Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2018 Proceedings | Southern (SAIS)

Spring 3-2018

SECURITY AND USER EXPERIENCE: A HOLISTIC MODEL FOR CAPTCHA USABILITY ISSUES

Jayalakshmi Raman
University of North Florida, n01382362@ospreys.unf.edu

Karthikeyan Umapathy
University of North Florida, k.umapathy@unf.edu

Haiyan Huang
Flagler College, hhuang@flagler.edu

Follow this and additional works at: https://aisel.aisnet.org/sais2018

Recommended Citation
Raman, Jayalakshmi; Umapathy, Karthikeyan; and Huang, Haiyan, "SECURITY AND USER EXPERIENCE: A HOLISTIC MODEL FOR CAPTCHA USABILITY ISSUES" (2018). *SAIS 2018 Proceedings*. 27.
https://aisel.aisnet.org/sais2018/27

This material is brought to you by the Southern (SAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in SAIS 2018 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

SECURITY AND USER EXPERIENCE: A HOLISTIC MODEL FOR CAPTCHA USABILITY ISSUES

Jayalakshmi Raman
University of North Florida
n01382362@ospreys.unf.edu

Karthikeyan Umapathy
University of North Florida
k.umapathy@unf.edu

Haiyan Huang
Flagler College
hhuang@flagler.edu

ABSTRACT

CAPTCHA is a widely adopted security measure in the Web, and is designed to effectively distinguish humans and bots by exploiting human's ability to recognize patterns that an automated bot is incapable of. To counter this, bots are being designed to recognize patterns in CAPTCHAs. As a result, CAPTCHAs are now being designed to maximize the difficulty for bots to pass human interaction proof tests, while making it quite an arduous task even for humans as well. The approachability of CAPTCHA is increasingly being questioned because of the inconvenience it causes to legitimate users. Irrespective of the popularity, CAPTCHA is indispensable if one wants to avoid potential security threats. We investigated the usability issues associated with CAPTCHA. We built a holistic model by identifying the important concepts associated with CAPTCHAs and its usability. This model can be used as a guide for the design and evaluation of CAPTCHAs.

Keywords

CAPTCHA, Usability, Security, Conceptual Framework

INTRODUCTION

CAPTCHA, an acronym for Completely Automated Public Turing tests to tell Computers and Humans Apart, is a program intended to distinguish humans from bots (von Ahn et al. 2004). The purpose of CAPTCHA is to identify and block malicious bots that may spam and/or make unauthorized use of websites. These malicious program's harmful effects extend to extracting private data, spamming signups and registrations, and swaying polls in websites. CAPTCHA is designed as a challenge response test (also known as human interaction proofs), that is simple enough for humans but hard for the bots. This is achieved as a visual test in most scenarios as computers lack the ability human eyes have, to process patterns.

Almost everybody has experienced some form of CAPTCHA while surfing the Web. The most common one is a set of blurry texts that must be recognized and typed correctly. CAPCTHAs are designed as the gateways of websites to grant the access to "legitimate" site visitors. There are several distinct categories of CAPTCHAs. Some popular types of CAPTCHAs are (Singh and Pal 2014): text-based (images of distorted text), image-based (set of images with patterns among them), audio-based (distorted sound clips), video-based (video describing tag words), and 3D CAPTCHAs (animated texts or verification code). CAPTCHA architecture, its innerworkings, and how it secures a website from bot attack can be found at (Banday and Shah 2011).

CAPTCHA is widely adopted as a defense mechanism across commercial websites to determine whether a potential user is a human. That being said, the usability of CAPTCHAs also contributes significantly to the quality of user experience one obtains from the website. The design nature of CAPTCHA is meant to be easy on humans, but hard for the automated software/bots. However, with the advent of machine learning algorithms, deep learning techniques and pattern recognition algorithms; bots are getting better at reading CAPTCHAs (Sivakorn et al. 2016; Tam et al. 2009; Yan and El Ahmad 2007). As a result, some additional features are incorporated into the design of CAPTCHAs to make the tests harder for bots to pass. However, the improved CAPTCHAs sometimes are considered to be interfering with usability and productivity because of their cumbersome nature (C. A. Fidas et al. 2011).

As a widespread security measure encountered by most Internet users, it is important to study CAPTCHAs state-of-the-art schemes and the related usability issues (C. Fidas et al. 2015; Yan and El Ahmad 2008). Usability and functionality are two important aspects of HCI (Jain and Sivaselvan December 2012) and this research focuses on the usability factor in the domain of CAPTCHAs. This paper intends to provide a holistic view of CAPTCHAs, its evolution, and studying the various issues encountered by users. The aim of this research is to develop a conceptual framework that can shed light on how to design

effective and highly usable CAPTCHAs. This framework will be developed based on empirical facts claimed in literature thus serving as a model for evaluation for future CAPTCHA designs.

RESEARCH METHODOLOGY

The aim of this research is to provide a comprehensive understanding of CAPTCHA, its schemes and purpose, to determine the usability issues associated with CAPTCHAs, and to provide a means of identifying the balance between usability and security in CAPTCHAs. To achieve these goals, we conduct a comprehensive study to gain an in-depth understanding of user's view of CAPTCHA and develop a holistic model that would in turn help in designing an effective and adoptable CAPTCHA. This paper uses a qualitative method proposed by Jabareen (2009) for conducting systematic study of the phenomena involved (CAPTCHA) and building the conceptual framework based on the analyzed concepts. A thorough understanding of relevant concepts such as evolution of CAPTCHAs, various CAPTCHA schemes, usability issues experienced by users, distinguishable usability features, and frameworks for examining usability are essential to gain comprehensive understanding of the phenomena and to develop the framework. The major phases involved in building such a conceptual framework (Jabareen 2009) are: (1) identifying all data sources related to the phenomenon, (2) reading and analyzing the literature collected, (3) identifying the concepts, (4) deconstructing and categorizing the concepts, (5) integrating the similar concepts, (6) building the conceptual framework, and (7) validating the framework. In this paper, we address the first six phases of the methodology.

Empirical evidence on the practical issues confronted by users when solving CAPTCHA challenge was collected from findings reported in the peer-reviewed literature. Through reviewing literature, we gathered evidences to form the basis for developing a list of applicable usability features and concerns. These identified features and concerns laid the foundations for developing the holistic model of CAPTCHA usability.

HOLISTIC MODEL OF CAPTCHA USABILITY

A review of multidisciplinary literature on CAPTCHA and its usability reveals the lack of a comprehensive framework for understanding the phenomena under consideration. There are few frameworks that enlist the factors affecting CAPTCHA usability (C. Fidas et al. 2015; Yan and El Ahmad 2008). These frameworks were not developed using systematic approach, did not utilize available empirical data, did not consider the impact of technological advances, nor are they applicable to variety of CAPCHA schemas. In this section, we present a theoretical conceptual framework that is based on empirical evidences reported in the literature obtained through qualitative and grounded theory approach described in Jabareen (2009).

CAPTCHA being a challenge response test, the difficulty of the challenge presented is escalated when combined with bad user experience. It is often believed that when considering both security and usability, one of these must be compromised and there is essentially a trade-off between the two. However, that is not necessarily the case. Yee (2004) stated that conflicting security and usability goals can be solved by effective incorporation of these goals in the design process. The holistic model formed after understanding the security and usability goals of CAPTCHA also focuses on the various design factors that could be considered without compromising security and user experience of the challenge response test. We reviewed relevant literature to identify relevant design and conceptual difficulties in CAPTCHA usability for constructing the holistic model. Figure 1 depicts the holistic model and a brief description of the various identified concepts is listed below.

Content Genericity

CAPTCHA is one of the most prevalent, widely used security measure on the Web. CAPTCHAs are used to block automated software/bots from accessing secured functionalities such as retrieving data from the Web, signing up or registering for a web application, and downloading documents. The advent of World Wide Web enabled easy access of repository of information/data to anybody in the world irrespective of their locations. The web applications are built to be accessed from all over the world and access to these applications must not be constrained because of the lack of knowledge about a specific language or culture. Hence, it is important to consider the genericity of CAPTCHA challenge responses and allow users to take these challenges regardless of their geographic, culture, or content knowledge.

Language

Research studies by Banday & Sheikh (2013) and Tangmanee & Sujarit-apirak (2012) show the difficulties and constrains a language poses to a non-native user. The accessibility of regional websites can be constrained because of the usage of English language based CAPTCHA's. The study resulting from (Bursztein et al. 2010; C. Fidas and Voyiatzis 2013) show that even users with basic knowledge of English struggle to solve the Latin challenges. It has to be noted that one of these studies (Bursztein et al. 2010) took place in the US. Yet the study found that despite these participants being bilingual, Latin CAPTCHAs are harder for them to solve. These results show that an option of providing native language CAPTCHA should be considered or an equivalent option with that of universal appeal (like a mathematical or image schema). While designing the challenge response test, it is very critical to consider the barriers posed by the language.

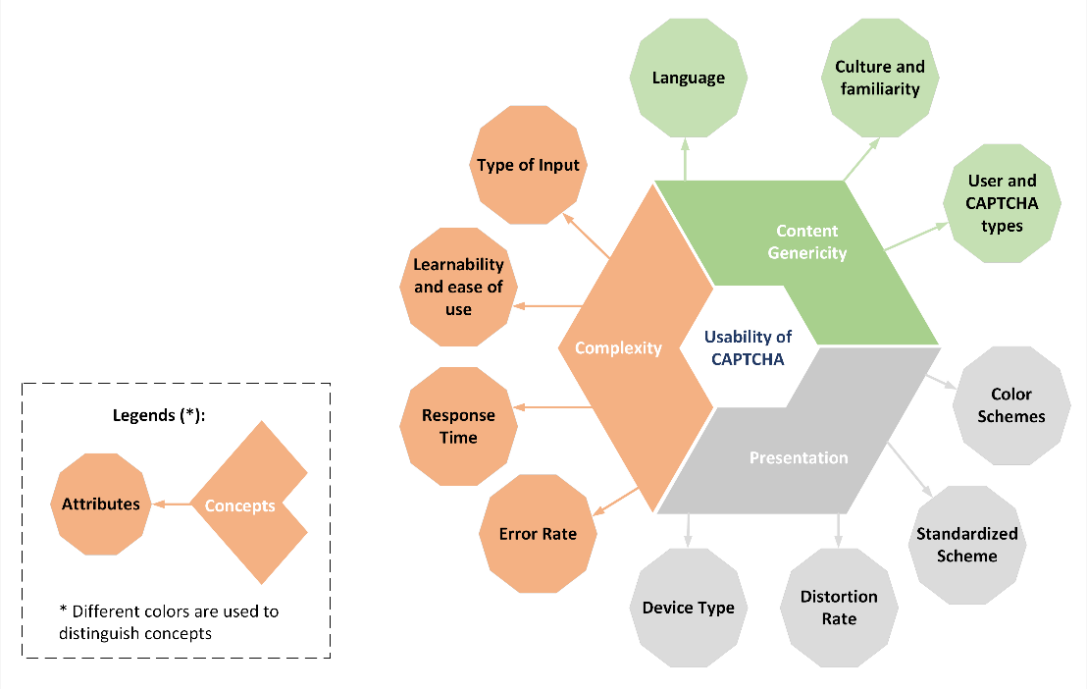

Figure 1. Holistic Model for CAPTCHA Usability

Culture and Familiarity

Challenge response tests are sometimes based on the human comprehension on road signs and objects which are presumed to be popular, known, familiar, or common among people. Similar to language, these are not generic in nature and things that are assumed to be a common knowledge may be in fact common only in certain specific countries/ regions (mostly in developed nations) (Kelly 2013; Morgan 2000; Onibere et al. 2001). Identification of street signs might not be in everybody's familiar context. Representation of street signs varies from country to country. This coupled with a below par English reading skill, aggregates the difficulty in solving these kinds of CAPTCHA. Designers have to consider designing CAPTCHA's with objects that are easily recognizable and familiar among all users irrespective of any culture or language. For example, animal images, geometric shapes, or other simple entities that are globally recognized.

User and CAPTCHA Types

Users from numerous demographic groups access the Web including disabled individuals. The rationale of making CAPTCHA challenges generic across language and culture is applicable to these varied set of demographic groups too. Alternative options to solve these challenges in case of visual impaired or any other disability should be strongly considered while designing CAPTCHAs. Failure to abide by content genericity factors would make CAPTCHAs in violation against the Web Accessibility Initiative guidelines (WAI-W3C 2017); as these are not mere steps to improve the usability but to provide availability and access to the resources.

Presentation

Appropriate presentation of contents is a direct reflection of a system usability. Presentation is one of the primary dimensions of web application usability (Costabile et al. 2005). Existing frameworks on CAPTCHA usability also address the presentation aspect of contents used in a challenge response test (C. Fidas et al. 2015). Depending on the types of CAPTCHA scheme used, application of an appropriate and effective presentation plays a vital role in easing the learnability and usability of CAPTCHAs.

Color Schemes

Colors enhance a design and can be used to quickly get the user's attention. Color variations increase the usability in most cases as different colors can be used to get the user's focus on various functionalities, thus enhancing the user interface designs (Ahmad et al. 2012). However, Ahmad et al., (2012) show how colors can complicate the readability of CAPTCHA's. Even though the usage of colors in CAPTCHA's can facilitate recognition, using simple color schemes or avoidance of color schemes can also accomplish the job effectively. Google, reCAPTCHA as well as Microsoft's CAPTCHA, are examples of simple

CAPTCHA designs without using any colors. So, designers have to consider the usage of color as a significant factor while designing a CAPTCHA.

Standardized Scheme

Currently, the majority of CAPTCHA schemes utilize texts, images, and audios in designing the challenge response tests. Variations among these schemes are substantial and sometime users need to learn how to solve different types of CAPTCHA schemes. Imposing a standardized scheme would minimize the required learning effort while improving user experience of CAPTCHA. Since there is no single standard in use currently, designers can opt for the most popular choice of CAPTCHA scheme to ensure familiarity among users. Text-based CAPTCHA is the widely used scheme but advances in computer vision have made them vulnerable (Nayeem et al. 2014). Consequently, image-based CAPTCHAs are gaining popularity and are known to perform better among humans in comparison to audio-based schemes (Bursztein et al. 2010). We suggest designing a hybrid standardized scheme that is easy for humans but harder for bots.

Distortion Rate

CAPTCHA designers employ distortion and/or noise within the challenge response tests to make it harder for bots to detect patterns. However, excessive application of distortion will make it hard for humans to detect patterns as well. For example, in case of text-based CAPTCHAs, accurately identifying distorted characters is harder especially for a non-native user. Multiple studies have stressed the importance of applying the right amount of distortion (Naor 1996; Yan and El Ahmad 2007). Distortion also makes it hard to read certain characters (like "o" and "0") and distinguish single character from set of characters (distortion of "cl" makes it look like "d") (Yan and El Ahmad 2007). This results in several wrong attempts by a legitimate user thus burdening both the user and the system.

Device Type

A study conducted by Wismer et al., (2012) on the usability of CAPTCHA's on Apple iPad devices shows users prefer CAPTCHAs involving touch inputs as opposed to audio inputs. Their findings reveal that users performed better with touch inputs as they had lower errors and took less time to complete CAPTCHA challenge. The presentation of a CAPTCHA on mobile devices, tablets and iPads might be very different to how a CAPTCHA appears in a desktop machine. Text and image CAPTCHA's might be even more difficult when viewed in a smaller screen. The usage of CAPTCHA's in these devices has to take output (screen size) and input (touch vs audio) mediums into consideration. With the growth of smartphone and tablet devices, the type of device used to access web resources should also be a critical factor of consideration while designing a CAPTCHA.

Complexity

The degree of complexity directly reflects on the usability of the system. Human interaction proof tests posed by CAPTCHAs have become solvable by bots due to advancements with computer vision and machine learning technologies. Thus, CATPCHA designers are increasing the complexity of CAPTCHA challenges while scarifying the usability (Banday and Shah 2011; Chandavale et al. 2009; Mori and Malik 2003). Even though security supersedes usability, it is important to strike a balance between the two. Designers can take below described factors into consideration to determine degree of complexity of CAPTCHA challenges.

Error Rate

The study by (C. A. Fidas et al. 2011) shows that despite users being familiar with CAPTCHAs, only 48% of the users were able to solve the CAPTCHA challenge in their first try. The reason for such unsuccessful attempt could be any of the factors listed above in this section. Irrespective of the reason, such repeated unsuccessful attempts cause inconvenience to the users, not to mention the added weight on the system to generate more challenges. The number of tries required to solve the challenge is a direct reflection of the complexity posed by the CAPTCHAs (C. A. Fidas et al. 2011; Yan and El Ahmad 2007). Thus, designers should strive to develop challenge response tests that can be solved by humans in their first attempt.

Response Time

Response time is the time taken by the users to solve a CAPTCHA challenge. Even without any errors, users might take considerable time to solve a challenge because of the complexity it may pose in terms of readability (Sauer et al. 2008). The delay could be because of distortion or difficulty with interpreting an audio (especially for non-native users) or the need for additional aid to solve the CAPTCHA (Sauer et al. 2008). The user's goal is to gain access to the website not to solve these challenges. The more time users spend to solve these challenges, the more frustration they will have, which may lead to bad user experience. Bursztein et al. (2010) collected over 5000 CAPTCHAs containing 21 schema variations and requested humans to solve those CAPTCHAs via Amazon's Mechanical Turk. Based on the study findings, they suggest that 10 seconds

should be considered as an optimal response time and 20 seconds or more should be considered as substantial burden on users. Thus, we recommend designers to ensure that users can solve CAPTCHA challenge within 10 seconds in the first attempt and if additional attempts are required then the total expected time should not cross 20 seconds.

Learnability and Ease of Use

Learnability can be defined as a "Measure of how easily the users can accomplish a task in their first trial. How easily can they learn and adopt to the design such that they accomplish the task quickly in the next consecutive trials." (Yan and El Ahmad 2007). Learnability and usability go hand in hand. These two factors are harmonious, and learnability is considered to be an important component of usability (Yan and El Ahmad 2007). Designers should use CAPTCHA challenges that humans can easily learn to identify the patterns and quickly solve it.

Type of Input

Study on effective usability features (Pakdel et al. 2011) shows that users find CAPTCHAs expecting inputs from mouse to be much easier compared to challenges requiring keyboard entries. Another study supports this evidence (Wismer et al. 2012) of inputs on mobile device, showing touch inputs were much easier when concerning CAPTCHAs. Considering these empirical evidences, designers should consider CAPTCHAs that makes use of mouse and/or touch input methodologies.

CONTRIBUTIONS

The holistic model constructed in our study is essentially derived from secondary empirical evidences on the usability of CAPTCHA. Most of the previous works on CAPTCHA usability frameworks (C. Fidas et al. 2015; Yan and El Ahmad 2008) were not developed using appropriate methodological approach and do not consider the empirical evidences reported in the literature. Our framework is based on a thorough review of the published literatures. We believe this framework can help designers and researchers make sense of the challenges associated with balancing the effectiveness and the usability of CAPTCHAs.

CONCLUSION

CAPCTHA is a widely used security measure that is designed to distinguish humans from bots, in order to prevent unauthorized access to websites which would result in exploiting the Web resources. Initially designed to be an easy and effective mechanism of security, CAPTCHAs have turned quiet challenging with the advent of pattern recognition and machine learning algorithms. In this work, we try to capture factors of CAPTCHA that can cause difficulties in usage. We conducted a systematic review of literature to identify characteristics of CAPTCHA that influence the usability, and developed a conceptual framework that categorize these factors. We believe this framework will aid researchers and designers by making them aware of the most crucial characteristics of a CAPCTHA that provides good user experience.

REFERENCES

1. Ahmad, A. S. E., J. Yan, and W. Y. Ng. (2012). CAPTCHA Design: Color, Usability, and Security, *IEEE Internet Computing* 16, 2, 44-51.

2. Banday, M. T., and N. A. Shah. (2011). A Study of CAPTCHAs for Securing Web Services, *International Journal of Secure Digital Information Age* 1, 2, 66-74.

3. Banday, M. T., and S. A. Sheikh. (2013). Design of CAPTCHA Script for Indian Regional Websites, *Proceedings of the Security in Computing and Communications,* August 22-24, 2013, Mysore, India, 98-109.

4. Bursztein, E., S. Bethard, C. Fabry, J. C. Mitchell, and D. Jurafsky. (2010). How Good are Humans at Solving CAPTCHAs? A Large Scale Evaluation, *Proceedings of the IEEE Symposium on Security and Privacy,* 16-19 May 2010, Berkeley/Oakland, CA, USA, 399-413.

5. Chandavale, A. A., A. M. Sapkal, and R. M. Jalnekar. (2009). Algorithm to Break Visual CAPTCHA, *Proceedings of the Second International Conference on Emerging Trends in Engineering Technology,* 16-18 December 2009, Nagpur, India, 258-262.

6. Costabile, M. F., M. D. Marsico, R. Lanzilotti, V. L. Plantamura, and T. Roselli. (2005). On the Usability Evaluation of E-Learning Applications, *Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences,* 6 January 2005, Big Island, HI, USA, USA, 6b.

7. Fidas, C. A., A. G. Voyiatzis, and N. M. Avouris. (2011). On the Necessity of User-Friendly CAPTCHA, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* May 07 - 12, 2011, Vancouver, BC, Canada, 2623-2626.

8. Fidas, C., H. Hussmann, M. Belk, and G. Samaras. (2015). iHIP: Towards a User Centric Individual Human Interaction Proof Framework, *Proceedings of the Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, April 18 - 23, 2015, Seoul, Republic of Korea, 2235–2240.

9. Fidas, C., and A. G. Voyiatzis. (2013). On Users' Preference on Localized Vs. Latin-Based CAPTCHA Challenges, *Proceedings of the Human-Computer Interaction – INTERACT*, September 2-6, 2013, Cape Town, South Africa, 358-365.

10. Jabareen, Y. R. (2009). Building a Conceptual Framework: Philosophy, Definitions, and Procedure, *International Journal of Qualitative Methods* 8, 4, 49-62.

11. Jain, S., and B. Sivaselvan. (2012). Usability Aspects of HCI in the Design of CAPTCHAs, *Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research*, 18-20 December, Coimbatore, India, 1-4.

12. Kelly, M. (2013). A Systematic Scoping Investigation of Cross-Cultural Visual Communication Design, Doctoral thesis awarded by Monash University, .

13. Morgan, K. (2000). Cross-Cultural Considerations for Simulation-Based Learning Environments, *Simulation & Gaming* 31, 4, 491-508.

14. Mori, G., and J. Malik. (2003). Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA, *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 18-20 June 2003, Madison, WI, USA, 141 vol.1.

15. Moni Naor. (1996). *Verification of a human in the loop or Identification via the Turing Test*, http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human.pdf, Retreived on: December 27, 2017.

16. Nayeem, M. T., M. M. R. Akand, N. Sakib, and M. W. U. Kabir. (2014). Design of a Human Interaction Proof (HIP) using Human Cognition in Contextual Natural Conversation, *Proceedings of the IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing*, 18-20 August 2014, London, UK, 146-154.

17. Onibere, E. A., S. Morgan, E. M. Busang, and D. Mpoeleng. (2001). Human–computer Interface Design Issues for a Multi-Cultural and Multi-Lingual English Speaking Country — Botswana, *Interacting with Computers* 13, 4, 497-512.

18. Pakdel, R., N. Ithnin, and M. Hashemi. (2011). CAPTCHA: A Survey of Usability Features, *Research Journal of Information Technology* 3, 4, 215-228.

19. Sauer, G., H. Hochheiser, J. Feng, and J. Lazar. (2008). Towards a Universally Usable CAPTCHA, *Proceedings of the Symposium on Accessible Privacy and Security (SOAPS)*, July 23-25, 2008, Pittsburgh, PA, 1-4.

20. Singh, V. P., and P. Pal. (2014). Survey of Different Types of CAPTCHA, *International Journal of Computer Science and Information Technologies* 5, 2, 2242-2245.

21. Sivakorn, S., I. Polakis, and A. D. Keromytis. (2016). I Am Robot:(Deep) Learning to Break Semantic Image Captchas, *Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P)*, 21-24 March 2016, Saarbrucken, Germany, 388-403.

22. Tam, J., J. Simsa, S. Hyde, and L. V. Ahn. (2009). Breaking Audio CAPTCHAs, *Proceedings of the Advances in Neural Information Processing Systems*, December 6 – 8, 2009, Vancouver, B.C., Canada, 1625-1632.

23. Tangmanee, C., and P. Sujarit-apirak. (2012). Attitudes Towards CAPTCHA: A Survey of Thai Internet Users, *Journal of Research and Practice in Information Technology* 44, 4, 441-455.

24. von Ahn, L., M. Blum, and J. Langford. (2004). Telling Humans and Computers Apart Automatically, *Communications of the ACM* 47, 2, 56–60.

25. WAI-W3C. (2017). *Web Accessibility Initiative (WAI)*, https://www.w3.org/WAI/, Retreived on: December 28, 2017.

26. Wismer, A. J., K. C. Madathil, R. Koikkara, K. A. Juang, and J. S. Greenstein. (2012). Evaluating the Usability of CAPTCHAs on a Mobile Device with Voice and Touch Input, *Proceedings of the Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, October 22-26, 2012, Boston, MA, USA, 1228-1232.

27. Yan, J., and A. S. El Ahmad. (2007). Breaking Visual Captchas with Naive Pattern Recognition Algorithms, *Proceedings of the Annual Computer Security Applications Conference*, 10-14 December 2007, Miami Beach, FL, USA, 279-291.

28. Yan, J., and A. S. El Ahmad. (2008). Usability of CAPTCHAs Or Usability Issues in CAPTCHA Design, *Proceedings of the Proceedings of the 4th Symposium on Usable Privacy and Security*, July 23 - 25, 2008, Pittsburgh, PA, USA, 44–52.

29. Yee, K. (2004). Aligning Security and Usability, *IEEE Security Privacy* 2, 5, 48-55.