



Aplicación de cifrado contra de adversarios clasificadores, para el correo electrónico

Título del Trabajo Terminal

Trabajo Terminal No. 2015-A010

Alumnos: Arcos Ayala Jonathan, Zepeda Ibarra Allan Ulises*

Directores: Díaz Santiago Sandra, Soto Ramos Manuel Alejandro

e-mail: tt.aplic.cifrado@gmail.com

Resumen – En este Trabajo Terminal se desarrollará una herramienta de cifrado que protegerá al correo electrónico, contra un tipo especial de adversario, denominado adversario clasificador. El objetivo de este adversario es analizar una gran cantidad de información, para clasificar al usuario en categorías predeterminadas. La herramienta que se propone utiliza de manera novedosa los CAPTCHAs y una técnica criptográfica conocida como secreto compartido, para facilitar el acuerdo de las claves de cifrado. Adicionalmente, la aplicación utilizará un servidor de llaves para la autenticación de los usuarios para proveer una forma segura de enviar mensajes cifrados y recuperarlos.

Palabras clave – Criptografía, Correo electrónico, Secreto compartido, CAPTCHAs.

1. Introducción

Actualmente, una gran cantidad de personas hacen uso del internet y de las nuevas tecnologías para comunicarse. Con ello, también se incrementa la cantidad de información que se transmite y/o almacena. En diversas ocasiones, esta información es susceptible a sufrir distintos tipos de ataques, tales como acceso no autorizado, modificación o destrucción de la misma, entre otros. Adicionalmente, cada día aparecen nuevos tipos de ataques a los sistemas de información. Por lo tanto, surge la necesidad de proteger dicha información.

Una de las tecnologías ampliamente usada para comunicarse es el correo electrónico [1]. Los mensajes que envían y reciben los usuarios de correo electrónico pueden ser de diferentes tipos: personales, transaccionales, de notificación o de publicidad. Por lo tanto, cada vez que se escribe y envía un correo electrónico, se está revelando información acerca de las preferencias y/o intereses del usuario. Estos datos, son el insumo más importante, para distintas entidades, entre las cuales están empresas que realizan publicidad en línea, proveedores de internet, instituciones de gobierno, entre otros [3]. El propósito de tener estos datos puede ser realizar publicidad efectiva, vender los datos a empresas de publicidad o averiguar si determinado usuario es una amenaza para el gobierno. Para obtener información acerca de los intereses y/o preferencias del usuario, se hace uso de programas de cómputo denominados *clasificadores*. Los clasificadores son herramientas informáticas que analizan una gran cantidad de información, haciendo uso de técnicas de *machine learning*[4], y posteriormente clasifican un mensaje en determinada categoría o perfil. En este contexto, los clasificadores pueden constituir una amenaza para algunos usuarios del correo electrónico, por tal motivo de ahora en adelante a los programas que clasifican se les denominará *adversarios clasificadores*.

Ante tal escenario, surge la pregunta ¿cómo se puede proteger un usuario contra los adversarios clasificadores? Una posible respuesta es hacer uso de algoritmos de cifrado estándar. Sin embargo, hacer uso de tales algoritmos, implica que los participantes en la comunicación acuerden una clave de cifrado. Desafortunadamente, acordar una clave, no es un proceso sencillo para el usuario común. Otra desventaja de esta primera solución, es que los algoritmos de cifrado estándar ofrecen un alto nivel de seguridad, el cual resulta excesivo cuando se considera los recursos y el objetivo de un adversario clasificador[5].

Lo que se pretende en este trabajo terminal, es ofrecer al usuario una solución alternativa para proteger al correo electrónico, contra adversarios clasificadores. Dicha solución se considera más fácil de usar y además ofrece un nivel de seguridad adecuado, teniendo en cuenta las características de dichos adversarios. La solución que se propone, hará uso de CAPTCHAs y de un algoritmo criptográfico, conocido como *secreto compartido*. Los CAPTCHAs son programas de cómputo, cuyo propósito es distinguir si están interactuando con una máquina o con un ser humano.

El secreto compartido es una técnica criptográfica, que permite dividir un secreto en “n” partes, este secreto puede ser por ejemplo un CAPTCHAs, finalmente las “n” partes se dividen entre diferentes entidades. Para poder recuperar el secreto no es necesario recuperar las “n” partes en las que se dividió el secreto, sólo es necesario recuperar un número mínimo de partes para deducir el secreto, este número mínimo debe ser menor o igual al número de partes en que se dividió el secreto y está definido por la implementación de la técnica criptográfica; en caso de no recuperar el número mínimo de partes del secreto la técnica nos dicta que no es posible recuperar el secreto.

Recibi Protocolo
17-JUN-2015

Recibi Protocolo
Nidia Cortez

Existen aplicaciones que cifran el correo electrónico, aunque ninguna de ellas esta enfocada específicamente a combatir a los adversarios clasificadores. Dichas aplicaciones usan diversas técnicas criptográficas para proteger la información, en la **Tabla 1** vemos algunas de ellas.

SOFTWARE	CARACTERÍSTICAS
Aplicación Trend Micro Email Encryption Client [6]	<ul style="list-style-type: none"> • Usa un servidor de claves para administrar los mensajes • Usa cifrado basado en identidad • Usa AES y ECC • El descifrado es por medio del navegador • Cifra todo el mensaje incluyendo archivos adjuntos. • Licencia por equipo de cómputo. • Costo por licencia: 60 – 90 Euros.
Cifrador de Outlook 2007 [7]	<ul style="list-style-type: none"> • Usa certificado de llave pública • Usa 3DES y RC2 • Envío de claves por correo electrónico
Mailvelope [8]	<ul style="list-style-type: none"> • Envío de claves por correo electrónico • Soporta Gmail, GMX, Outlook, Yahoo • token de seguridad • Usa PGP
Thunderbird [9]	<ul style="list-style-type: none"> • Envío de claves por correo electrónico • Usa Open PGP

Tabla 1. Resumen de productos similares.

2. Objetivo

Desarrollar una herramienta para un cliente de correo electrónico que permita cifrar el contenido de los correos para evitar su clasificación, basándonos en la técnica de criptográfica de secreto compartido y asegurando el envío y recepción de los CAPTCHAs a través de un repositorio, basándonos en un esquema de cifrado por identidad.

2.1 Objetivos Específicos

- Desarrollar un algoritmo de cifrado y descifrado basado en secreto compartido.
- Desarrollar una herramienta en un cliente de correo electrónico para el envío y recepción de los correos cifrados y la generación, envío y recepción de CAPTCHAS.
- Desarrollar un servidor de llaves que reciba, aloje y envíe los CAPTCHAs a los usuarios para descifrar los correos electrónicos.

3. Justificación

Lo que se pretende en este trabajo terminal, es ofrecer al usuario una solución alternativa para proteger al correo electrónico, contra los clasificadores. Dicha solución se considera más fácil de usar y además ofrece un nivel de seguridad adecuado, teniendo en cuenta las características de los clasificadores. La solución que se propone, hará uso de CAPTCHAs y de un algoritmo criptográfico, conocido como *secreto compartido*. Los CAPTCHAs son programas de cómputo, cuyo propósito es distinguir si están interactuando con una máquina o con un ser humano. El secreto compartido es una técnica criptográfica, que permite dividir un secreto K en w partes, de tal manera que si se tienen al menos u de w , donde $u \leq w$, es posible recuperar K . Si se tienen menos de u partes no es posible recuperar K [11].

Este algoritmo criptográfico tiene una gran ventaja al momento de la generación de llaves, ya que sus llaves son simétricas a diferencia de muchos algoritmos estándares que utilizan una generación de un par de llaves asimétricas, estos algoritmos criptográficos asimétricos nos llevan a necesitar una comunicación previa entre el emisor y el receptor del mensaje enviado.

Mientras que al usar secreto compartido solo es necesario que el emisor genere una llave, la divida y envíe los CAPTCHAs, y que el receptor resuelva los CAPTCHAs, recupere la llave y posteriormente el mensaje de correo electrónico.

El envío de los correos se propone hacerlo enviando el correo electrónico con el contenido cifrado a un servidor de correo electrónico donde se alojará hasta que el cliente de correos electrónico instalado en el equipo de cómputo del receptor lo descargue por medio del protocolo POP3, al mismo tiempo se enviarán los CAPTCHAs que permiten recuperar la llave de cifrado a un tercer agente llamado servidor de llaves, el cuál verificará que la petición hecha por el receptor es válida y que el receptor es un usuario válido. El protocolo SSL se usará para garantizar el envío de los CAPTCHAs por parte del emisor, la correcta recepción por parte el servidor de llaves y la recuperación por parte del receptor para la correcta recuperación de la llave de cifrado y posterior descifrado de los correos electrónicos. El servidor de llaves es fundamental para el funcionamiento de este sistema, ya que esto le da un nivel de seguridad un poco más elevado que si lo enviáramos todo en un sólo paquete.

4. Productos o Resultados esperados

Los productos esperados en el presente Trabajo Terminal, teniendo en cuenta el tiempo de desarrollo, se enlistan a continuación.

1. Herramienta para un agente de usuarios de correo electrónico.
 2. Un servidor de CAPTCHAs.
 3. Manual de usuarios.
 4. Reporte Técnico.
- Herramienta para un agente de usuarios de correo electrónico.

Esta Herramienta se desarrollará en un agente de correo electrónico y tendrá los siguientes módulos:

1. Cifrado del contenido del correo.
 2. Generación de llaves y catpchas.
 3. Envío de CAPTCHAs al servidor de CAPTCHAs.
 4. Interfaz de conexión al servidor de CAPTCHAs.
 5. Descifrado del contenido del correo.
 6. Interfaz de visualización de CAPTCHAs.
- Servidor de CAPTCHAs.

Se entregará el servicio de servidor de CAPTCHAs que contendrá los siguientes elementos:

1. Repositorio de CAPTCHAs.
2. Envío y recepción de CAPTCHAs

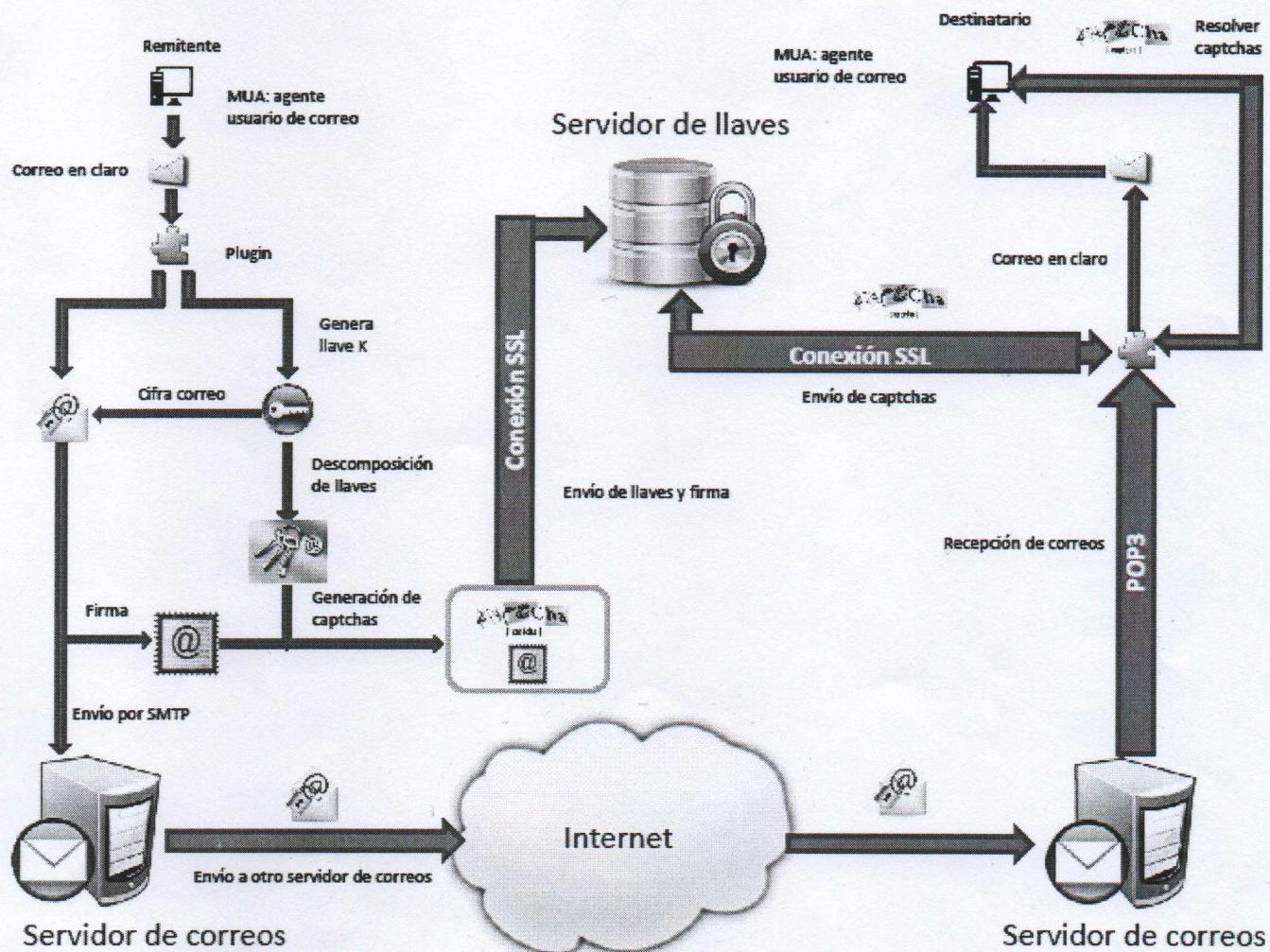


Figura 1. Esquema de envíos de correos.

- Manual de usuario.

Este documento contendrá una explicación detallada de la instalación de la herramienta en el agente de correo electrónico, la configuración para la comunicación con el servidor de CAPTCHAS y su uso en conjunto con el agente de correo electrónico.

- Reporte técnico.

En este último documento encontraremos todo el desarrollo y el desglose del proyecto bajo la metodología ágil SCRUM [11].

5. Metodología

En este trabajo terminal se utilizará la metodología ágil Scrum ya que proporciona un marco lo suficientemente flexible para trabajar problemas complejos en cortos períodos de desarrollo. Otro de los beneficios obtenidos con esta metodología es que propone hacer pequeños prototipos al final de cada ciclo de operación, estos ciclos de operación son llamados por la metodología iteraciones.

Estas iteraciones inician con una planificación de la iteración, en donde se define el objetivo que se debe cumplir en ésta iteración; cuales son las tareas que se tienen que realizar para cumplir el objetivo y quienes son los responsables de la culminación de cada

tarea. Esto nos ayuda a saber cuáles son las tareas específicas que tenemos que hacer en cada iteración y cuál es el producto final al que se debe de llegar al término de la iteración.

Una vez finalizada la iteración es evaluado el desempeño del equipo y del producto entregable. Con estas evaluaciones podemos hacer ajustes en la manera de trabajo o el desempeño de los miembros del equipo y tomas, de una manera oportuna, las medidas correctivas necesarias para que la siguiente iteración mejore.

Este marco de trabajo nos beneficia ya que los entregables propuestos en este trabajo terminal pueden ser desarrollados por separado para posteriormente ser integrados y que trabajen como una sola aplicación, esto se debe al hecho de que la herramienta se trabajará en el desarrollo de una herramienta que complementará a un cliente de correo electrónico instalado en un equipo de cómputo y por otro lado tendremos un servidor de llaves que hará la gestión de las llaves de cifrado y descifrado de los correos electrónicos. Para finalizar se necesita establecer la comunicación entre la herramienta desarrollada y el servidor de llaves para hacer el cifrado y descifrado de correos electrónicos [10].

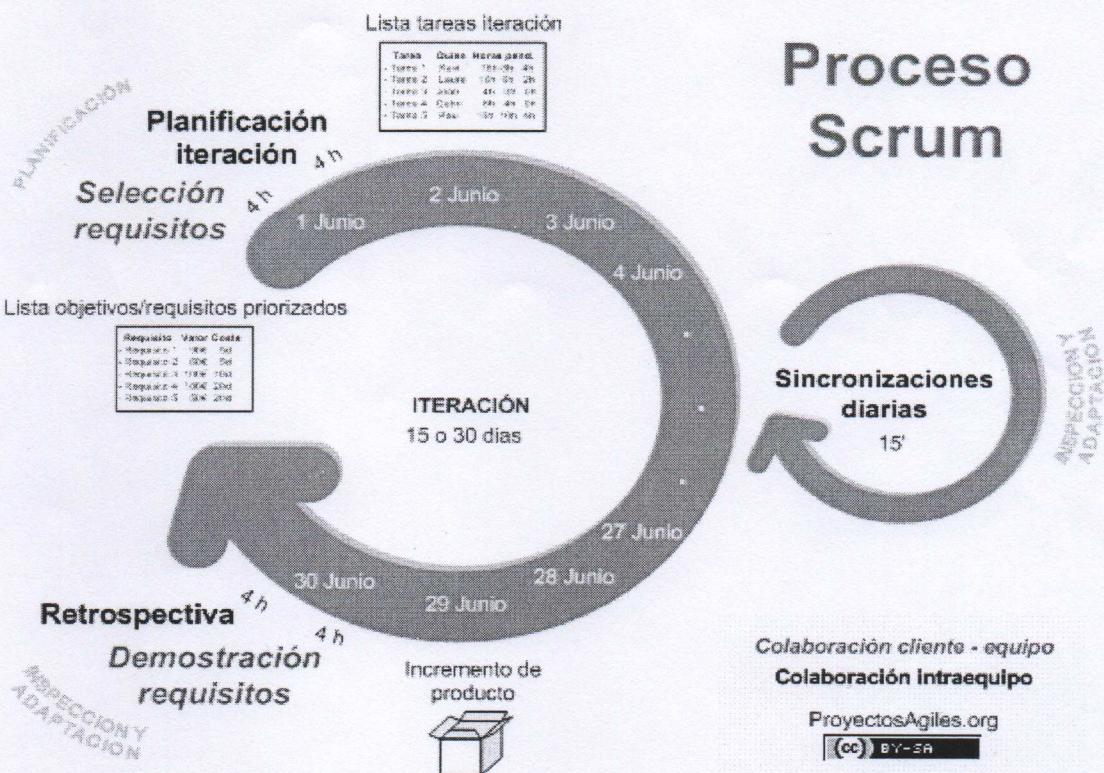


Figura 2 Esquema de la metodología Scrum

6. Cronograma

Nombre del alumno(a): Jonathan Arcos Ayala
Título del TT:

TT No.: 2015-A010

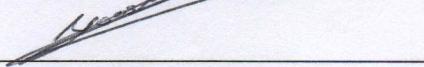
7. Referencia

- [1] "Email", Internet: <http://en.wikipedia.org/wiki>Email>, Mayo, 2015
- [2] B. Templeton, "Essays in Junk E-mail (Spam)", Internet: <http://www.templetons.com/brad/spam/>
- [3] Interactive Advertising Bureau, Marcelo Brodsky, "Reflexiones jurídicas sobre el e-marketing en Chile", Internet: <http://www.iab.cl/reflexiones-juridicas-sobre-ele-marketing-en-chile>.
- [4] D. Jurafsky, Text Classification, Stanford University Natural Language Processing.
- [5] S. Díaz Santiago y D. Chakraborty. "On Securing Communication from Profilers." Proceedings of International Conference on Security and Cryptography, Secrypt 2012, pp.154-162, Rome, Italy, 2012.
- [6] Trend Micro, "Email encryption", Internet: <http://www.trendmicro.es/productos/email-encryption/>
- [7] Office, "Cifrar mensaje de correo electrónico", Internet: <https://support.office.com/es-es/article/Cifrar-mensajes-de-correo-electr%C3%B3nico-84d7e382-5f76-4d71-8705-324489b710a2?CorrelationId=d5c846d3-8fb7-4935-b67e-6548a430acd4&ui=es-ES&rs=es-ES&ad=ES>
- [8] Mailvelope, "Documentation", Internet: <https://www.mailvelope.com/help>
- [9] Thunderbird, "Firma digital y cifrado de mensajes", Internet: <https://support.mozilla.org/es/kb/firma-digital-y-cifrado-de-mensajes>
- [10] K. Schwaber y J. Sutherland, "Scrum guides", Internet: <http://www.scrumguides.org/scrum-guide.html>, Julio, 2013.
- [11] D. R. Stinson, "Cryptography Theory and Practice", 3a ed, Ontario, Canada. Chapman&Hall/CRC. 2006

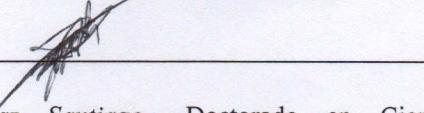
8. Alumnos y Directores

Jonathan Arcos Ayala.- Alumno de la carrera de Ing. En Sistemas Computacionales en ESCOM, Boleta: 2011600070, Tel. 55-1153-7443, email jonas.arcos.99@gmail.com

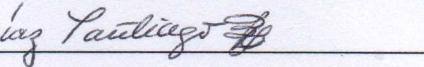
CARÁCTER: Confidencial
FUNDAMENTO LEGAL: Art. 3, fracc. II, Art. 18, fracc. II y Art. 21, lineamiento 32, fracc. XVII de la L.F.T.A.I.P.G.
PARTES CONFIDENCIALES: No. de boleta y Teléfono.

Firma: 

Allan Ulises Zepeda Ibarra.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Boleta: 2011630588, Tel.55-3470-5635 , email balaju01@gmail.com

Firma: 

Sandra Díaz Santiago.- Doctorado en Ciencias en Computación en CINVESTAV-IPN, en 2014, Maestría en Ciencias (Matemáticas) en la UAM-Iztapalapa, 2005. Licenciatura en Computación en UAM-Iztapalapa, en 2008. Profesor en ESCOM (Departamento de Ciencias e Ingeniería de la Computación), desde 2004, Áreas de Interés: Criptografía, Pseudoaleatoriedad, Seguridad Demostrable, Ext 52022, email: sdiazs@gmail.com, sdiazsa@ipn.mx.

Firma: 

Soto Ramos Manuel Alejandro.- M. en C. de la Computación, del Centro de Investigación en Computación del IPN en 2006, Ing. Mecánico Electrónico-Electrónico de la UNAM en 2003, Profesor de ESCOM/IPN (Departamento de Sistemas Computacionales) desde 2010, Áreas de Interés: Redes, Super-Cómputo, Cloud y Grid Computing. Ext. 52050, email msotoa06@yahoo.com.mx

Firma: 