Securing User eXperience: A Review for the End-Users' Software Robustness

Panagiotis Zagouras and Christos Kalloniatis(✉) [iD]

Privacy Engineering and Social Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, 81100 Mytilene, Lesvos Island, Greece
{ctd16015,chkallon}@aegean.gr

Abstract. Millions of users all over the world nowadays spend many hours daily using social networks on a range of devices (desktop, tablet, mobile), in many languages and countries, under very different systems of governance, and in wide-ranging social, religious, cultural and political environments. But the same software (System Services, Operating Systems "OSes", Hypervisors, Applications and Utilities) is still called upon to function in contexts defined by these vast differences in terms of quality, reliability, efficiency and security. All domestic appliances, contemporary cars and almost everything powered by electricity is now equipped with at least a rudimentary interface and ready-to-run software. Electronic transactions are now routine and there is a huge need for online security and privacy. Bring your own device (BYOD) is a trend that is appearing even in SMBs (Small and Midsize Business) with aspects, policy considerations, security models and traps. The success off all the above depends on User eXperience where the user intersects with the product (software). In this paper, we analyse the different approaches taken under the concept of User eXperience (UX) in tandem with the development of contemporary software, and examine their ramifications for the level of security and privacy. We will show that UX is a different concept from usability, examine the different academic approaches and their underlying viewpoints, and show how the tasks in question relate to security. We believe that the interface between UX and security is a demanding area which requires research in multiple dimensions. The need for designing and developing contemporary software which is smart, user-friendly, adaptive, secure and capable of protecting every type of user is immense.

Keywords: User eXperience · Usability · Security

1 Introduction

It is absolutely obvious that the concept of computing today has changed completely. Technology is ubiquitous in industrialized countries (Weiser 2002). Everyday procedures are not conducted as they once were and computers no longer interface with humans — "they interact" (Cooper 2012). "Smart shoes, appliances and phones are already here, but the practice of User eXperience (UX) design for ubiquitous computing is still

relatively new" (Kuniavsky and Founder 2010). Mobile communications are probably the fastest-evolving area within the ubiquitous computing sector (Hartson and Andre 2001) and are one of the areas featuring the most intense work on designing a quality User eXperience (UX). UX is an entire scientific field with extensions 'Beyond Usability' (Zimmermann and Eth 2012) while additionally different purposes for the usability and User eXperience (UX) evaluation methods (Bevan 2009) are introduced continuously. Various standards introduce different concepts for user experience like ISO 9241-11 which includes the concepts of effectiveness, efficiency, satisfaction, and content of use, while ISO 13407 provides guidance on designing usability with reference to ISO 9241-11. While the aforementioned efforts provide a sufficient map of concepts for dealing with user experience during system development security is still not clearly related with the specific concept during the development process (Jokela et al. 2003). While it is clear that usability differs from user experience the relationship with security and their interrelation is not sufficiently addressed.

In our modern and networked society people provide personal information in various online services over insecure networks and without having a satisfactory degree of awareness in using these services in a secure way. One of the major issues related to security is the way that these services alert and interact with the user and the degree of user's experience in dealing with these issues accordingly. Considering the fact that new GDPR legislation demands a higher degree of interaction with Internet users for various types of approvals/consents developing methods and tools that consider user experience as an important aspect of enhancing system's security and user's protection is immense.

The terms "look" and "feel" while using a modern and secure software, are now more than ever very important. In every daily interaction (work applications, finance transactions, social media responses) it's already reasonable and acceptable that "End Users play a critical role in computer security" (Minge & Thüring 2018) and we must research about the "interplay between usability and visual aesthetics" and focus seriously in "halo effects". Further difficulties also present themselves when we try to create 'relationships' between the UX and Security. There is now a pressing need to develop frameworks and methodologies capable of combining more specialized UX extensions with cutting-edge technologies for designing, developing, installing and monitoring secure IT systems. The new software that results will have to be user-friendly while combining ease of use with results in terms of security and privacy in whatever natural environment the device interacts with.

Given the aforementioned concerns the specific paper examines the role of security in connection with User eXperience. More specifically, it presents a review of all existing frameworks dealing with user experience along with their basic characteristics. Additionally, every framework is examined regarding its security extensions. Finally, the basic UX characteristics of these frameworks are examined and matched with the three basic security principles (Confidentiality, Integrity and Availability) in order to identify how every UX characteristic impacts security.

More specifically the paper is structured as follows. In Sect. 2 the relationship between security and user experience is presented. In Sect. 3 a review of the current User experience frameworks is presented along with the presentation of their characteristics and their relationship with basic security principles. Finally Sect. 4 concludes the

paper by providing discussion on the studied works and raises issues for future research on the respective field.

2 User eXperience (UX) and Security

Recent years have witnessed vast changes in the field of design encompassing product design, semantics and emotional response in line with social change, the conservation of resources and energy, emerging environmental problems, and customer-oriented trends.

Products have a range of technical, practical and semantic functions. Monö in (Demirbilek & Sener 2003) defines four semantic functions for products. By allowing the designer to communicate 'cleanly' with the system, these functions create the conditions that govern what can and cannot be achieved in terms of communication with the product. The proposed semantic functions are: (a) *To Describing*: The product gestalt describes facts (e.g. its purpose is to define the task), mode of use, handling. (b) *To Expressing*: The product gestalt expresses the product's values and qualities. (c) *To Signalling*: The product gestalt urges the user to react in a specific way—for example, to be careful and precise in his/her work. (d) *To Identifying*: The product gestalt identifies the origin, nature and area of the product, its connection to the system, family, product range etc., and the function and placement of individual parts. The specific semantic functions thus seem to define the desired boundaries of the product in every situation in which it interacts with the user. The above approach is more technocratic and understandable to designers with IT knowledge.

Another approach which focuses more on the user, proposes a model of software design based on emotional flow (Demirbilek & Sener 2003). Authors believe that the emotional response or reaction to meaning triggered by a product varies between people from different backgrounds, social classes, levels of education, religion etc. The same authors have identified six different types of affective programs which involve 'happy' feelings, joy, or the evocation of dreams. The different types are: senses, fun, cuteness, familiarity, metonymy and colour. The above factors allow the user to use the software correctly and for the purpose for which it was designed for. Mistakes made while using the software can have irreparable consequences. Social structures (which have a direct bearing on human life), military installations and every simple, everyday item must be secure and 'respectful' of the human aspect of their use.

The beginning of security analysis in IT environments was set by using formal methods and the basis of those methods were discrete maths and logic. The progress took place by introducing business dynamics methodology (Sterman 2000) and the socio—technical systems. However, during the last years, security research and analysis has been orientated towards human behaviour. Nowadays, Information Security lies in various and different aspects and fields like: Philosophical, Behavioural, Technical, Managerial. It deals with prevention and detection of intrusions, as well as more specific fields of today, such as socio philosophical fields and socio organizational fields (Zagouras et al. 2017).

We appreciate that the field of User eXperience (UX) has not been recently researched in combination with the development cycle for contemporary, secure software while similar efforts from the field of Usability Engineering and HCI have addressed similar issues (Kainda et al. 2010; Yee 2004). There is thus a need to create methodologies

and tools which will provide assistance to software engineers involved in the modern software industry.

This paper will bring together research projects which have taken a wide range of different approaches to the subject-matter, creating a reference point of our own which we believe warrants thorough exploration through the combination of different research approaches. The extensions of User eXperience (UX) in our contemporary software-dominated reality are vast and bring together different fields which may not have been associated before. Below, we will present research conducted in the field in question, looking at how the different strands can be combined and parameterized, and anything else that might be of service to the software creation industry.

3   Related Works

We now know that the concept of User eXperience (UX) is a different field of research from usability and contains issues that go beyond satisfaction. It is a highly demanding field, because it involves a set of entirely different and complex factors (parameters) and combines methodologies and fields which have not been applied together in this context. A target approach for UX mentions exemplary: "UX is not only about the times when people are using our products, but also about the times when they are not. In the era of ever-vibrating smartphones and increasingly demanding apps, there is no better user experience than peace of mind"[1].

Our research focused on the search for User eXperience frameworks while also exploring their security extensions. In relation to UX Frameworks in general, Blythe (Law et al. 2007) proposed five bipolar dimensions to characterize UX frameworks as shown in Table 1. These dimensions were used for comparing the UX frameworks as shown below.

Table 1. Dimensions to characterize UX Frameworks.

Aspect	Content Dimension
Theory	Reductive—Holistic
Purpose	Evaluation—Development
Method	Quantitative—Qualitative
Domain	Work Based –Leisure based
Application	Personal—Social

A review paper from (Zarour and Alharbi 2017) explains each element of the UX in detail. Specifically, the article compares the frameworks that have been created for UX, parametrized them with its own approach before ultimately presenting the authors' preferred framework.

---

[1] https://uxdesign.cc/designing-for-less-98d64259f770.

The framework in question categorizes UX disciplines, dimensions, aspects, categories and descriptions, illustrates the dimensions, presents the different measurement methods for UX, illustrates them with dimensions, and analyzes one by one the various proposed UX Frameworks currently dealt with in the literature. At the end, it outlines a proposed framework for UX which includes dimensions, aspects categories and measurement methods. Specifically the suggested UX dimensions are: (a) *Value*: This is related to the studies that have been focused on the gained value. (b) *User Needs Experience (NX)*: This is related to the studies that have been focused on user needs and gained qualities. (c) *Brand Experience (BX)*: This is related to the studies that have focused on the organization's brand image. (d) *Technology Experience (TX)*: This is related to the studies that have focused on the technology that has been used to deliver the product or the service. (e) *Context*: This is related to the studies that have focused on the context of use and the interaction between the previous dimensions.

The identified UX frameworks are shown in Table 2. Specifically Mahlke (Sascha & Aus Berlin 2008) presents in detail for UX the influencing factors, the instrumental and no instrumental quality perceptions, the emotional user reactions and the consequences of UX. (Vyas et al. 2012) "deals" with the affordances in interaction. It proposes two broad classes of affordances: Affordance in information and affordance in articulation and the notion of affordance should be treated at two levels: at the 'artefact level' and at the 'practice level'. The third framework proposed by Jetter and Gerken (2007) basic concepts are the 'product', the 'user' and the 'organization' and emphasizes in traditional Human – Computer Interaction that is different with the Extended Human – Computer Interaction. Authors in (Möller et al. 2009) taxonomies the quality of service and quality of experience that they carry following a multimodal human-machine interaction. Katrin Schulze and Heidi Krömker in (Schulze & Krömker 2010) saw that the motivation – emotion – reflection are basic components for the UX by mentioning basic human needs and product qualities. In (Chen & Zhu, 2011) authors put forward four dimensional assessment system of mobile application user eXperience: User characteristic, app properties, app system supports and context parameters. Gegner et al. in (2012) discuss the managing of UX components between value – benefit- attribute following the Means End theory. In (Fuchsberger et al. 2012) authors consider the Values In Action (ViA). The approach ViA consider Usability (U), User eXperience (UX) and User Acceptance (UA) a priori as equally important. In (Gross & Bongartz 2012) authors make an experiment with three different mobile applications and present a regression analysis with important results. In (Pc & Prabhu 2012) authors focus on requirements engineering (RE) and user experience design (UXD) and how these values effect the entire scientific field (UX). Tan et al. (2013) taxonomies usability and UX attributes using a well – known Goal Question Metric (GQM) approach. Gao et al. (2013) construct an evaluation index system of user experience and a user experience quality evaluation. In (Kujala et al. 2012) authors proposed quality dimensions that are related to no-instrumental qualities. Kremer et al. (2017) present the ExodUX approach about the application methodologies, the factor representation sheets (FRS) and the general process documentation (GPD). Finally, in (Zarour and Alharbi 2017) authors present a retrospective user experience evaluation method called "UX Curve" revealing long—term aspects of user experience.

In Table 2 the aforementioned frameworks along with their basic characteristics and a brief description are shown.

Table 2. UX Frameworks published on the research community.

Authors of the Framework	Basic UX Components	Small Description
Mahlke	Perception of instrumental qualities, emotional user reactions and perception of non-instrumental qualities	"Non-instrumental quality perceptions and emotional user reactions are considered as distinct aspects of user experience and complement the perception of instrumental quality"
Vyas and van der Veer	Affordance in Information and affordance in Articulation	Affordance in information refers to users' understanding of a technology based on their semantic and syntactic interpretation; and affordance in articulation refers to users' interpretations about the use of the technology
Hans-Christian Jetter and Jens Gerken	User, product, organization	The traditional or extended human—computer interactions have different user and organizational values
Sebastian Möller et al.	Quality of Service (QoS) and Quality of Experience (QoE)	"The taxonomy consists of three layers, two of them addressing QoS and one addressing QoE". (1) QOS-INFLUENCING FACTORS, (2) QOS INTERACTION PERFORMANCE ASPECTS, (3) QOE ASPECTS
Katrin Schulze and Heidi Krömker	Basic human needs, Product qualities, Motivation, Emotion, Reflection	The specific approach defined UX as "the degree of positive or negative emotions that can be experienced by a specific user in a specific context during and after product use and that motivates for further usage"
Zhi Chen and Shangshang Zhu	User characteristics, App properties, App system supports and context parameters	The specific approach "study mobile application User eXperience (UX) and quantitative assessment through Analytic Hierarchy Process"

<div align="right">(continued)</div>

Table 2. (*continued*)

Authors of the Framework	Basic UX Components	Small Description
Lutz Gegner et al.	Strategy—ladder, Studio—ladder, Life—ladder, Value, Benefits (Consequences), Attribute	The framework follows the Means-End Theory proposed by Gutman and the elements of the framework have links between them in order Value — > Benefits — > Attribute
Verena Fuchsberger et al.	Usability (U), User Experience (UX), User Acceptance (UA)	The values: Interpersonal, Emotional, Social, Functional, Conditional, Epistemic encapsulates the ViA (Values in Action) Usability, UX and UA
Alice Gross and Sara Bongartz	Aesthetics, Fun, SUS (System Usability Scale), SAM (SELF-ASSESSMENT MANIKIN), Overall judgment	This approach consists of an experiment with three different mobile applications with a specific device and specific operating system. The Regression analysis of UX components have bring important results
Anitha PC and Beena Prabhu	Requirements engineering (RE) and user experience design (UXD)	The framework has "several synchronization points where RE and UXD professionals should collaborate"
Jia Tan et al.	A taxonomy for usability and UX attributes and generic questions and measures for developing measurements instruments	The framework evaluation have done in a small telecom company and the results can lead better decisions to improve the usability and the UX of the mobile industry products
Gao Changyuan et al.	Instinct reflection layer, interaction layer, depth perception layer	This approach "constructs the evaluation index system of user experience and also does the user experience's quality evaluation"
Sari Kujala et al.	Hedonic product quality. Quality dimensions that are related to no-instrumental qualities such us aesthetics, innovativeness and originality	The retrospective user experience evaluation method "UX Curve" is a "promising method to reveal long—term aspects of user experience"

Table 2. (*continued*)

Authors of the Framework	Basic UX Components	Small Description
Simon Kremer et al.	Setting, aesthetics, interaction, cognitive processes, technology	The application methodologies, the factor representation sheets (FRS) and the general process documentation (GPD) create a three—part framework to improve the flows of the proposed framework
Mohammad Zarour and Mubarak Alharbi	UX Dimensions, aspects categories, aspect, measurements methods	This framework proposes the relation between value and UX Dimension :Value, user need experience (NX), brand experience (BX), technology experience (TX)

Studying in detail the aforementioned frameworks, we have focused on the information analysis that reports security extensions. We can see that an approach reports security references in system factors and context factors. Other approaches focus on security references when it comes to basic human needs and psychological needs. More technical approaches report: security features or attributes like safety etc. Table 3 below presents more clear a list of the referenced UX frameworks proposed in literature in association with security and privacy issues they propose.

Table 3 shows that the 'connection' between UX και Security is "weak" and there is a gap between presentation and studying. Specifically the UX field needs to be linked with all the security extensions provided by contemporary software. None of the proposed frameworks comes with a detailed presentation and exploration of the available security. Recent bibliography has resulted in 3 basic areas based on (Mishra & Harris 2006) for creating secure information systems: technical, formal and informal systems. However, the term "Information Systems" has gotten different connotations from different researchers.

Various and varied studies and approaches have been developed on the basis of theories and frameworks from other academic fields to explore contingent factors of the end user's security behaviours. As stated in (Hu et al. 2011) "The rational decision-making process will be subject to a variety of individual and situational factors". We must focus to "those information security misbehaviours that are intentionally performed by insiders without malicious intent" state the authors in (Dang-Pham et al. 2017).

For better understanding how the aforementioned UX frameworks are related with the basic security principles in order to safeguard the basic security principles (C.I.A) we have initially identifies all UX characteristics presented in all fifteen frameworks and matched then with the respective security principles. More specifically we created a group of categories which include the specific attributes (from all the frameworks) in accordance with the approach taken by (Arhippainen & Tähti 2003). We then categorized the components for the UX: user, social factors, culture factors, context of use, product

Table 3. UX Frameworks in association with security and privacy issues.

	UX Framework	Security (References–Components)
1.	Mahlke	**–**
2.	Vyas and Van Der Veer	–
3.	Jetter and Gerken	–
4.	Moller et al.	System factors (security- critical systems), Context factors (privacy and security issues)
5.	Schulze and Krömker	Basic human needs: security. Feel secure, feel not being watched, build trust, hand over responsibility, have data control
6.	Chen and Zhu	–
7.	Gegner et al.	The life ladder: UX is primarily a result of the satisfaction of psychological needs such as security (calmness, order, routines, relaxation)
8.	Fuchsberger, Moser, and Tscheligi	–
9.	Gross and Bongartz	–
10.	Anitha and Prabhu	Myth2#: RE and UXD Can be Done by Architects or Domain Professionals: "Architect came up with an excellent security feature…" Myth4#: User Experience = Usability: Visceral processing help users make rapid decisions about what is good, bad, safe, or dangerous
11.	Tan, Ronkko and Gencel	Taxonomy for Usability and UX Attributes Attributes Safety. Sub—attributes Security
12.	GAO Changyuan et al.	Rational judgment: Security Depth perception layer: Safety of operation
13.	Kujala et al.	–
14.	Kremer et al.	–
15.	Zarour and Alharbi	UX Aspects: Trustworthiness, privacy

(system in our approach) in line with the UX aspects proposed by (Hiltunen et al. 2002) which are user, task space, physical context, social context, technological context, device and connection.

It should be noted that the tables below have been compiled in line with a user-oriented approach to each attribute. Our research sought to analyze the security approaches from the user's point of view. Thus, the tables list all the attributes taking a consistently user-oriented approach (Tables 4, 5 and 6).

For the user (U) we can see that attributes Confidentiality (C) and Integrity (I) have very strong presentation compared to availability. For the system (S) we can see that the C.I.A. attributes have a huge dissemination in all attributes. It is very important

Table 4. UX attributes User and System in association with security C.I.A. issues

User (U)				System (S)			
Attributes	C	I	A	Attributes	C	I	A
Age	✔	✔		Acceptability	✔	✔	✔
Assessment (every user)	✔	✔		Acceptance	✔	✔	✔
Attention	✔	✔		Accessibility			
Autonomy	✔	✔		Access restrictions	✔	✔	✔
Beautiful of colour, text, graphics				Acoustic	✔		
Behavioural tendencies	✔	✔		Adaptivity	✔	✔	✔
Brand loyalty	✔	✔		Aesthetics	✔		
Choise of alternatives	✔	✔		Ambiguity	✔	✔	✔
Cognitive appraisals	✔	✔		Appeal	✔	✔	
Competencies	✔	✔		Appearance	✔	✔	
Computer anxiety	✔	✔		Appropriation-Enactment	✔	✔	✔
Consistent layout	✔	✔	✔	Attractiveness	✔	✔	
Consumer experience	✔	✔		Authenticity	✔	✔	
Coolness	✔	✔		Balance (Interaction)	✔	✔	✔
Cultural background	✔	✔		Beauty	✔		
Cultural differences	✔	✔		Challenge	✔		✔
Curiosity	✔	✔		Clarity of navigation	✔		✔
Decision	✔	✔	✔	Clear	✔	✔	
Emotional status	✔	✔	✔	Closely (View)	✔	✔	
Emotions	✔	✔		Communicative symbolics	✔	✔	
Enjoyment	✔	✔		Compatibility of users knowledge	✔	✔	
Fun	✔	✔		Completeness	✔	✔	
Gender				Compliance	✔	✔	
Generalizability	✔	✔		Consistency	✔		
General SAM	✔			Content rich	✔		
Haptic quality	✔	✔	✔	Controllable	✔	✔	✔
Hedonic	✔	✔	✔	Convenience	✔	✔	
Image	✔		✔	Correlation of search results	✔	✔	
Influence	✔	✔		Credibility	✔	✔	✔
Instincts	✔	✔		Desirability	✔	✔	
Knowledge	✔	✔		Dialog acts	✔	✔	✔

Table 4. (*continued*)

User (U)				System (S)			
Attributes	C	I	A	Attributes	C	I	A
Learning	✔			Dialogue	✔	✔	✔
Likeability	✔			Ease of use	✔	✔	
Logic between interfaces	✔	✔	✔	Effectiveness			✔
Memories	✔	✔		Effective of link	✔	✔	
Motivation	✔	✔		Emotional value	✔	✔	✔
Motor expressions	✔	✔		Epistemic value	✔	✔	
Native language	✔	✔		Everyday operations	✔	✔	
Needs				Exciting	✔	✔	
Novelty	✔	✔		Extensibility	✔		
Overall judgments	✔	✔		Fault tolerance	✔	✔	✔
Perceptions	✔	✔		Flexibility	✔	✔	✔
Personality	✔	✔		Fluidity	✔		✔
Physiological reactions	✔	✔		Functionality	✔	✔	✔
Pleasure	✔	✔		Functional value	✔	✔	
Popularity	✔	✔		General SUS	✔	✔	✔
Predispositions	✔	✔		Gesture	✔	✔	
Preference	✔	✔		Goals	✔	✔	
Product use	✔	✔		Hedonic quality	✔	✔	✔
Readability	✔	✔		Helpfulness	✔	✔	
Relatedness	✔	✔	✔	Highlight important info	✔	✔	
Relevance	✔			Identification	✔	✔	✔
Safety	✔	✔	✔	Impressive	✔	✔	
Satisfaction	✔	✔	✔	Inter-behavioural	✔	✔	
Security	✔	✔	✔	Interesting	✔	✔	
Sensory (Sensitivity)	✔	✔	✔	Learnability	✔		✔
Sexiness	✔	✔		Memorability	✔	✔	
Skills	✔	✔	✔	Motivational aspects	✔	✔	
Stimulation	✔	✔		Navigability	✔	✔	✔
Simplicity	✔	✔		Operability	✔		
Subjective feelings	✔	✔	✔	Operation	✔		

Table 4. (*continued*)

User (U)				System (S)			
Attributes	C	I	A	Attributes	C	I	A
Surprise	✔	✔		Response time		✔	
Time	✔	✔	✔	Personality system	✔	✔	
Trustworthiness	✔	✔	✔	Platform stability	✔	✔	✔
Uncertainty	✔	✔	✔	Presentation	✔		
Usage behaviour	✔	✔	✔	Productivity	✔		
Usage mode	✔	✔	✔	Reliability	✔	✔	✔
User Performance			✔	Safety of operation	✔	✔	✔
User's knowledge	✔	✔	✔	Speech	✔	✔	
Verbal ability	✔	✔	✔	Supporting	✔	✔	
Visual aesthetics	✔	✔	✔	Symbolic aspects	✔	✔	
				Understandability	✔	✔	
				Usability	✔	✔	
				Useful	✔	✔	
				Utility	✔	✔	
				Visual attraction	✔		
				Vocabulary	✔	✔	

therefore to include these aspects in the system development lifecycle and especially during system design.

Again in Table 5 we see that all attributes belonging to physical Context play a critical role for the security of a system as well as Task Space attributes. It should be noted that Task space is very critical from a user point of view since it is the area were the user interacts with the system and any type of misunderstanding or misbehavior may potentially harm system security or user's privacy.

Finally, in Table 6 we see the same pattern as in the previous tables. In both the technological context and the device attributes all three security aspects have a connection with the UX elements. Except from the retail experience and usage volume all other elements have an impact on systems confidentiality, Integrity and Availability.

The above tables allow us to conclude, first off, that the group consisting of Physical Context (PHC), Task space (TS), Technological Context (TC), and Device (D) includes attributes whose C.I.A. attributes are very close to 100%. This is logical, given that the attributes in this group–the physical context in which the user employs the software, the attributes of the tasks, the technological context and the devices users employ–are all directly linked to the actual system use. There are differences between the user and system groups in terms of their C.I.A. attributes, but we can still see a significant dovetailing of values for the C.I.A. attributes, meaning that the security extensions have

Table 5. UX attributes Physical Context and Task space in association with security C.I.A. issues.

Physical Context (PHC)				Task space (TS)			
Attributes	C	I	A	Attributes	C	I	A
Accuracy	✔	✔	✔	Number of available tasks	✔	✔	✔
Activities	✔	✔	✔	Task consequences	✔	✔	✔
Appropriateness	✔	✔	✔	Task frequency	✔	✔	✔
Availability	✔	✔	✔	Tasks complexity	✔	✔	✔
Conditional value	✔	✔	✔	Time behaviour	✔	✔	✔
Environment (Accuracy)	✔	✔	✔	Type of tasks	✔	✔	✔
Home environment	✔	✔	✔				
Lighting condition	✔	✔	✔				
Mobile environment	✔	✔	✔				
Office environment	✔	✔	✔				
Potential parallel activities	✔	✔	✔				
Precision	✔	✔	✔				
Public usage	✔	✔	✔				
Resulting costs	✔	✔					
Space (condition)	✔	✔	✔				
Transmission channels also sensory	✔	✔	✔				

Table 6. UX attributes technological context and device in association with security C.I.A. issues

Technological Context (TC)				Device (D)			
Attributes	C	I	A	Attributes	C	I	A
Controllability	✔	✔	✔	Brand	✔	✔	✔
Efficacy	✔	✔	✔	Business communications	✔	✔	✔
Efficiency	✔	✔	✔	Marketing	✔	✔	✔
Infrastructure	✔	✔	✔	Retail experience			
Platform technology	✔	✔	✔	Strategy (Brand)	✔	✔	✔
Service response time	✔	✔	✔	Usage volumes			✔

a significant impact on the UX. The extent to which the C.I.A. attributes are influenced by UX components is clear.

From the above we can safely conclude that these approaches provide a huge amount of knowledge and lay the foundations for creating contemporary, smart, adaptive software for every user. However, the problem remains on how to create a secure and user-friendly environment to house every aspect of the average user's everyday experience using smart and adaptive software.

Developments in desktops, tablets, smartphones have been huge in recent years. Millions of users around the world now use smartphone apps for every sort of everyday procedure. Frequently, their functionality "relies on, and produces, sensitive and personal data" (Gerber et al. 2017). All values are stored on the device, including usage data, location and biometrics. There have been numerous instances of unintended live sessions on Instagram and of personal moments being shared live due to software being set up and used incorrectly.

The "privacy paradox" is also frequently observed, following the development of social networks: "The privacy paradox explained as a temporally discounted balance between concerns and rewards" (Hallam & Zanella 2017) presents the way in which contemporary users behave. "The privacy paradox has significant implications for e-commerce, e-government, online social networking, as well as for government privacy regulation" (Kokolakis 2017).

We understand the importance of the phenomenon in question and how important security and privacy now are. Thus, the need to "develop products capable of automatically adapting to any given environment or user" (Zagouras, n.d.) is huge, and requires the incorporation of concepts such as understanding, concerns, awareness, attitudes and feelings into the software and its users.

Our study has shown us that psychological needs are a very important aspect of this research. Features like autonomy, competence, relatedness, self-actualization, security, popularity, money/luxury, physical/bodily, self-esteem, stimulation, and keeping it meaningful must be taken into account at every stage in the software creation process, and especially in those aspects relating to user interaction.

An interest work about the psychological needs as motivators for security and privacy actions on smartphones is presented from Kraus et al. (2017) with details about the behaviour for security and privacy action in smartphones. The need is growing every day. However, the users must acquire knowledge both via the distributors and the software itself. We must also do our utmost to ensure, given the speed of the technological advances and the human needs for privacy, that data is not lost.

4   Discussion and Conclusion

This paper has analyzed the field of User Experience (UX) across the whole spectrum of academic research from the last quarter century. We have presented the changing meanings ascribed to the concept of a software product in recent years and the changing reality that has taken shape in the procedures pertaining to the everyday use and experience of software. We have separated the concept of 'usability' from the concept of 'user experience', focusing on usability as a non-emotional aspect and UX being felt internally by the user. We have looked at the different academic fields involved in the latter, which include human computer interaction (HCI), psychology, design approaches,

marketing and philosophy. The theories on which the examined approaches are based are well-known and have produced important scientific results.

The approaches that have been taken to the combination of security and User eXperience are numerous, but it seems that the research is still overly-generalized and needs to develop approaches and frameworks which take a more specialized look at software development. It is obvious that data leaks via social media and other organizations made deliberately and for gain must be stopped, not at the level of policy decisions within the company but at the level of the software being used to protect data privacy. The software must be equipped with the technology and the 'judgment' required to deny the possibility even to its creator of using data of this kind for purposes other than those for which it was provided, or to transfer it elsewhere.

There is a need to create contemporary smart software using the best software development techniques, artificial intelligence — and always in full awareness of the security and privacy issues — which emphasizes and empathizes with the future user population. We believe that the field of UX with security (and privacy) extensions requires more research and has to connect the psychological needs of the users with UX approaches under the prism of security and privacy, to minimize the software's entropy. This area is still in its infancy. Methodologies of this sort will help the users to use — and the manufacturers to create — contemporary, smart and safe (for the user) software globally. The key conclusion from the aforementioned analysis is that UX elements presented in various studies have a huge impact on all three aspects of Information Security which means that designers and software analysts should consider UX as a key design factor when eliciting security (and privacy) requirements for the system to be. Providing a holistic approach for assisting analysts in this direction will be one important extension for both Usability Engineering and Security Engineering domains.

References

Arhippainen, L., Tähti, M.: Empirical evaluation of user experience in two adaptive mobile application prototypes. In: Proceedings of the 2nd International Conference, pp. 27–34 (2003). http://www.ep.liu.se/ecp/011/007/ecp011007.pdf

Bevan, N.: What is the difference between the purpose of usability and user experience evaluation methods? (2009). https://www.researchgate.net/publication/238775905

Chen, Z., Zhu, S.: The research of mobile application user experience and assessment model. In: Proceedings of 2011 International Conference on Computer Science and Network Technology, ICCSNT 2011, vol. 4, pp. 2832–2835 (2011). https://doi.org/10.1109/ICCSNT.2011.6182553

Cooper, A.: The Inmates are Running the Asylum (2012). https://doi.org/10.1007/978-3-322-99786-9_1

Dang-Pham, D., Pittayachawan, S., Bruno, V.: Exploring behavioral information security networks in an organizational context: An empirical case study. J. Inf. Secur. Appl. **34**, 46–62 (2017). https://doi.org/10.1016/j.jisa.2016.06.002

Demirbilek, O., Sener, B.: Product design, semantics and emotional response. Ergonomics **46**(13–14), 1346–1360 (2003). https://doi.org/10.1080/00140130310001610874

Fuchsberger, V., Moser, C., Tscheligi, M.: Values in action (ViA): combining usability, user experience and user acceptance. In: Proceedings of the 2012 ACM Annual Conference Extended Abstracts on Human Factors in Computing Systems Extended Abstracts, pp. 1793–1798. ACM, New York (2012). ISSN: 978-1-4503-1016-1

Gao, C., Wang, S., Zhong, C.: Research on user experience evaluation system of information platform based on web environment. In: Proceedings of 2013 2nd International Conference on Measurement, Information and Control, ICMIC 2013 (2013). https://doi.org/10.1109/MIC.2013.6758026

Gegner, L., Runonen, M., Keinonen, T.: Oscillating Between Extremes: A Framework for Mapping Differing Views on User eXperience (2012)

Gerber, P., Volkamer, M., Renaud, K.: The simpler, the better? Presenting the COPING Android permission-granting interface for better privacy-related decisions. J. Inf. Secur. Appl. **34**(March), 8–26 (2017). https://doi.org/10.1016/j.jisa.2016.10.003

Gross, A., Bongartz, S.: Why do I like it? Investigating the product-specificity of user experience (2012)

Hallam, C., Zanella, G.: Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. Comput. Hum. Behav. **68**, 217–227 (2017). https://doi.org/10.1016/j.chb.2016.11.033

Hartson, H.R., Andre, T.S., Williges, R.C.: Usability evaluation methods (2001)

Hiltunen, M., Laukka, M., Luomala, J.: Mobile User Experience. IT Press, Finland (2002)

Hu, Q., Xu, Z., Dinev, T., Ling, H.: Does deterrence work in reducing information security policy abuse by employees? Commun. ACM **54**(6), 54–60 (2011). https://doi.org/10.1145/1953122.1953142

Jetter, H.-C., Gerken, J.: A simplified model of user experience for practical application (2007). http://nbn-resolving.de/urn:nbn:de:bsz:352-opus-31516

Jokela, T., Iivari, N., Matero, J., Karukka, M.: The standard of user-centered design and the standard definition of usability: Analyzing ISO 13407 against ISO 9241-11. Design **46**, 53–60 (2003). https://doi.org/10.1145/944519.944525

Kainda, R., Fléchais, I., Roscoe, A.W.: Security and usability: analysis and evaluation. In: International Conference on Availability, Reliability and Security, Krakow, 2010, pp. 275–282 (2010). doi:https://doi.org/10.1109/ARES.2010.77

Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Comput. Secur. **64**, 122–134 (2017). https://doi.org/10.1016/j.cose.2015.07.002

Kraus, L., Wechsung, I., Möller, S.: Psychological needs as motivators for security and privacy actions on smartphones. J. Inf. Secur. Appl. **34**, 34–45 (2017). https://doi.org/10.1016/j.jisa.2016.10.002

Kremer, S., Schlimm, A., Lindemann, U.: The ExodUX framework: Supporting comprehensive user experience design. In: PICMET 2017 - Portland International Conference on Management of Engineering and Technology: Technology Management for the Interconnected World, Proceedings (2017). https://doi.org/10.23919/PICMET.2017.8125371

Kujala, S., Roto, V., Väänänen-Vainio-Mattila, K., Sinnelä, A.: Identifying hedonic factors in long-term user experience (2012). https://doi.org/10.1145/2347504.2347523

Kuniavsky, M., Founder, T.M.: Smart Things Ubiquitous Computing User Experience Design. Morgan Kaufmann Publishers Inc, San Francisco (2010). https://doi.org/10.1016/C2009-0-20057-2

Law, E., Vermeeren, A., Hassenzahl, M., Blythe, M.: An analysis framework for user experience (ux) studies: A green paper. In: International Conference HCI 2007, September 2007

Minge, M., Thüring, M.: Hedonic and pragmatic halo effects at early stages of user eXperience. Int. J. Hum. Comput. Stud. **109**, 13–25 (2018). https://doi.org/10.1016/j.ijhcs.2017.07.007

Mishra, S., Harris, M.A.: Human behavioral aspects in information systems security literature review (2006)

Möller, S., Engelbrecht, K.-P., Kühnel, C., Wechsung, I., Weiss, B.: A taxonomy of quality of service and quality of experience of multimodal human-machine interaction. In: International Workshop on Quality of Multimedia Experience, San Diego, CA, pp. 7–12 (2009). https://doi.org/10.1109/QOMEX.2009.5246986

Pc, A., Prabhu, B.: Integrating requirements engineering and user experience design in product life cycle management. In: First International Workshop on Usability and Accessibility Focused Requirements Engineering (UsARE), Zurich, pp. 12–17 (2012). https://doi.org/10.1109/UsARE.2012.6226784

Sascha, D.-P., Aus Berlin, M.: User experience of interaction with technical systems (2008)

Schulze, K., Krömker, H.: A framework to measure user experience of interactive online products (2010)

Sterman, J.D.: Business Dynamics. McGraw Hill, Boston (2000)

Tan, J., Rönkkö, K., Gencel, C.: A framework for software usability & user experience measurement in mobile industry. In: Proceedings - Joint Conference of the 23rd International Workshop on Software Measurement and the 8th International Conference on Software Process and Product Measurement, IWSM-MENSURA 2013 (2013). https://doi.org/10.1109/IWSM-Mensura.2013.31

Vyas, D., Chisalita, C.M., van der Veer, G.C.: Affordance in interaction (2012). https://doi.org/10.1145/1274892.1274907

Weiser, M.: The computer for the 21st Century. IEEE Pervasive Comput. **1**(1), 19–25 (2002). https://doi.org/10.1109/MPRV.2002.993141

Yee, K.-P.: Aligning security and usability. IEEE Secur. Priv. **2**(5), 48–55 (2004). https://doi.org/10.1109/msp.2004.64

Zagouras, P., Kalloniatis, C., Gritzalis, S.: Managing user experience: Usability and security in a new era of software supremacy. In: Tryfonas, T. (ed.) HAS 2017. LNCS, vol. 10292, pp. 174–188. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58460-7_12

Zarour, M., Alharbi, M.: User experience framework that combines aspects, dimensions, and measurement methods. Cogent Eng. **4**(1), 1–25 (2017). https://doi.org/10.1080/23311916.2017.1421006

Zimmermann, P.G., Eth, D.N.: Beyond usability – measuring aspects of user experience thesis June 2008 (2012)