iHIP: Towards a User Centric Individual Human Interaction Proof Framework

Christos Fidas
Department of Cultural Heritage Management and New Technologies, University of Patras, GR-26504 Patras, Greece
fidas@upatras.gr

Heinrich Hussmann
Media Informatics Group, University of Munich (LMU)
Amalienstr. 17, 80333 Munich, Germany
hussmann@ifi.lmu.de

Marios Belk
Department of Computer Science, University of Cyprus
CY-1678 Nicosia, Cyprus
belk@cs.ucy.ac.cy

George Samaras
Department of Computer Science, University of Cyprus
CY-1678 Nicosia, Cyprus
cssamara@cs.ucy.ac.cy

CHI'15 Extended Abstracts, Apr 18-23, 2015, Seoul, Republic of Korea
ACM 978-1-4503-3146-3/15/04.
http://dx.doi.org/10.1145/2702613.2732748

Abstract
A Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a widely used Human Interaction Proof mechanism to protect on-line services against automated software agents. Nowadays, there is a consensus among researchers, practitioners and users that current design approaches of CAPTCHA need to be improved in order to provide a fair trade-off solution between security and usability. In this paper, we propose a shift from a generic Human Interaction Proof (HIP) to a more user-friendly Individual Human Interaction Proof (iHIP) approach by incorporating a dynamic and extendable human and technology factor based user-centric framework. Such an approach provides an alternative point of view to current state of the art practices aiming to deliver the best-fit CAPTCHA to each individual by taking into consideration contextual and behavioral interaction data.

Author Keywords
Usable Security; CAPTCHA; Framework Design

ACM Classification Keywords
H.5 Information Interfaces and Presentation

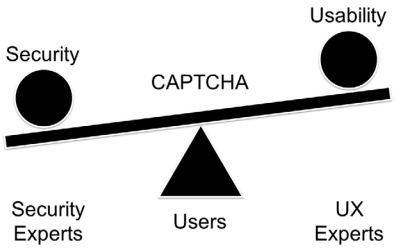

Figure 1. Security vs. Usability in CAPTCHA design

Introduction

Design and development of CAPTCHA represents a typical example of a cross-roads priority problem, between security and usability, which emerge from contradictory requirements posed by different stakeholders (Figure 1), inherent to the function and purpose of CAPTCHA. It's a security mechanism users rarely benefit from, but it's necessary from a system's security perspective. In particular, security experts increase continuously the security levels of a CAPTCHA, end-users demand transparent, adaptable and user-friendly solutions, and service providers are trying, together with user experience experts, to find a viable equilibrium among security and usability. However, a variety of empirical studies report that typical end-users have increased difficulties in solving CAPTCHA challenges [1, 2], so we are far from reaching a viable solution with current state of the art design and technological approaches.

Today's most popular on-line services follow a "one-size-fits-all" CAPTCHA approach. In fact, the CAPTCHA challenge remains the same for all users regardless of the interaction device type, the context of use or the user's individual characteristics and preferences. Such approaches seem not really adequate for nowadays fast moving information society which embraces the utilization of CAPTCHA challenges on a variety of interaction device types, heterogeneity of users with unique preferences and characteristics and diverse contexts of use.

In this realm, the work presented in this paper is primarily driven by the need to apply a User Centered Design (UCD) approach related to CAPTCHA mechanisms. According to the ISO 9241-210 [3] standard, UCD approaches start with understanding user needs and requirements as an integral part of information systems design which is critical to its success. Therefore, this paper attempts an initial literature review related to contextual (human, technology and CAPTCHA design) factors that affect user experience in CAPTCHA. Subsequently, we present initial ideas related to the design of the iHIP framework aiming to deliver personalized Individual Human Interaction Proofs (iHIP) as a viable alternative to current state of the art approaches.

Factors affecting User Experience related to CAPTCHA

Human Factors

A recent study reported in [1] notes that lingual characteristics of users affect users' perceptions and effectiveness in CAPTCHA-related tasks. Results have shown that a considerable number of participants prefer to solve text-recognition CAPTCHA that are using characters from their native-speaking language alphabet instead of the traditional Latin-based. Another recent study which investigated the effects of human cognitive differences in information processing within CAPTCHA tasks provides indications that cognitive processing characteristics of users have an influence towards preference and performance with respect to different types of CAPTCHA challenges (text-recognition and image-recognition) [4]. From an accessibility perspective, a number of CAPTCHA have been proposed for supporting users with vision problems and other disabilities [5].

Technology Factors

A recent study [6] which investigated the usability of text-, image- and speech-recognition CAPTCHA on

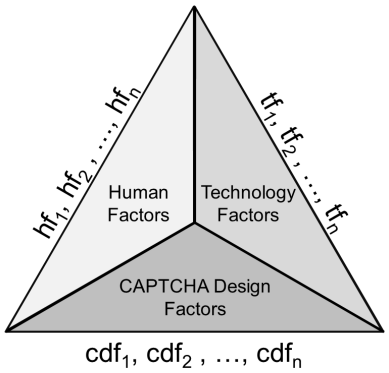

Figure 2. The interplay among human, technology and CAPTCHA design factors on CAPTCHA task performance.

mobile devices revealed the users' positive attitude and preference towards image-recognition CAPTCHA. Another study [7] suggested several design guidelines for mobile-based CAPTCHA interactions such as, taking into account the users' context while interacting (e.g., standing, sitting, walking), providing minimal instructions and avoiding interactions that require zooming as well as taking into account network and bandwidth usage.

Furthermore, research works have proposed CAPTCHA mechanisms that leverage interaction design capabilities of mobile devices, such as SeeSay CAPTCHA [8], that requires users to say the answer (instead of typing it) based on a visual stimulus. Another example includes Clickable CAPTCHA [9] that converts regular text-recognition CAPTCHA into clickable CAPTCHA challenges aiming to simplify and speed-up the entry of the text-based solution.

CAPTCHA Design Factors

According to [10], increasing the security of text-recognition CAPTCHA could be achieved with the following design principles: i) randomize the CAPTCHA length and font size; ii) rotate the characters in a wave fashion; iii) use lines with the same width and color as the characters; and iv) collapse the characters. Using a background image with noise in the challenge has shown to be insecure and is not suggested to be included in CAPTCHA designs [10].

Regarding image-recognition CAPTCHA, based on [11], increasing the security of an image-recognition CAPTCHA could be achieved as follows: i) use graphical objects with unambiguous high-level semantics; ii) use a higher number of graphical objects and a variety of object types; and iii) eliminate the possibility of using a priori knowledge for the challenge (i.e., the current challenge should be independent to past challenges).

Finally, the security features for speech-recognition CAPTCHA include increasing the CAPTCHA character length and alphabet, and adding background noise [5].

Conceptual Design of the iHIP Framework

A conclusion that can be derived from the presented literature review is that there exist interdependencies among human, technology and CAPTCHA design factors (Figure 2) which affect users' preference and performance related to CAPTCHA. Therefore, from a conceptual point of view the iHIP framework aims at transforming these interdependencies into formal representations for offering adaptive and personalized CAPTCHA solutions based on human and technological driven factors while preserving security factors.

The purpose of the envisioned framework is to generate a unified abstraction of the users' context of interaction by converting it to a set of statements based on a predefined ontology which entails appropriate metadata for each involved entity (user, technology, CAPTCHA) that constitutes the user's overall context of interaction. Thus, semantic capabilities can be added, allowing the service provider to reason about the context of use and produce intelligent CAPTCHA challenges to pre-defined and specific context-based rules to the benefit of the users.

As shown in Figure 3, the iHIP framework consists of the following main modules: i) *the individual context model*; and ii) *the personalization module*.

Table 1. Table of symbols

Symbols	Description
U	Set of users $\{u_1,u_2,\ldots,u_n\}$
FC	Set of factors $\{hfc_1,hfc_2,\ldots,hfc_n, tfc_1,tfc_2,\ldots,tfc_n, cdfc_1,cdfc_2,\ldots,cdfc_n\}$
$UCM_j(u_i)$	Set of factors of the individual context model of user u_i
CR	Set of context rules $\{cr_1,cr_2,\ldots,cr_n\}$
Blc	Boolean logical connectives $\{AND,OR,NOT,XOR,\ldots\}$
Opr	Operators $\{=,==,<,>,!=,\ldots\}$

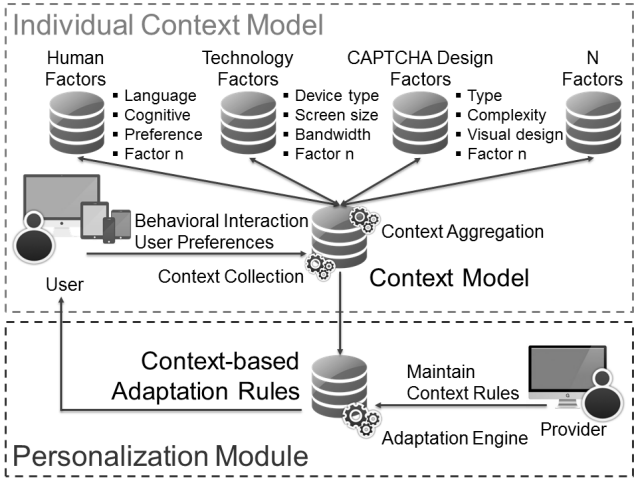

Figure 3. The iHIP framework (conceptual design)

Individual Context Model

This module aims to define and set the specifications for modeling human factors like lingual and cultural aspects, comprehension and perceptual abilities, cognitive representation of information, along with technology factors like security levels and preferences, and interaction device attributes. Contextual explicit and implicit information gathering techniques are used for creating and maintaining appropriate static and dynamic models of users which reflect behavioral data over time but as well users' preferences.

Personalization Module

The personalization module is responsible to decide and deliver the best-fit CAPTCHA solution to each user, aiming to balance the security and usability factors of the challenge based on the individual context models. In this context, adaptation mechanisms are applied within different perspectives, namely, adaptivity based on human factors, adaptivity based on technology factors, and adaptivity based on CAPTCHA design factors. Simple user customization and rule-based mechanisms are envisioned to be used to decide what adaptation will be performed. On the other hand, collaborative mechanisms could assist the adaptation process by modeling the behavior of users with similar preferences and characteristics.

Formalization. Table 1 describes the symbols of the formalization. Accordingly, let U denote a set of users $\{u_1,u_2,\ldots,u_n\}$. Let FC denote a set of factors which are maintained by the service provider $\{hfc_1,hfc_2,\ldots,hfc_n, tfc_1,tfc_2,\ldots,tfc_n, cdfc_1,cdfc_2,\ldots,cdfc_n\}$. Let $UCM_j(u_i)$ denote a set of factors of the individual context model of user u_i. The result of $UCM_j(u_i)$ is a set of triplets of the form (u_i, fc_i, val), where j is the triplet identifier, u_i is the user, fc_i is the factor of the model (e.g., age, device, etc.) and val is the value of the factor fc_i, where val can be any value type (e.g., Numeric, String, Boolean, etc.).

Figure 4 depicts a simple instance of a best-fit CAPTCHA challenge generation for a particular *user* u_1 that was generated based on his *Individual Context Model* $UCM_1(u_1)$. According to the individual context model values (e.g., $UCM_1(u_1)=(u_1, age, 65)$; $UCM_1(u_1)=(u_1, nationality, German)$, etc.), the system will decide the best-fit CAPTCHA.

The best-fit CAPTCHA algorithm uses a rule-based engine which allows the maintenance of context-based rules. Let CR denote a set of context rules which are maintained by the service provider $\{cr_1,cr_2,\ldots,cr_n\}$. Each context-based rule is based on a decision making model which has one hypothesis part related to human and

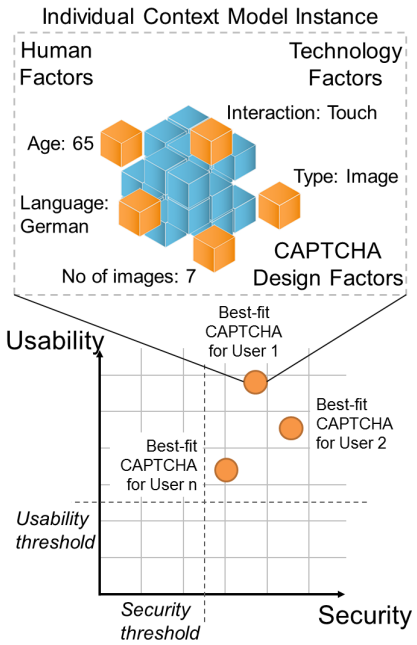

Figure 4. An instance of a best-fit CAPTCHA recommendation

technology factors and precisely one decision part related to CAPTCHA design factors. As such, the service administrator could select certain factor properties/attributes, set the desired values and relate them with the appropriate Boolean logical connectives and Operators (Table 1) in order to construct fully parenthesized expressions of arbitrary complexity that can be applied to a group of users or to specific individuals following deductive or inductive reasoning.

Use Case Scenarios. Rolf, an older adult that suffers from deteriorating vision, uses a desktop computer for his daily online activities. The iHIP framework maintains an expanded context model of Rolf and compares the static values of his profile with other registered users with similar static (age, language, cognitive abilities, etc.) and dynamic (speed, number of attempts to solve a CAPTCHA, etc.) characteristics. Taking into consideration that the cognitive and visual strengths of humans decline over time, the framework enables a pre-defined context-based rule and uses a collaborative mechanism that exploits the preference and recommendations of other users (sharing similar models). As a result, the framework decides to recommend to Rolf an image-recognition CAPTCHA than the usual text-recognition which requires from a user to recognize distorted characters (that is a heavier cognitive process and requires better visual abilities).

Angelos is a young architect student from Greece, he posts comments on the educational portal of the University several times per week. Angelos uses interchangeably interaction device types (desktop, mobile or tablet) to access the portal. The iHIP framework maintains for Angelos a static and dynamic user profile. Angelos has a Verbal cognitive style (he processes more efficiently textual information), and accordingly, the framework provides him a text-recognition CAPTCHA challenge [4]. In addition, since Angelos is a native Greek speaker, the method provides a localized text-recognition CAPTCHA challenge (illustrating Greek characters) [1]. However, the history of interactions has shown that Angelos has difficulties when solving the text-recognition CAPTCHA challenge when interacting on his mobile device and therefore, the method decides that an image-recognition CAPTCHA might be a better solution for him when interacting through touch-based mobile devices.

Conclusions and Future Work

The overall objective of the iHIP framework is to incorporate an extendable factor-based context model that can be applied for the delivery of personalized CAPTCHA challenges based on human and technology factors. From an architectural point of view the iHIP framework could follow an Application Service Provider model through two main published services: i) the Individual Context Modelling Service, responsible to generate the context models by initially collecting and processing data about the users' behavioral patterns and preferences; and ii) the Personalized CAPTCHA Service for personalizing the CAPTCHA tasks based on specific adaptation mechanisms.

In this context, the main skepticism on the feasibility of such an attempt is focused on the challenge to personalize a task which by definition is difficult to personalize since the existence and identity of the user is not known. However, rethinking current delivery approaches of CAPTCHA mechanisms seems to be a promising research direction given the diversity of users and contexts of interactions. Apparently, the

added value of such an endeavor entails many benefits. Examples are: non-Latin users will be able to solve a CAPTCHA challenge in their own alphabet; users could set up rule-based adaptations in order to specify which CAPTCHA type they prefer according to pre-defined context-based rules. Users with certain perceptual abilities, especially older adults, will be able to solve a CAPTCHA adapted to their own needs by taking also into consideration technological and contextual factors.

Finally, from a security perspective, such an attempt might strengthen the security aspects of CAPTCHA. In particular, the malicious software has to pretend to be a specific individual than a general human being. This is by definition a more difficult problem to address which requires working around a credible user model which is maintained on the service provider's premises. On the other hand, personalization approaches embrace new vulnerabilities related to security that need closer attention, e.g., malicious software might pretend a particular human behavior (e.g., setting a user profile with limited eye sight etc.) which leads to easier to break CAPTCHA. From this perspective, the framework could have a minimum security threshold which can be overlapped only for users who successfully verify particular characteristics and preferences (e.g. by following validation processes).

Taking into account that the process of designing and developing CAPTCHA is limited only by the availability of supporting technology, the idea to move from a generic Human Interaction Proof (HIP) to a more user-friendly Individual Human Interaction Proof (iHIP) can be of general value aiming to increase user acceptance related to CAPTCHA.

References

[1] Fidas, C., Voyiatzis, A., Avouris, N. On the necessity of user-friendly CAPTCHA. In *Proc. CHI'11*, ACM (2011), 2623-2626.

[2] Bursztein, E., Bethard, S., Fabry, C., Mitchell, J., Jurafsky, D. How Good are Humans at Solving CAPTCHAs? A Large Scale Evaluation. In *Proc. SSP'10*, IEEE Computer Society (2010), 399-413.

[3] ISO 9241-210:2010. Ergonomics of human-system interaction, Part 210: Human-centred design for interactive systems.

[4] Belk, M., Fidas, C., Germanakos, P., Samaras, G. Do cognitive styles of users affect preference and performance related to CAPTCHA challenges? *Ext. Abstracts CHI'12*, ACM (2012), 1487-1492.

[5] Bigham, J., Cavender, A. Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use. In *Proc. CHI'09*, ACM (2009), 1829-1838.

[6] Wismer, A., Madathil, K.C., Koikkara, R., Juang, K., Greenstein, J. Evaluating the usability of CAPTCHAs on a mobile device with voice and touch input. In *Proc. HFES'12*, 1228-1232.

[7] Reynaga, G., Chiasson, S. The usability of CAPTCHAs on smartphones. In *Proc. SECRYPT'13*, 427-434.

[8] Shirali-Shahreza, S., Penn, G., Balakrishnan, R., Ganjali, Y. SeeSay and HearSay CAPTCHA for mobile interaction. In *Proc. CHI'13*, ACM (2013), 2147-2156.

[9] Chow, R., Golle, P., Jakobsson, M., Wang, L., Wang, X. Making CAPTCHAs clickable. In *Proc. HotMobile'08*, ACM (2008), 91-94.

[10] Bursztein, E., Martin, M., Mitchell, J. Text-based CAPTCHA strengths and weaknesses. In *Proc. CCS'11*, ACM (2011), 125-138.

[11] Zhu, B., Yan, J., Li, Q., Yang, C., Liu, J., Xu, N., Yi, M., Cai, K. Attacks and design of image recognition CAPTCHAs. In *Proc. CCS'10*, ACM (2010), 187-200.