A Taxonomy to Classify Risk End-User Profile in Interaction with the Computing Environment

Karla Susiane Pereira, Eduardo Feitosa[(✉)], and Tayana Conte

Institute of Computing (ICOMP), Federal University of Amazonas (UFAM),
Manaus, Amazonas, Brazil
{karla.pereira, efeitosa, tayana}@icomp.ufam.edu.br

Abstract. The objective of this paper to summarize the current knowledge in Human Computer Interaction (HCI) and Information Security (IS) areas regarding the classification of the end-user profile and present a new taxonomy to classify risk end-user profile in interaction with the computing environment in the information security perspective. A systematic mapping study was performed to assess the taxonomy of end-users. From an initial set of 105 papers based on string search, we conducted and selected a total of 21 papers. After the full reading of these 21 papers, only 02 papers were selected and 01 new paper were manually added. The results obtained allowed us to identify gap profiles of end-users related to the risk they cause to the computing environment. Thus, we propose a taxonomy to classify risk end-user profile in interaction with the computing environment.

Keywords: Risk end-user · Taxonomy, Computing environment

1 Introduction

With the massive introduction of technologies in various environments, the human factor has become a major threat in the Information Security (IS) perspective. Wrong behavior, distraction, ignorance and curiosity are examples related to users and security fails in information technology (IT) area. Different studies show the real link between incidents and security flaws and the interaction of end-users with the computing environments [1–3]. To sum up, IS community has a jargon that says: "the end-user is the weakest link in any security process".

Different from Information Security area, in Human-Computer Interaction (HCI) the end-user is not blameworthy. On the contrary, all responsibility for any security flaws is the system developer. It is he who needs to worry when the end-user makes something wrong. By the way, the correct and safe use is not an end-user function. The argument is that common errors in system design, interfaces and interaction process can lead to security bugs in the operating system by end-users [4]. Thus, the identification and correction of these errors allows end-users to use safer operations.

Although both areas have different and contradictory views on the role of the end-user, the hard fact is that human being makes mistakes or failures, even in the

presence of well-established processes. Thus, the following question arises: is it possibility to classify the risk end-user profiles from the information security perspective? Such an evaluation may be useful in that it allows describing the characteristics of the end-users, as the information is used and, finally, which user profiles can present a risk to the computing environment.

The objective of this paper is to summarize the current knowledge in Human Computer Interaction (HCI) and Information Security (IS) areas regarding the classification of the end-user profile and present a new taxonomy to classify risk end-user profile in interaction with the computing environment.

2   Background

This section presents the concepts of risk in both Information Security (IS) and Human Computer Interaction (HCI) areas. However, we also present some security concepts necessary for better explain risk and its analysis.

2.1   Fundamentals and Information Security Concepts

The Information Security area is governed by ISO/IEC 27000 family, whose main objective is the protection of information (data and systems) against various types of threats.

In general, the focus of these rules is to ensure three fundamental principles of information [5]: confidentiality - the information only is accessible by authorized persons; integrity - the guarantee of accuracy and completeness of information and processing methods; and availability - ensures availability to ensure reading success, of transport and storage of information.

In addition to these fundamental principles, Table 1 explains some useful and essential concepts in Information Security area.

Table 1. Concepts of Information Security area

Concepts	Definition
Security Incident	Is the occurrence of undesired and unexpected events, which has high probability of prejudice business operations and threatens the security of information [6]
Attack	Is a type of security incident characterized by the existence of an agent (attacker) that seeks to get some kind of return, reaching some asset value [6]
Attacker	Is a term used to indicate an individual or group of individuals who can make a threat [7]
Asset	Any element that has value to the organization (for example, information, physical assets, software, services and people) [5]
Threats	Are agents or conditions that, by exploiting vulnerabilities, may cause damage or loss [8]

(Continued)

Table 1. (*Continued*)

Concepts	Definition
Vulnerability	Is a weakness of an asset or group of assets that can be exploited by one or more threats [5]
Probability	Is the chance of a security flaw in relation to the asset vulnerabilities and the threats that may exploit this vulnerability [7]
Impact	The impact of a security incident is measured by the consequences it might cause to business processes supported by the asset [7]

2.2 Risk Concepts

In general, the term risk is defined as the possibility of danger, uncertain but predictable, that is the threat of damage to person or thing [9].

In Information Security area, the risk is understood as a condition that creates or increases the potential for damage and loss. The ISO/IEC 27005 [7] defines that the risk of information security is the ability of a specific threat exploits vulnerabilities of an asset or set of assets, harming the organization. According to ISO/IEC 31000 [10], risk is the effect of uncertainty on objectives, where an effect is a deviation from the expected behavior (positive and negative) and objectives may have different aspects (financial goals, health, safety and environmental, for example) and may apply at different levels.

In HCI area, one of the most considered risks is the communication breakdown. The best concept that assigns is the communication breakdown. It is the moment of interaction in which the end-user demonstrates not has understood the meta-communication designer or times when the end-user finds it difficult to express their intention to communicate the interface [11]. However, it is important to note that communication breakdown, even if treated, can lead to errors and, consequently, the losses and potential damage.

3 Research Method

Our systematic mapping study, to categorize end-user profiles, was performed in three steps: planning, conducting, and reporting.

3.1 Planning Step

In this step, we performed the following activities in order to establish a review protocol: (1) establishment of the research question; (2) definition of the search strategy, (3) selection of primary studies. Each of them is explained in detail as follows.

Research Question. The goal of our study is to examine the profiles of end-users from the point of view of the following research question: "*What are the classifications of end-users in computing environment context?*".

Search Strategy. We adopt three criteria in research sources selection: (i) search for papers in digital library; (ii) availability query papers; and (iii) papers available in English. For primary studies, we choose Scopus because it is the largest database indexing abstracts and citations [12]. The reviewed period include studies published from 1989 to 2012. We also manually search in journals and books available on the web.

We used a search string consists of two concepts: user computing and computing environment, according to the Table 2.

Table 2. Search String

Concept	Alternative terms & Synonyms
User Computing	("user computing" OR "user participation" OR "computer user" OR "user security risk" OR "user risk") **AND**
Computing Environment	("computing environment" or "computer environment")

Selection of Primary Studies. In the first step, called 1st filter, we evaluated only the title and the abstract of each paper to according inclusion and exclusion criteria and selecting papers that would be within the scope of the research question. In the second stage (or 2nd filter), researchers conducted a thorough reading of the selected papers from the 1st filter. And the papers were included/excluded according to the inclusion and exclusion criteria (Tables 3 and 4).

Table 3. Inclusion Criteria

#	Inclusion Criteria
IC1	Papers that discuss concepts of user profiles or category of users in computer environment.

Table 4. Exclusion Criteria

#	Exclusion Criteria
EC1	Papers in which the language is different from english cannot be selected;
EC2	Papers that are not available for reading and data collection (papers that are only accessible through paying or are not provided by the search engine) cannot be selected;
EC3	Duplicated papers cannot be selected;
EC4	Publications that do not meet any of the inclusion criteria cannot be selected.

3.2 Conducting Step

The application of the review protocol yielded the following preliminary results. The application of the review protocol yielded the following preliminary results. A total of 105 papers were returned from the search string. In the first filter, we selected 21 papers

(01 paper was doubled). In the second filter, we selected 02 papers by systematic review. We also manually added 01 paper. The search results revealed that the research papers concerning user profiles classification, based on the string round, are scarce.

4   Research Results

Based on counting the primary studies, the overall results are presented in Table 5.

Table 5.   Research Question

What are the classifications of end-users in computing environment context?
Title: User Cube: A Taxonomy of End Users
Keywords: End-User Computing; Morphological Analysis; Taxonomy; User Cube.
Authors: Cotterman, William W., Kumar, Kuldeep.
Year: 1989
Source: Communications of the ACM - Journal Metrics.
Type: Paper
Type of study: Morphological Analysis.
Search: Automated Search
Title: Management of End User Computing.
Keywords: Information Systems; Database Systems.
Authors: Rockart, John F. and Flannery, Lauren S.
Year: 1983
Source: Communications of the ACM
Type: Paper
Type of study: Exploratory Research.
Search: Automated Search
Title: A Guide to Computer User Support for Help Desk and Support Specialists
Keywords: Customer; User; Support.
Authors: Fred Beisse
Year: 2012
Source: Course Technology, Cengage Learning.
Type: Book
Type of study: Guide
Search: Automated Search

Cotterman and Kumar [13] proposed an end-users model classification to assist managers in identifying users who operate out of function, allowing for measures to increase end-users productivity and satisfaction. The authors argue that end-users can be differentiated according to the form that interacts with a computer system within a company at: producers, those that generate results (information products); consumers, those who eat results; and producers/consumers, who produce and consume results. To understand the variety of environments and situations in which organizations provide technical support to their knowledge workers, Beisse [1] classified end-users in six categories: environment, skill level, frequency of use, software use, features used and relationship.

Rockart and Flannery [3] elaborate the first end-user classification. They argued that end-user profile is a result of the functions performed into the organization. Based on this, six distinct end-users categories were proposed: non-programming end-users, command level users, end-user programmers, functional support personnel, end-user computing support personnel and programmers.

5 Proposal of Taxonomy

As can be seen in the systematic mapping, we found the limited number of end-user taxonomies and none of them related to information security area. Thus, this work proposes a taxonomy aiming to show a more direct view of end-user, about information security perspective, using three pillars: knowledge, experience and use of information. Figure 1 shows the proposed taxonomy schema.

It is important to clarify that our classification model of the end-user profile is based on models proposed by Rockart and Flannery [3], Beisse [1], Cotterman and Kumar [13].
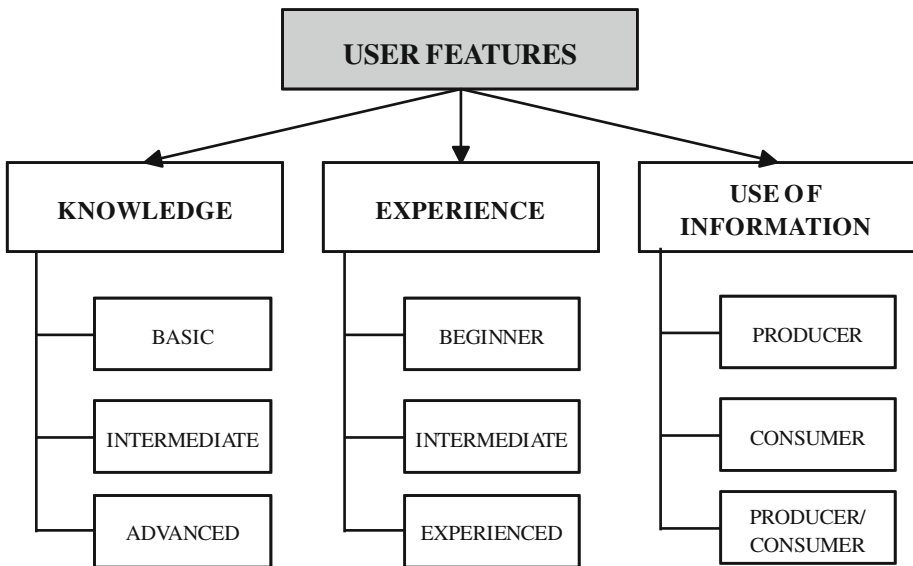

Fig. 1. Proposed Taxonomy Schema

The first pillar of our taxonomy is knowledge, whose purpose is to identify the level of information in computer area. The knowledge is divided into three levels: (1) Basic, end-user who knows the basics of computer; (2) Intermediate, end-user who knows the information technology concepts and solutions and information systems; and (3) Advanced, end-user who knows the advanced concepts of information technology and has the capacity to offer solutions for information systems.

As proof of the importance of computer knowledge, Adams and Sasse [14] applied a web-based questionnaire with 139 responses from employees of an organization.

They found that users do not understand the authentication process, confusing the user identification (ID) and password sections. In others words, users lack security knowledge.

The second pillar is **experience**, which refers to the frequency and expertise conducting daily computing tasks. Experience is divided into three levels: (1) Beginner, lay end-user, without ability to perform efficiently the tasks in information systems and/or access data through menus; (2) Intermediate, command level end-user with the ability to perform tasks in information systems as well as developing procedures for obtaining necessary data and generate simple reports; and (3) Experienced, end-user with the ability to perform efficiently the tasks in information systems as well as working with functional support, support to the end user and computer programming.

The third and final pillar is the **use of information**, used to determine the information applicability by the end-user. This group is also divided into three levels: (1) Producer, the end-user who inserts information; (2) Consumer, the end-user who consumes information; and (3) Producer/Consumer, the end-user who consumes and inserts information.

5.1   Comparison

In order to better illustrate the difference between our proposal and other classifications of end-user profiles, we explore a example of a trainee: "He has 18 years old, works in the information technology department of a company, in a support function for end-user."

In our taxonomy, he is classified as an end-user with intermediate knowledge and experience, and producer/consumer of information. For Rockart and Flannery taxonomy [1], the same user is considered as end-user computing support personnel. In Cotterman and Kumar [13], he is regarded controller/operator and in the taxonomy proposed by Beisse [3] he is considered a professional user with intermediate knowledge and low qualification that uses with regularity software used in the company.

In general lines, the model proposed by Rockart and Flannery is simple, focused only on the functions that the end-user performs in the organization. The model proposed by Cotterman and Kumar is intermediate because it focuses on three dimensions (development, operation and control) of end-user performance. In contrast, the model proposed by Beisse is the most complex, covering six categories (environment, skill level, used applications, frequency use, end-user features and relation).

It is important to mention that the access environment (domestic, corporate, public or private) is not part of the group features presented in our taxonomy because it considers that the evaluation is performed in the computing environment organizations.

5.2   Why Use the Proposed Taxonomy?

The taxonomies of Rockart and Flannery [3], Beisse [1], and Cotterman and Kumar [13] make use of knowledge, experience and use of information to build end-user profiles. However, these pillars are seen as independent elements. For instance, using only knowledge and/or experience it is possible to build an end-user profile.

Otherwise, our taxonomy allows determining the behavior of end-users regarding the computing environment, especially in an information security perspective where identify the applicability of user information is fundamental to ensure data security. For example, in November 2012, Google services were limited during 27 min in regions of Asia. The reason was the leak of Internet routes. An IT employee of Maratel Company, during maintenance of Internet routes, made a misconfiguration [15].

Analyzing the case using our taxonomy, we can assume that the IT employee has advanced knowledge and good experience with the platform (routers and Internet routes). Moreover, it is a producer user/consumer that performs system settings and maps the returned information. As result, we can suppose that although the employee has high competence, experience in implementation activities and use of information, a supervision system that evaluate the activities before the final execution could have prevented the problem.

In other words, our taxonomy allows to set an risk end-user profile, enabling the creation of prevention against future risks.

6   Conclusions

The use of technology has become increasingly present in daily life and in this scenario, from information security perspective, the end-user is a threat to computing environments. But how to identify users that can represent a security risk?

The literature research directly related to risks in computer interaction is not vast. The research on end-user profile has different point of views and uses. It is applicability depends on researcher experience and the way it performs the classification.

This work allowed us to identify the existent gap among end-users profiles, especially when they are related to risk in computing environment. For that, this paper introduced the reader in the concepts of risk in both Information Security (IS) and Human Computer Interaction (HCI) areas. Following, the research method and results of a systematic review mapping was presented, proving the low interest in to measure end-users and risks.

Finally, this study presents a new taxonomy to classify end-users profiles in computing environments. Using three pillars (knowledge, experience and use of information), our taxonomy allows to set an risk for an end-user profile, enabling the creation of prevention mechanisms against future threats.

References

1. Beisse, F.: A Guide to Computer User Support for Help Desk and Support Specialists, 5th edn. Course Technology Cengage Learning, USA (2012)
2. Iachello, G., Hong, J.: End-user privacy in human-computer interaction. Found. Trends Hum. Comput. Interact. **1**(1), 1–137 (2007)

3. Rockart, J.F., Flannery, L.S.: The management of end user computing. ACM Commun. **26**(10), 776–784 (1983)
4. Rogers, Y., Sharp, H., Preece, J.: Interaction Design: Beyond Human - Computer Interaction, 4th edn. Elsevier Editora Ltda., London (2015)
5. ISO/IEC: ISO/IEC 27002:2005 - Information technology – Security techniques – Code of practice for information security management. Technical report (2005)
6. ISO/IEC: ISO/IEC 27000: 2009 information technology - security techniques - information security management systems -overview and vocabulary. Technical report (2009a)
7. ISO/IEC: ISO/IEC 27005:2008: Information Technology - Security Techniques - Information Security Risk Management. Technical report (2008)
8. ISO/IEC: ISO/IEC 13335-1: 2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management. Technical report (2004)
9. Oxford Dictionary of English. OUP Oxford, 3rd edn. (2010)
10. ISO/IEC 31000: 2009: Risk management? Principles and guidelines. Technical report (2009b)
11. Barbosa, S.D.J., de Souza, C.S., Paula, M.G.: The semiotic engineering use of models for supporting reflection-in-action. In: HCII2003 - HCI International, 2003, Creta, Human-Computer Interaction: Theory and Practice (Part I), vol. 1, pp. 18–22. Lawrence Erlbaum, Mawah (2003)
12. Kitchenham, B., Charters, S.: Guidelines for Performing Systematic Literature Reviews in Software Engineering, Version 2.3, EBSE Technical Report, Keele University, UK (2007)
13. Cotterman, W.W., Kumar, K.: User cube: a taxonomy of end users. Commun. ACM **32**(11), 1313–1320 (1989)
14. Adams, A., Sasse, M.A.: Users are not the enemy. Mag. Commun. ACM **42**(12), 40–46 (1999)
15. Paseka, T.: Why google went offline today and a bit about how the internet works. https://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about/ (2012)