J., Álvarez-Rodríguez, F.: A Methodology For Designing Information Security Feedback Based On User Interface Patterns. *Advances in Engineering Software* 40, 1231–1241 (2009)
19. Fléchais, I.: *Designing Secure and Usable Systems*. PhD Thesis, University College London Department of Computer Science (February 2005)
20. Kuo, H.M., Chen, C.W.: Study Of Merchandise Information And Interface Design On B2C Websites. *Journal of Marine Science and Technology* 19(1), 15–25 (2011)
21. Liu, Y., Huang, D., Zhu, H., Rau, P.L.P.: Users' Perception of Mobile Information Security. In: 2011 International Conference for Internet Technology and Secured Transactions (ICITST), December 11-14, pp. 428–435 (2011)
22. Kim, C., Tao, W., Shin, N., Kim, K.: An Empirical Study of Customers' Perceptions of Security and Trust in E-Payment Systems. *Electronic Commerce Research and Applications* 9(1), 84–95 (2010); Special Issue: Social Networks and Web 2.0
23. Morris, M.G., Dillon, A.: How User Perceptions Influence Software Use. *IEEE Software* 14(4), 58–65 (1997)
24. Faily, S.: *A Framework for Usable and Secure System Design*. In: PhD Thesis, University of Oxford Wolfson College (2011)
25. González, R.M., Muñoz-Arteaga, J., Martín, M.V., Álvarez-Rodríguez, F., Calleros, J.G.: A Pattern Methodology to Specify Usable Security in Websites. In: IEEE 20th International Workshop on Database and Expert Systems Application (2009)
26. Cyr, D., Bonanni, C., Bowes, J., Ilsever, J.: Beyond Trust: Website Design Preferences Across Cultures. *Journal of Global Information Management* (January 2005)
27. Chiasson, S., Forget, A., Biddle, R., van Oorschot, P.C.: User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords. *Int. J. Inf. Secur.* 8, 387–398 (2009)
28. Egger, F.N.: Affective Design of E-Commerce User Interfaces: How to Maximize Perceived Trustworthiness. In: *Proceedings of the International Conference on Affective Human Factors Design*, London (2001)
29. Chang, H.H., Chen, S.W.: Consumer perception of interface quality, security, and loyalty in electronic commerce. *Information & Management* 46, 411–417 (2009)
30. Radke, K., Boyd, C., Brereton, M., Nieto, J.G.: How HCI Design Influences Web Security Decisions. In: *OZCHI 2010*, Brisbane, Australia, November 22-26 (2010)
31. Fogg, B.J., Soohoo, C., Danielson, D.: *How Do People Evaluate a Web Sites Credibility?* Report. Persuasive Technology Lab Stanford University (2002)