Security Guidelines for the Development of Accessible Web Applications through the implementation of intelligent systems

Edward Rolando Núñez Valdez[2], Oscar Sanjuán Martinez[1], Gloria García Fernández[2], Luis Joyanes Aguilar[2] and Juan Ml. Cuevas Lovelle[1]
[1] *University of Oviedo, Computer Science Department, Oviedo, Spain*
[2] *Pontifical University of Salamanca, Computer Science Faculty, Madrid, Spain*

Abstract - Due to the significant increase in threats, attacks and vulnerabilities that affect the Web in recent years has resulted the development and implementation of tools and methods to ensure security measures in the privacy, confidentiality and data integrity of users and businesses. Under certain circumstances, despite the implementation of these tools do not always get the flow of information which is passed in a secure manner. Many of these security tools and methods cannot be accessed by people who have disabilities or assistive technologies which enable people to access the Web efficiently. Among these security tools that are not accessible are the virtual keyboard, the CAPTCHA and other technologies that help to some extent to ensure safety on the Internet and are used in certain measures to combat malicious code and attacks that have been increased in recent times on the Web. Through the implementation of intelligent systems can detect, recover and receive information on the characteristics and properties of the different tools and hardware devices or software with which the user is accessing a web application and through analysis and interpretation of these intelligent systems can infer and automatically adjust the characteristics necessary to have these tools to be accessible by anyone regardless of disability or navigation context. This paper defines a set of guidelines and specific features that should have the security tools and methods to ensure the Web accessibility through the implementation of intelligent systems.

Keywords: PSDCA, PSDAWA, PSDTVA, Web Security, Web accessibility, CAPTCHA, Virtual keyboards, Intelligent Systems.

I. INTRODUCTION

THE use of the Internet every day it becomes more imperative to conduct the activities of everyday life, where we can make all types of transactions from our computer (Purchases, Sales, banking, exchange of information (videos, photos, music, voice and so on.). and a lot of different types of transactions that are done daily via the Web) and the boom that is taking social networking (Collaborative Web or Web 2.0) make every day the content of the Web will increase substantially due the collaboration of those Internet users who are mostly those who use, distribute, share and eat the contents of the Web. Due to this significant increase in the use of the Web in its full context, we have the following question Do all persons with disabilities (permanent or temporary) have access to such content? Obviously the answer is Not because there are significant barriers to accessibility on most web sites that hinder access to such content to a large number of people worldwide who have disabilities.

Referring to Disabilities the World Health Organization, known more commonly as WHO in [1] defines it as "Is an umbrella term, covering impairments, activity limitations, and participation restrictions. Impairment is a problem in body function or structure; an activity limitation is a difficulty encountered by an individual in executing a task or action; while a participation restriction is a problem experienced by an individual in involvement in life situations". This means that any disabled person can use efficiently the Web so that you can access information from the accessed Web resource without any limitations that may be caused by some deficiency, either handicap or disability of vision, hearing, physical, cognitive, neurological, speech, or environmental technology in a natural way or through the use of assistive technology.

Assitive technologies can be defined according to ISO 9999 in [2], as "Products, Tools, and Equipment or technical systems manufactured specifically for use by people with disabilities and/or older; available on the market to prevent, compensate, mitigate or neutralize a diversit".

A Web accessible not only benefits people with disabilities as above, but also to individuals and organizations according to certain circumstances transitional or definitive access to the Web but are limited either because of knowledge, experience, language, hardware, software, slow connections to the Web, geographic location, or simply people who have an accident that has caused some physical fracture and cannot use the Web as usual.

On the other hand, Internet users who currently use the Web not only affected by the problems presented by the accessibility to Web applications, but also security issues that

This work was supported in a collaboration by the University of Oviedo and Pontifical University of Salamanca.

affect the privacy, confidentiality and integrity of data transmitted through on the Web, causing considerable economic losses to individuals and companies that are victims of attacks and malicious activities carried out by cybercriminals.

Security in web applications aimed at satisfying the needs of information transmitted via the web in precise, concise, timely, confidential and secure, ensuring the protection and privacy of information during the exchange and transmission of information between the client and server.

The boom that has taken in recent years the use of the Internet and the need to transmit information and conduct transactions via the Web led to a number of threats and attacks (phishing, malware, virus, spam, and so on.) that compromise the security of information and computational resources of clients and businesses. These attacks and threats are made by unauthorized persons and is usually performed on vulnerabilities exist in web applications. To ensure the exchange of information and conduct secure transactions through the Web and ensure that users are free from any threat either intersection, interruption, alteration or invention of information that may be caused by unauthorized persons is use different security mechanisms and techniques for solving these problems that affect the security of transmitting information across the Web.

The statistics on security in the Web show that is an immediate need to use technology in some way help to control or minimize these attacks and ensure greater security in the protection of confidential data from users, for them there are many tools security on the Web that are used to protect user information from possible attacks of malicious code such as the Virtual Keyboard, the CAPTCHA, and so on.

The problem we found on the Web at present is that many of these security methods and tools that are used to ensure the protection of confidential information to some degree provide security in the transmission of information, but it´s may not offer adequate levels of accessibility to an application can be used by anyone regardless of their navigation and therefore impossible for any person with a kind of permanent or temporary disability cannot access content and services available in the Web. For these reasons a study of the security tools that affect web accessibility, analysis tools and methods used by security institutions dedicated to e-commerce, online banking and other activities on the Web.

This paper raises a number of criteria or recommendations to be followed the Web applications to ensure that the security tools that are accessible, and that through the implementation of intelligent systems is to analyze, interpret and adapt the characteristics of the devices and tools (hardware & software) that are used by users to navigate and interact on the Web in different contexts, allowing in this way to achieve a convergence between security and Web accessibility, ensuring that no one act over another.

II. SECURITY TOOLS THAT INFLUENCE ON THE WEB ACCESSIBILITY.

Nowadays on the Web there are a number of tools and security methods that are used to ensure privacy, confidentiality and data integrity to protect the users and enterprises from threats and attacks that affect the Web. Many of these tools and methods influence web accessibility since they are not accessible to persons with disabilities.

To Symantec in [3] the Web is now the primary conduit for attacks and theft of confidential information and that managers and vendors of tools for network security have fortified the perimeters defenses with the use of tools such as firewalls, intrusion detention systems and prevention systems, so instead of trying to penetrate the networks attackers have centered most of their techniques to the various attacks computers via the Web.

These security tools that are not accessible are the virtual keyboard, and the CAPTCHA and others, for which discusses and defines a set of guidelines and characteristics that contribute to making these tools and methods can be accessed by anyone regardless of disability or navigation context. These tools are used as countermeasures to minimize the attacks that are stealing confidential information from users. When we speak of countermeasures according to OWASP in [4] is any defensive technology that is used to detect, detain or deny attacks in applications.

A. CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

CAPTCHA is a security tools or program that is automatically generated from a test or challenge to an answer that humans are able to resolve but the machines can not.

These security programs which consists of decoding a text is composed of distorted images to be decrypted to enter or register on the website, and some researchers from the Carnegie Mellon University in Pittsburgh who are the pioneers in developing and implementing this method say that a machine is not able to understand and decode the text correctly and that only a human could achieve.

These distorted images that the majority of cases are not understood by humans because of the high degree of complexity that is generated with the text and that is a serious problem for Web Accessibility is not only because people with disabilities cannot access them, but also non-disabled person would have trouble identifying and understanding the text of the distorted image. See Figures 1, 2, are examples of distorted images that require much effort to understand and identify its contents.

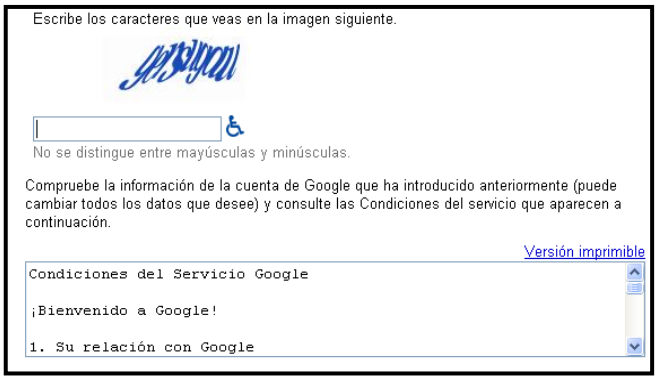

Figure 1 CAPTCHA generated by Gmail
Source: Gmail

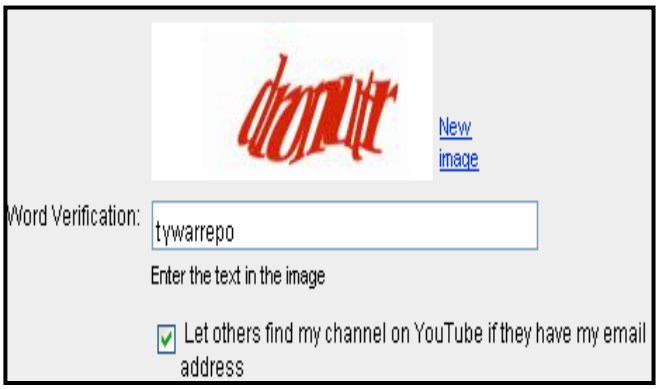

Figure 2: CAPTCHA generated by Youtube
Source: Youtube

The CAPTCHA is a security tool on the web but is not the panacea of anti-spam and Web security say W3C is a security tool that provides its bit for the security and privacy of data on people and businesses on the Web. In the work [5] the authors mentioned some important features that these tools have by definition:

- Code and data used by a CAPTCHA should be publicly available. This indicates that a CAPTCHA to ensure security, because although they know exactly how it is very difficult for someone to develop a software that can pass the test generated by a CAPTCHA. All that was hidden in the tool is the randomness used to generate the evidence.
- The CAPTCHA is a Turing tests automated. This test is to distinguish humans from one computer to be achieved through a series of questions in which a judge has to identify one another. At the original trial judge in Turin is a human and in the CAPTCHA the judge is a computer.
- Are completely automated. This creates a number of benefits both in cost and reliability as it does not require any maintenance or human intervention for its implementation and use.
- The breaking of a CAPTCHA is a problem in artificial intelligence. The problem of breaking a CAPTCHA is a problem in artificial intelligence, because as this uses an public algorithm the problem is not the complexity of breaking an algorithm secret.

This is questioned by many features as some research has succeeded in breaking CAPTCHA systems some results which indicate that these systems can be defeated by computers with 88% and 100% accuracy using optical character recognition [6]. In the work [7] the authors say that the CAPTCHA in general are designed to prevent bots (computer programs that attempt to mimic human behavior through the implementation of various functions) abuse of Internet services. These bots are driven to sell and register thousands of email accounts per minute, sending millions of spam messages. With these infiltrating chat rooms, collecting personal information and post links to promotional Web sites. They also generate worms, break password systems and invade the privacy of information. These automated Bots are a real problem for the privacy and security of information on the Web so it is very important to resolve this problem through the use of security tools (like CAPTCHA), but without affecting the other important areas on the Web, such as accessibility and usability. In the works [8] [9] the authors say that the CAPTCHA have various applications in use as a tool to support security on the Web, these may be appointed as follows:

- Protection of registration of Web sites. The majority of companies that offer e-mails using CAPTCHA to ensure that only humans can get a free email account and thus avoid automated script that can create thousands of accounts automatically.
- Protection of email addresses of Scrapers. The CAPTCHA provide an effective mechanism to hide the email address of Scrapers through the idea of requiring users to solve a CAPTCHA before showing your email address.
- Prevent dictionary attacks. The CAPTCHA can also be used to prevent dictionary attacks in password systems by the idea that instead of locking the password after a number of start of section without success, the user is encouraged to solve a CAPTCHA to validate the user and prevent an attacker to block accounts at will.
- Search engine bots. Sometimes it is desirable to maintain the web pages not indexed to prevent other people can find it easily. There is an html tag to prevent search engine bots from reading web pages. The label, however, does not guarantee that the robots do not read a web page
- Worms and spam. The CAPTCHA also offer a plausible solution against email worms and spam: "I will only accept an email if you know that there is a human being behind the other team.". A few companies are already marketing this idea.
- Preventing comment spam in blogs. Most bloggers are familiar with programs that provide false feedback, usually with the aim of raising the rank in search engines for some sites. By using a CAPTCHA, only a human can enter comments on a blog. There is no need for users to register before entering a comment.
- CAPTCHA tests are based on open problems in

artificial intelligence (AI): In the paper [8] the authors say "*decoding distorted images of text, for example, goes far beyond the capabilities of modern computers. Therefore, the offer CAPTCHA challenges defined for AI community, and lead to security researchers, and other malicious programs, to advance the work in the field of artificial intelligence. CAPTCHA, therefore, is a win-win situation: for if a CAPTCHA is broken and there is no way to differentiate humans from computers then a problem of artificial intelligence is resolved.* "

1) Accessibility problems in the CAPTCHA.

Because these tools are used and implemented to ensure some level of safety on the Web in many areas, the reality is that although they are designed and intended to be interpreted by human beings to access protected resources on the Web, really these prevent them can be accessed and understood by humans and especially for people with disabilities such as people with hearing, visual or learning disabilities like dyslexia, but they can be used in some cases solutions artificial intelligence such as voice recognition software, characters or images to access the CAPTCHA.

Another problem that adds to the accessibility of CAPTCHA is to be a tool designed specifically to be performed by beings humans, assistive tools used by people with disabilities such as Braille keyboards and other tools that are used to access the Web cannot interpret the contents of the CAPTCHA, and so these tools are locked at the time they are faced with this security system and therefore the user can not access the web resources.

This is impossible for people with disabilities to interact with freedom on the Web as they are with the disadvantages that they cannot do business online, participate in social networks, etc. create accounts., Which leads to the idea of involving users to the web what is now known as Web 2.0 is affected by the idea of these types of security systems do not consider people with disabilities as "human beings" but as "machines" because the block resources, or block access to the same users are being treated like machines.

2) Security guidelines for the development of accessible CAPTCHA (PSDCA)

Although W3C in the document [6] recommends the use of other systems of access control mechanism that can be more accessible and more effective as the heuristic checks for the presence of users Robot by collecting volumes of data, IP addresses, signatures and other information can be collected at the time of the user to access the Web resource, or the spam filter used by the applications of "Hot Words" to indicate the content of spam, or other Bayesian filtering to detect patterns consistent with the spam, as well as the use of Logical Puzzle, sound output, biometric systems, etc.

The reality is that if we can develop a security system based on the methodology CAPTCHA in combination with any of the aforementioned safety systems and standards for Web accessibility and security that exists in today's market, taking into consideration that the it does not develop at the expense of other technologies that today and tomorrow are the cornerstone of development and advancement of the Web such as accessibility, usability, Web 2.0, the Semantic Web and so on. Not only combat the problems of spam that is the main idea that was conceived with the CAPTCHA, but other security problems currently affecting the security and privacy of the people as the problem of PHISHING that one of the security problems which currently affects millions of more users and causes economic losses to many individuals and businesses.

The reality is that just as security is not possible to achieve 100% accessibility to the Web because there are cases of people with disabilities who require higher requirements than others to access the Web, such as for example a person who is blind, deaf mute is almost impossible for a person with these types of disabilities combined access to the Web, because the major iteration of the Web are based on sight, sound and voice recognition. So that it can try to combine different options to ensure that increasing numbers of people with disabilities can access the Web and this is done by a series of recommendations for systems that rely on CAPTCHA can minimize problems Accessibility facing at the moment but this can be achieved with the implementation of intelligent systems to assess, collect and process information from different devices (hardware and software) involved in the process of user interaction with the Web by combining this system with other security features and built-in properties and by combining it with other security systems. Here we mention some features or capabilities that must have a security system based CAPTCHA to be accessible:

B. Virtual Keyboard

Currently most of the attacks and malicious code created in the last few months are going to the Web with the purpose of stealing confidential information and passwords to users from cyber criminals for the purpose of financial gain. According to statistics from the threats and attacks on the Web in recent months published by Symantec in [3] Trojans represent the highest percentage (71%) of malicious codes that are distributed over the Internet. In the same way phishing attacks is the malicious activity that has increased in recent years, specifically increased 167% compared to last survey. These attacks are designed to steal confidential user information, specifically data related mostly to personal information, passwords, credit cards, and so on., That is private information that are used mostly in electronic commerce, online banking, and so on. Another important fact is that most of these attacks are directed at a high rate to the financial area, specifically 66% of all attacks were directed this area.

These statistics show us that it is an immediate need to use some form of technology that contribute to combat or

minimize these attacks and to ensure greater security to protect confidential data from users is that many of these banks use the “Virtual Keyboard" to try to minimize these types of attacks specifically protected from phishing attacks.

The virtual keyboard: is a tool that allows users to enter sensitive data in the Web securely, without the need to use a physical keyboard, thus avoiding a keylogger that can capture keystrokes on the keys and make a phishing attack. (See Figure 3 and Figure 4)

Figure 3: The Virtual Keyboard used by Santander Group

Figure 4: The virtual keyboard used by Caixa Sabadell Spain

This is a security system that protects you from phishing attacks confidential information of users to a certain level, because there are trojans that can record or take pictures of each of the movements of the cursor keys and thus steal confidential information from users . But despite this, The virtual keyboard in some form helps to security on the Web, but not working with the Web Accessibility because the virtual keyboards are not accessible to persons with disabilities.

1) Advantages and disadvantages of virtual keyboards on the web

Like other security tools the virtual keyboards are advantages and disadvantages to consider in determining the feasibility of using this tool in web environments.

Advantages:

- The use of virtual keyboard protects users from malware type Trojans key logger which specifically capture the keystrokes of keys on a normal keyboard can steal confidential information from the user.
- Can be implemented as device entries in the given case a failure of the normal computer keyboard.
- Provides more sense of security to users.

Disavantages:

- Are not accessible to persons with disabilities.
- Does not guarantee the protection of confidential information of Trojans that can record the movements of the cursor around the screen.

2) Security guidelines for the development of accessible virtual keyboard (PSDTVA)

The main problem with the virtual keyboard is not accessible to persons with disabilities so that the tool has a negative impact on safety and accessibility. Because it is a tool that helps combat the security problems that affect the Web and especially phishing attacks. Below are quoted some special characteristics that should be the virtual keyboard to be used as security tools and also be accessible to persons with disabilities:

- Allow access to keypad through assistive tools for people with motor disability. That a means that data capture can be through a mouse or a mouse adapted for people with disabilities.
- Allow user to change the contract size and the letters in each of the keys. For people with low vision disabilities.
- Providing a sound system for the virtual keyboard that could identify the letters of keyboard to move the mouse cursor over it. For people suffering from blindness.
- Give the virtual keyboard a word prediction system to expedite the processing capability that allows the text and reduce the number of keystrokes.
- Give the virtual keyboard a voice recognition system.

Other Guidelines and important features to make a virtual keyboard a feasible security tool and significantly increase the protection of the user before the attacks on the Web quote below:

- The virtual keyboard to scroll the screen in each keypress to prevent a key logger to capture the coordinates of the screen and see where we move when pressed with the mouse and click.
- Allow the keyboard to increase or decrease the contrast to make it difficult to display a short distance, and thus prevent anyone near the user can see the information you are typing.
- An important feature of this system security but that largely depends on the user and avoiding the theft of confidential data and the password of the user, is that the user enter data using combinations of movements, ie at the time Enter the password that the user can enter in part using a virtual keyboard and another using a standard input device.

For example if a key has 10 digits you can enter 5-digit using the virtual keyboard and 5 using the normal keyboard, which lets you have a trojan that captures keystrokes capture the key is not complete, or if a trojan records cursor movements not record all typed characters.

C. Security guidelines for the development of accessible web applications (PSDAWA)

As we have seen in previous issues of security problems we are facing today with regard to loss and theft of confidential information caused by threats and attacks on the Web are serious and the majority of problems are caused by malicious codes and activities such as phishing and Trojans that steal confidential information from users who perform transactions through electronic pages are devoted to electronic commerce or banking, These entities to ensure the protection of confidential information using security tools that provide security largely on the execution of transactions, but in many cases, these security measures are not accessible to persons with disabilities. In the above items mentioned some safety guidelines to make the CAPTCHA and virtual keyboards accessible, then cite some security measures and methods used by institutions engaged in commerce or electronic banking and also make several recommendations or criteria that should be continue to ensure that safety features are accessible, ie, not acting safety and accessibility at the expense of one another.

1) SSL Connection (Secure Socket Layer)

Connect using SSL encryption algorithm with a key of 64 bits, 128 bits, 256 bits and so on. provides a secure connection between the client and the server data processing company, ensuring that information security and integrity by avoiding travel to outsiders intercept, modify or steal the information.

Recommendations:

At the time the user is accessing a Web application that uses the SSL security protocol; this has to be able to tell the user that is going to make a secure connection with a secure server, indicating the following criteria:

- Indicate to which server you are connecting.
- Indicate institution belongs to the server.
- This information should be accessible to assistive tools.
- The information provided should be equipped with this sound for people with visual disabilities.
- Is this secure server where the user really wants to connect?.
- Would you be the victim of phishing attacks and accessing a server that is not the one that really wants to access?
- The certificate is valid?
- Is this certificate issued by a valid certificate authority?

In reality there are many questions that the user is performed when accessing the application, it is important that the user can easily find the answer to these questions in the most simple and straightforward as possible. For this is a series of recommendations to improve accessibility and access to key information.

Recommendations:

When the user is connecting to a secure server, the application must indicate the most visible and clearly as possible the most important data indicating that the certificate is being used in the connection is good, valid, and ensures the identity of the remote server.

Following or giving the following considerations:

- This should indicate that the digital certificate is issued by a valid certificate authority.
- Display data of the certification authority
- Show the effective date of the digital certificate.
- This information must be accessible by assistive tools.
- The information provided must be equipped with this sound for people with visual disabilities.
- The application should not require the user to click on the icon of the certificate (closed padlock or key) to view this information. Should be visible somewhere in the application that the user can view it without an extra effort

3) Mechanisms of secret keys

Banking institutions mechanisms secret keys used to secure user authentication, are usually composed of the following elements:

- User: Code that identifies the person, which may be a personal number or a personal identification document. (Passport, DNI, NIF, NIE, and so on.).
- Password: Code secret that together with user ID allows the authenticated in the Internet Banking. Many banks defined as numeric and not require the user to be a strong key (consisting of numbers, characters and special characters)
- Digital Signature: usually when making a transaction is requested by the user typing values on the random positions of the same, never to complete full signature of the key digital signature
- Password Confirmation: For some operation the user must confirm a key in the system that is sent through a mobile phone.

This safety mechanism ensures the privacy and security of people because they offer an effective mechanism for security concerns, but at certain points due to accessibility to Web using validation methods that are not accessible to persons

with disabilities and for people who do not own the means necessary to complete the identification and validation of the user.

In the case of the digital signature do not have methods to indicate to the user with blindness that position the firm to modify or to extend or adapt the size and color of the letters to people with low vision. The confirmation code is sent to user via SMS (see Figure 6) prevents some people complete the validation of the operation because it is a platform independent and completely separate from the application. This makes this form of validation is not accessible because it limited to certain users to perform operation. This method of validating user is not accessible in the following cases:

- For a blind person who cannot see the key on the mobile phone.
- The user does not have a mobile phone to receive the message.
- The user has mobile phone coverage but no because you're on the road (in another country and does not have automatic roaming).
- The user has the mobile switched off because the battery is discharged.
- Mobile phone was damaged and I need to make a transfer an account to make a purchase.

2) Server Authenticity Certificate:

The authenticity certificate ensures that the user is connected to a secure server. By indicating a closed padlock or key in the entire bottom of the browser (see Figure 5). This ensures that the user is connected to a secure server, but in reality the following questions arise.

Figure 6: Entry screen confirmation code sent by SMS

In reality there are many cases that make this type of user authentication is not accessible for many reasons are cited the following recommendations for improving accessibility in this authentication method. Recommendations:

- When you apply the digital key to the user, which is random positions requires the user to enter must have the following characteristics:
- The information must be accessible by assistive tools.
- The information provided must be equipped with sound for people who have visual impairments, indicating the positions at random and change the position in which the user's cursor at the time.
- Allow the user to change size and contrast the positions of the digital signature. For people with low vision disabilities or daltonism.
- Allow data entry via voice recognition devices, such as a microphone. For people with motor disabilities.
- An application should not rely solely on an external tool to operate, thus the customer must provide alternatives to ensure that in certain cases be able to access the application without any inconvenience. Ie, the application must have a signature confirmation that is not through SMS messages, such as a system of questions and answers set by the users is stored and the user is passed in encrypted form and that example is presented to the user through an alternate accessible CAPTCHA.
- Perform an authentication mechanism that combines security tools used in the Web, without external tools depend. Examples combine the properties of the virtual keyboard and perform the validation with an accessible CAPTCHA instead of a confirmation by the mobile device.
- These tools must be developed with open security standards such as safety standards based on XML.

III. CONCLUSION

The information described in this article see the need to use tool and security methods to ensure that information flows through the Web safely, due to the increase in threats, attacks and vulnerabilities affecting Web applications.

When performing the verification of the statistics in the documents [3] and [10] published by Symantec and Panda Labs on attacks, threats and vulnerabilities affecting security, it is determined that the majority of attacks target Web applications, specifically targeting the theft of confidential information users, and that 71% of malicious code developed in recent months relate to the Trojans, which increased 136% in the last half of 2007 compared with the first half of the year and 571% over the second half of 2006, just as the attacks on the Web that have increased are Phishing Attacks and everything-based Trojans Keyloggers are used to steal information, plus 66% of these attacks were directed at the financial sector.

Due to the result of these statistics this article focuses on some methods and tools of security that guarantee safety on the Web, which is located between two specific security tools that are used to combat such attacks as the "Virtual Keyboard "used to share the Trojans kind Keyloggers and "CAPTCHA " used to ensure that those who are accessing or requesting information on the Web is a human and not a robot.

For these tools, which are not accessible, they have some security weaknesses, but they are tools that ensure a certain level of security defined a series of guidelines and/or features that should have these tools and to help improve security the accessibility of them.

Although some experts recommend using other security mechanisms in place of the CAPTCHA and the Virtual Keyboard for the weaknesses that are related to security and accessibility. With the guidelines defined in this paper to improve these tools provide a valuable contribution to

improving both the accessibility and security of these tools and other security mechanisms used on the Web.

The reality is that problems or at risk from any tool to be used in your environment or as simple as it should not stop using, but try to improve and correct any problems that present. A very simple example is that with the development and progress that have taken over all these centuries of military weapons (machine guns, battle tanks, long-range missiles, and so on.). But the soldiers continued to use the most ancient and simple their safety, "The Knife". So what can be said of the security tools discussed in this article is that they are simple, have their disadvantages but somehow contribute to security, that's why we make the necessary recommendations for the definition and implementation of safety guidelines for developing accessible Web applications.

The use and implementation of these guidelines to help correct and combat effectively the various attacks and vulnerabilities affecting the security of Web applications and thus protect and guarantee the security of the transmission of confidential and valuable information for users, and while ensuring that anyone regardless of disability or browsing context can access and use these tools efficiently and safely.

REFERENCES

[1] World Health Organization WHO, "Health topics", <http://www.who.int/topics/disabilities/en/>, [consulted in March 2009]

[6] Roca Dorda, Joaquín *, Roca González, Joaquín * and Del Campo Adrián, María. E. **, "For technical assistance to Assistive Technology", * G.I " Industrial Electronics and Medical" (EIMED) Politécnica de Cartagena University (UPCT), ** National University of Distance Education (UNED) ETSII of Cartagena: <http://tecnoneet.org/docs/2004/2-12004.pdf>

[7] Symantec Corporation, "Symantec Global Internet Security Threat Report. Trends for July–December 07", Volume XII, Published in April 2008.

[8] Open Web Application Security Project (OWASP), "Security Countermeasure", <http://www.owasp.org/index.php/Category:Countermeasure>, [consulted in January 2009]

[9] Von Ahn Luis, Manuel Blum, and John Langford, "Telling Humans a Computer Apart Automatically", Communications of the ACM, February 2004/Vol. 47, No. 2, ACM 0002-0782/04/0200.

[10] World Wide Web (W3C), "Inaccessibility of CAPTCHA", <http://www.w3.org/TR/turingtest/>, November 2005, [Consulted in January 2009]

[11] Palo Alto Research Center, "PARC's CAPTCHA", <http://www2.parc.com/istl/projects/captcha/index.htm>, [Consulted in January 2009]

[12] Carnegie Mellon University, all rights "CAPTCHA: Telling Humans and Computers Apart Automatically", < www.captcha.net/>, 2000-2007

[13] Von Ahn, Luis, Blum Manuel, J. Hopper Nicholas, and Langford John, "CAPTCHA: Using Hard AI Problems For Security", Computer Science Dept., Carnegie Mellon University, Pittsburgh PA 15213, USA, 2 IBM T.J. Watson Research Center, Yorktown Heights NY 10598, USA, [Consulted in August 2008].

[14] Panda Security, Quarterly reports Panda Labs (2008 April-June), June 2008