NoProfiling: multiplatform application to avoid the profiling of email users

Olga Villagrán-Velasco, Carlos Hernández-Nava

Instituto Politécnico Nacional, IPN,
Unidad Profesional Interdisciplinaria en
Ingeniera y Tecnologas Avanzadas, UPIITA, México.
ovvingtel@gmail.com; hernandez.nava@gmail.com;
http://sites.google.com/site/hernandeznava/

Abstract. The goal of this paper is to present the development of a Web application and a Mobile application that avoid the profiling of email users generated by BOT-attacks. It was implemented the P protocol, for the first time, that uses a symmetric encryption system in order to cipher the content (plaintext) of the email with a private key. To share that key, this project generates CAPTCHA images, achieving that only a human can observe and read the private key and decipher the encrypted email (ciphertext), allowing to users ensure their information without having to acquire some knowledge about computer security or cryptography. Also, this work provides to P protocol the chance of controlling the CAPTCHA difficulty through its parameters (rotation, deformation and size of characters). Currently, exists techniques to maintain secure the email content, like PGP or GPG through asymmetric encryption or symmetric encryption based on digital signature scheme. However, these systems require knowledge of computer security and sometimes even cryptography. One advantage of this work, is that the users does not need to remember a password to access the email content, but this does not mean that safety decreases as each email has a different key. This process allows to keep users data safe from BOT-attack, considering that the information obtained by these attacks may be exposed to a third party without permission. This application also allows anyone, with a computer or mobile device and internet access, use it with the gmail, yahoo or outlook account.

Keywords: Security, Host attacks, Defense mechanisms

1 Introduction

When an email is sent, it is expected to contain confidential information regardless of it is a free email service. Today, software seeks patterns of words in the text, that is used for collecting information contained in email without the users are aware of this process, such being a method that generates user profiles of email addresses according to the type of information contained to define the interests, devices that perform this process are technically called BOT. The most

pp. 99–106; rec. 2015-08-15; acc. 2015-09-21

common BOT attacks are profiling of users, sending junk email and identity theft.

All types of profiling have in common the aim of collecting personal information from users and according to the analysis are classified. Mainly companies use this kind of technologies to commercial and banking purposes. e.g. Alice asks Bob, by email, to lend her some money to buy a laptop. Then the bot attacker analized the email's content. After that, bot attacker's own sold the information to some bank (because she needs a loan) and to a online store (because she wants to buy a laptop).

All this generate that email users privacy is violated and collected in the users profile become misused, as these profiles can be so specialized and detailed as the information you write in the email. Therefore, the issue focuses on these profiles are released, that is, if made public or they are stolen from companies that generate them, unleashing targeted attacks (e.g. theft identity). This problem has been presented in [1].

As a solution to the problem mentioned above, it was design and programmed a multiplataform application that includes a Web application and one for mobile devices. To enable email users to use the services of their provider and ensure that those who read the emails content is a person and not a bot attacker; all without the user having to configure some extra tool. To achieve this result, the P protocol was implemented using a symmetry encryption system [2]. The bot attackers have a few chances to access to encrypted user information avoiding performing a user profile.

2 Development

The P protocol is a private key algorithm that gives security concept applying CAPTCHA in order to authenticate users for a service. According to [3], it is not mandatory that a user becomes aware of security concepts to protect your information and because of it proposes using CAPTCHA image as a channel to exchange private keys securely. P protocol v. Figure 1 consists of:

- A message (M) and an encrypted message (C).
- A set of character (k) obtained from an alphabet (STR).
- A *HASH* function H: k → K that will become the key.
- An Encryption scheme E: K x M → C where K is the key.
- A CAPTCHA generator that use as its input characters of the set G(k).

The NoProfiling system is based on the P protocol, described above, and the architectural design is based on the MVC-1 pattern (Model-View-Controller) logic level, which associates the presentation and business logic as shown in Figure 2. In MVC-1 only one component is responsible for receiving and responding requests made by web browsers.

In a physical level, the architecture is based on cliente-server model. This model aims to separate the activities of the system user and those that are going to execute temporarily in the server-side. This architecture applied to this work is

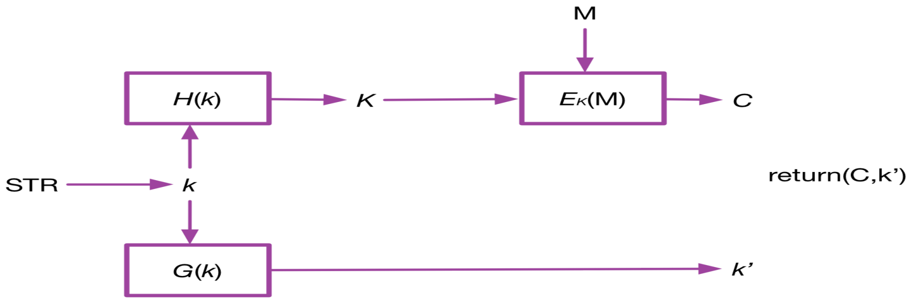


Fig. 1. P protocol

shown in Figure 3. In the first part of the system development were programmed key generation and SHA-256 hash function [4] to create the encryption key and generating CAPTCHA images

The first process is the key generation process that uses a dictionary of characters to get 8 elements which become the private key, to prevent visual confusions letters `l, o, q` and the numbers `1, 0` are removed.

Within CAPTCHA image generation process some transformations are applied to the image in the background, like circles of different diameters, and characters transformation like rotation, deformation and size [5]. These parameters are editable and can define the difficulty of the CAPTCHA.

With the process described above, it was possible to reach sending and receiving encrypted emails, for it used the library `javax.mail`. By using these protocols, is necessary include SMTP [6] and IMAP properties in the session. Each encrypted email sent by our system is marked at the final of the email subject with "- NoProfiling".

HTML5 allows the system to use WebSQL, which stores the email server domain's parameters. Also, Javascript (AJAX with jQuery), CSS, as Web technologies are used.

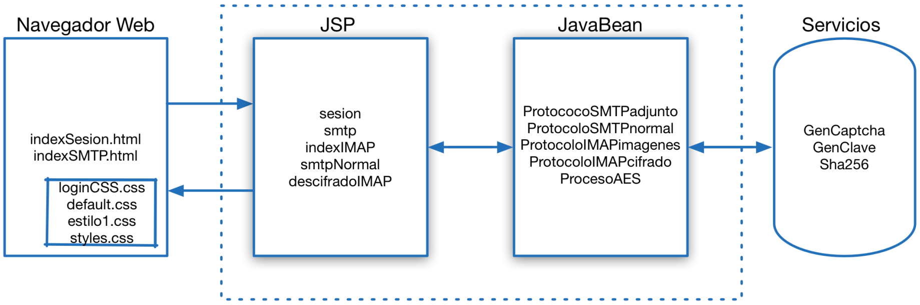


Fig. 2. Software Architecture type MVC-1 of the No Profiling System

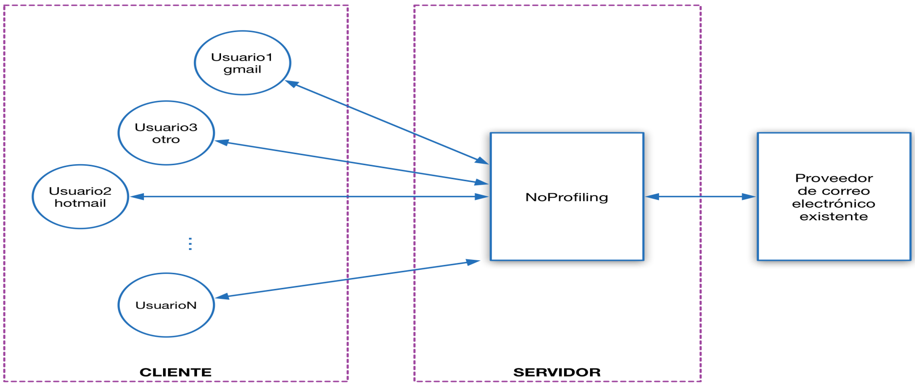
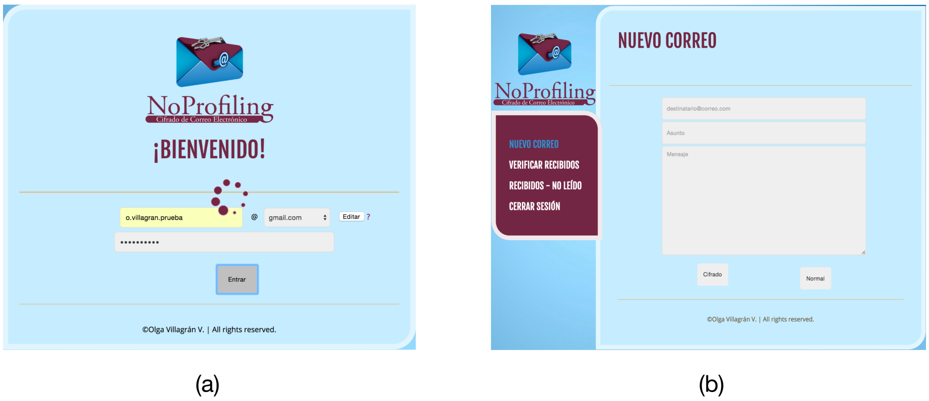


Fig. 3. Client-server architecture of the No Profiling System

Figure 4 (a), shows a login system screen, here, users must enter data in text fields and select the domain from their provider. The information registered here is passed to a JSP page to verify and only if it is correct, users can access and generate the image CAPTCHA from encrypted emails received so far.

Figures 5 and 4 (b) show the screen displayed for users to perform the tasks of sending and reading encrypted emails. In Figure 4 (b) in the left part have a menu to select the action by default the login show the option to send a email. In this part the user enter data in text fields corresponding to addressee information, before that user select a type to send the email encrypted or normal. If option is encrypted the system execute a JSP page to encrypt the email [7].

Figure 5 shows the screen where the users can read a encrypted and normal email. The screen show two emails the first one is a normal email and the second is a encrypted email this can be identifying bye the word "- NoProfiling" in the



o.villagran.prueba @ gmail.com

••••••••••

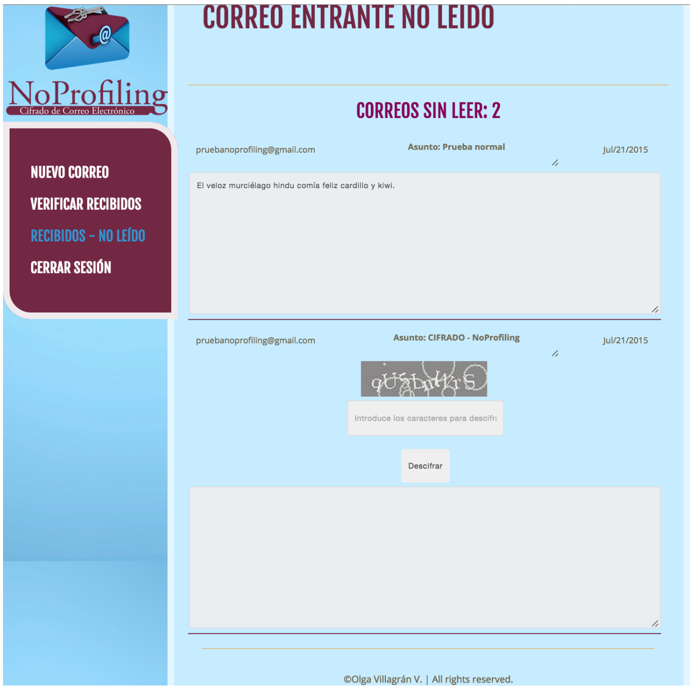
destinatario@correo.com

Asunto

Mensaje

Fig. 4. NoProfiling system screens: (a) login, (b) new email

subject, then is shown the corresponding image CAPTCHA, in the text field the user write the correct characters and clic “Descifrar” to show the email in the text area. Like is showing in Figure 6.



CORREO ENTRANTE NO LEIDO

CORREOS SIN LEER: 2

pruebanoprofiling@gmail.com Asunto: Prueba normal Jul/21/2015

El veloz murciélago hindu comía feliz cardillo y kiwi.

pruebanoprofiling@gmail.com Asunto: CIFRADO - NoProfiling Jul/21/2015

Introduce los caracteres para descifr

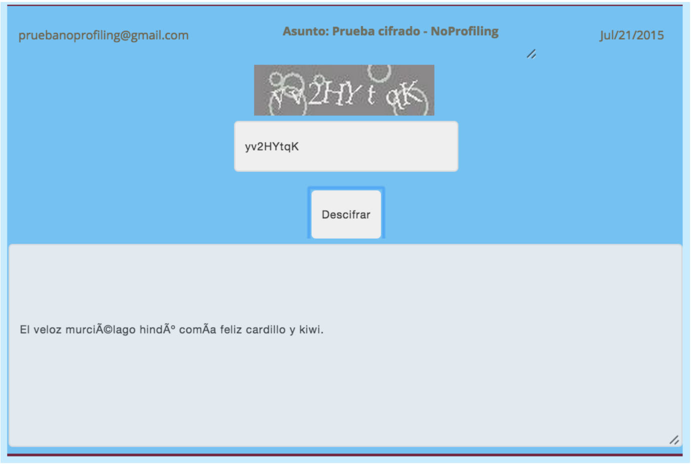
©Olga Villagrán V. | All rights reserved.

Fig. 5. NoProfiling screenshot: receiving email

The implementation of AJAX into the application is to exchange user’s data between JSP, to obtain the result and show it to the user. This technology allows to the server requests are made in second plane avoid that the user does not visualize this activities. The system uses JavaScript language to facilitates implementation the system business logic.

To execute the action to send a encrypted email, the user needs to press the button “Cifrado” it obtains the user’s data and the system passes them to JSP pages for the corresponding process.

For reading received emails, exists a preview process that allows the CAPTCHA image generation, this is performed knowing the number of emails that have not reading yet, after that, decrypting process is execute without knowledge of the user [8]. The programming of the mobile application v. Figure 7 it developed in the AndroidStudio IDE, it allows to make the login, this login interact with the process of the system.



pruebanoprofiling@gmail.com

Asunto: Prueba cifrado - NoProfiling

Jul/21/2015

yv2HYtqK

El veloz murciÃ©lago hindÃº comÃa feliz cardillo y kiwi.

Fig. 6. NoProfiling screenshot: decrypted email

3 Results

The obtained results of the test made, consist in:

- Result 1: For the proof to login into the system, contemplating the correct navigation, insert data and access to the system. In this test was entered with valid data and with all inputs completed correctly and different domains. As a result the introduced data was validated by email provides. As a special consideration have that the user needs a email account with access to less secure application permission inside account configuration.
- Result 2: Encrypt an email with a high level of usability. In this test was introduced the corresponding data to email addressee as the same time the subject and the message of the email, "Cifrado" was clicked to start the process. The result of this informed that it was realized the process of sending an email showing a GIF image, finally the system show an alert that the email was sending correctly.
- Result 3: Read and decrypt an email, check the use of CAPTCHAS in these process to received the key to decrypt the message. To realize this test it was clicked in "Recibidos - No Ledos", identified the encrypt email whit the phrase "- NoProfiling" include in the subject, writing the corrects characters of the CAPTCHA showed and "Descifrar" was clicked. As a result to introduce the correct characters of the CAPTCHA it was showed the original message.
- Result 4: The time to processing an encrypted email is 10 seconds approximated, that is because the system create a key to encrypt and insert attachments into the email and then send it. This process create a secure email from BOT attacks.

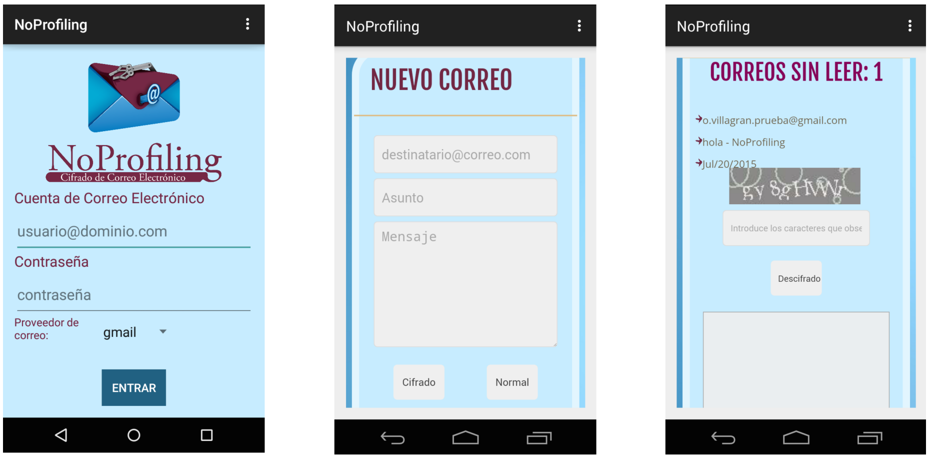


Fig. 7. Screenshot of NoProfiling mobile application

4 Conclusions

Thus, after design and develop the NoProfiling system they based the following conclusions. Technological impact:

- The use of corporative or free email services for academic, professional or personal purposes not condition the expose and use the information contained in it. Given this, the sending email protocols let the manipulation of information before send email on the Internet, offering the possibility to make transforms on information (in case of this project, encrypt).
- The encrypt algorithms implementation on emails services, give security on user information. Thus get to avoid attacks that wants to obtain and use information improperly. The symmetric algorithms when implemented in systems focus on usability offer an advantage in use the same key to encrypt and decrypt information.
- A form to store encrypt information is generate files with a specific extension, in relation with encrypt, that protocols accepts the pgp extension. This type to storage enable send encrypt information like attachment into a email. Thanks with that, the information can be send without drawback and then, avoid generate other methods to send encrypt information.
- CAPTCHA are elements that people use frequently although it use isn't knowing, these attribute let the implementation in any system to authentic people, doing a discrimination between people and machines, avoid that BOT attacks get into a system.

Social impact:

- An interface design is a important process to get the user to use the system effectively. For these reason, make the design focus on the final user increase the benefits in the system use.

- Market study on the users will be increase the system use. After email users study it was determined that the users with low or null knowledge on security are the more vulnerables in the face of cybernetic attacks in special BOT attacks that generate user profiles.

5 Future Work

On the results obtained in the develop and implementation in this project combined with the dizzying demand of more features and high level of usability, expose the future work that will be incorporate into NoProfiling system, highlighting:

- Due to existence of other email access protocols, is possible to implement them in the system to offer more options into NoProfiling system to the users.
- The information encrypt can be extend to attachments on the email.
- Include the option to generate a new CAPTCHA image to make a key with other distortions and visualize in other perspective the image. Also, with the evolution of CAPTCHA algorithms it can include the re-CAPTCHA in the system.
- Developing a desk application the NoProfiling system it going to increase the number of users of the system.

The good implementation of the previos features, will achieve the develop of a more robust system to avoid to generate user profiles.

References

1. BBC News Dave Lee, Technology reporter. Russian evgeniy bogachev sought over cybercrime botnet.
2. Advanced Encryption Standard (AES), November 2001.
3. Sandra Díaz Santiago and Debrup Chakraborty. On securing communication from profilers. *Department of Computer Science, CINVESTAV IPN*, 2012.
4. J. Menezes Alfred, C. van Oorschot Paul, and A. Vanstone Scott. *Handbook of Applied Cryptography.* CRC Press, 1997.
5. Kuenzang Norbu and Pattarasinne Bhattarakosol. Factors towards the effectiveness of CAPTCHA. *7th International Conference on Computing and Convergence Technology (ICCCT)*, 2012.
6. Jonathan B. Postel. RFC821: Simple Mail Transfer Protocol, August 1982.
7. Jakob Nielsen. Usability 101: Introduction to usability. *NN/g Nielsen Norman Group*, January 2012.
8. Joaqín Pintos Fernández. *UF1843: Aplicación de técnicas de usabilidad y accesibilidad en el entorno cliente.* ic editorial, 2014.